BANCA D'ITALIA
EUROSISTEMA

DOCUMENTO PER LA CONSULTAZIONE

DISPOSIZIONI DI VIGILANZA PRUDENZIALE PER LE BANCHE

SISTEMA DEI CONTROLLI INTERNI, SISTEMA INFORMATIVO E CONTINUITÀ OPERATIVA

Il presente documento contiene uno schema di disposizioni di vigilanza in materia di sistema dei controlli interni e di sistema informativo delle banche e dei gruppi bancari nonché di continuità operativa delle banche e di altri intermediari.

Osservazioni, commenti e proposte possono essere trasmessi, ***entro 60 giorni dalla pubblicazione****, all'indirizzo di posta elettronica certificata npv@pec.bancaditalia.it; in alternativa, l'invio può avvenire per posta cartacea al Servizio Normativa e Politiche di Vigilanza, Divisione Normativa prudenziale, via Milano 53 – 00184 ROMA.*

I commenti ricevuti durante la consultazione saranno pubblicati sul sito web della Banca d'Italia. I partecipanti alla consultazione possono chiedere che i propri commenti non siano pubblicati oppure siano pubblicati in forma anonima; una generica indicazione di confidenzialità presente nelle comunicazioni inviate per posta elettronica non sarà considerata una richiesta di non divulgare i commenti. I commenti pervenuti oltre il termine sopra indicato non saranno presi in considerazione.

Settembre 2012

Relazione illustrativa

1. Premessa e principali finalità

Il presente documento di consultazione contiene disposizioni in materia di sistema dei controlli interni, sistema informativo e continuità operativa delle banche e dei gruppi bancari.

Le principali finalità dello schema di disciplina sono:

– il rafforzamento della capacità delle banche di gestire i rischi aziendali, in linea con l'esperienza della recente crisi finanziaria che ha messo in luce l'importanza del sistema dei controlli per assicurare la sana e prudente gestione delle banche e la stabilità del sistema finanziario;

– la revisione organica dell'attuale quadro normativo, resasi necessaria a seguito dell'emanazione, negli ultimi anni, di una serie di disposizioni (di vigilanza, contabili e societarie) che hanno interessato il funzionamento del sistema dei controlli interni ([1]). In tale ambito, si è tenuto conto dell'esigenza di inquadrare in modo coerente nel sistema dei controlli delle banche l'attività delle diverse funzioni societarie di controllo previste dall'ordinamento o dalle fonti di autoregolamentazione, tra le quali in particolare il Codice di Autodisciplina di Borsa italiana, (es.: organismo di vigilanza istituito ai sensi della legge n. 231/2001, dirigente preposto alla redazione dei documenti contabili societari previsto dall'art. 154-*bis* del TUF, compiti del comitato controllo e rischi e dell'amministratore incaricato del sistema di controllo interno e di gestione dei rischi);

([1]) Alle disposizioni in materia di sistema dei controlli interni delle banche e dei gruppi bancari (Circolare n. 229 del 21 aprile 1999, "*Istruzioni di vigilanza per le banche"*, Titolo IV, Capitolo 11) si sono aggiunte, negli anni, una serie di disposizioni, non solo di vigilanza, che interessano il funzionamento del sistema dei controlli degli intermediari. Si rammentano, a titolo di esempio, il processo di controllo prudenziale ai sensi del secondo pilastro per le banche (Circolare n. 263 del 27 dicembre 2006, "*Nuove disposizioni di vigilanza prudenziale per le banche*", Titolo III), la disciplina della funzione di controllo di conformità alle norme delle banche (Comunicazione del 10 luglio 2007), il "Regolamento congiunto della Banca d'Italia e dalla CONSOB" del 29 ottobre 2007 in materia di organizzazione e controlli degli intermediari che prestano servizi di investimento e di gestione collettiva, le disposizioni in materia di governo societario delle banche (Comunicazione del 4 marzo 2008) e le relative linee applicative (Comunicazione dell'11 gennaio 2012), le disposizioni in materia di politiche e prassi di remunerazione e incentivazione nelle banche e nei gruppi bancari del 30 marzo 2011, le disposizioni in materia di governo e gestione del rischio di liquidità (Circolare n. 263 cit., Titolo V, Capitolo 2), i compiti dell'organismo di vigilanza ai sensi della legge 231/2001 e il ruolo del dirigente preposto ai documenti contabili ai sensi dell'art. 154-*bis* del TUF; a ciò si aggiungono le fonti di autoregolamentazione che attribuiscono agli amministratori indipendenti degli intermediari quotati specifici compiti in materia di sistema di controllo interno e gestione dei rischi (Codice di Autodisciplina, Comitato per la Corporate Governance, Borsa Italia S.p.A.). Inoltre, vari organismi internazionali hanno pubblicato, negli ultimi anni, linee guida e raccomandazioni riguardo all'organizzazione e al sistema dei controlli interni (cfr., ad es. EBA/CEBS: "*Guidelines on the Application of the Supervisory Review Process under Pillar 2*", 25 January 2006; "*Guidelines on outsourcing*", 14 December 2006; "*Guidelines on the management of operational risks in market-related activities"*, 12 October 2010; "*Guidelines on Internal Governance*", 27 September 2011; Commissione europea: libro verde in materia di "*Corporate governance in financial institutions and remuneration policies*", 2 June 2010; Senior Supervisors Group: "*Observations on Risk Management Practices during Recent Market Turbulence*", 6 March 2008; "*Risk Management Lessons from the Global Banking Crisis of 2008*", 21 October 2009; "*Observations on Developments in Risk Appetite Frameworks and IT Infrastructure*", 23 December 2010; Basel Committee on Banking Supervision: "*Fair value measurement and modelling: An assessment of challenges and lessons learned from market stress*", June 2008; "*Principle for enhancing corporate governance*", October 2010; "*The internal audit function in banks*", June 2012; Financial Stability Board, "*Enhancing Market and Institutional Resilience*", 7 April 2008).

- la definizione di un quadro normativo omogeneo che, in base al principio di proporzionalità, tiene conto della natura dell'attività svolta, della tipologia dei servizi prestati, della complessità operativa e della dimensione operativa delle banche;
- la definizione di una disciplina coordinata con le disposizioni, contenute nel Regolamento congiunto Banca d'Italia – Consob del 29 ottobre 2007, in materia di organizzazione e controlli per la prestazione dei servizi di investimento, che si applicano anche alle banche;
- l'allineamento alle previsioni contenute nella proposta di direttiva del Parlamento europeo e del Consiglio sull'accesso all'attività degli enti creditizi e sulla vigilanza prudenziale degli enti creditizi e delle imprese di investimento e che modifica la direttiva 2002/87/CE del Parlamento europeo e del Consiglio relativa alla vigilanza supplementare sugli enti creditizi, sulle imprese di assicurazione e sulle imprese di investimento appartenenti ad un conglomerato finanziario, nonché nella proposta di Regolamento del Parlamento europeo e del Consiglio sui requisiti prudenziali per gli enti creditizi e le imprese di investimento (c.d. "CRD IV").

2. Struttura dello schema normativo

Lo schema di disciplina definisce un quadro organico di principi e regole cui deve essere ispirato il sistema dei controlli interni, ma non esaurisce le disposizioni applicabili ai diversi profili operativi delle banche. Esso, piuttosto, rappresenta la cornice di riferimento per le disposizioni sui controlli dettate all'interno di specifici ambiti disciplinari (ad es. in materia di gestione di singoli profili di rischio, di sistemi interni di misurazione dei rischi per il calcolo dei requisiti patrimoniali, di processo ICAAP, di prevenzione del rischio di riciclaggio), che ne completano e integrano la portata.

In quest'ambito, lo schema definisce:

- i principi generali del sistema dei controlli interni. Sono, fra l'altro, definiti principi generali di organizzazione, nell'ambito dei quali assumono rilievo l'adeguatezza dei flussi informativi interni, la chiarezza della struttura organizzativa e della relativa suddivisione di compiti, la prevenzione dei conflitti di interessi, le misure per assicurare la continuità aziendale (Capitolo 7, Sezione I);
- il ruolo degli organi aziendali (organi con funzioni: di supervisione strategica, di gestione, di controllo), a cui è rimessa la responsabilità primaria di formalizzare le politiche di governo dei rischi, di istituire il processo di gestione dei rischi e di procedere al loro riesame periodico. Lo schema fornisce indicazioni circa il ruolo di ciascun organo aziendale, anche al fine di chiarire i relativi compiti e responsabilità; inoltre, sono dettate specifiche disposizioni volte a promuovere il coordinamento delle diverse funzioni di controllo societarie (Capitolo 7, Sezione II);
- l'istituzione e i compiti delle funzioni aziendali di controllo (funzioni di: controllo dei rischi; conformità alle norme; revisione interna). Sono definiti i requisiti di indipendenza delle funzioni, la programmazione e la rendicontazione della loro attività, i rispettivi compiti e rapporti reciproci nonché i rapporti con le altre funzioni aziendali. In termini generali, è previsto che le banche istituiscano funzioni di controllo dei rischi, di conformità alle norme e di revisione interna indipendenti e fra loro separate; se coerente con il principio di proporzionalità, è consentito alle banche di istituire un'unica funzione di conformità alle norme e di controllo dei rischi, ferma restando l'esigenza di mantenere in ogni caso separata la funzione di revisione

interna per assicurare l'imparzialità dei controlli di *audit* sulle altre funzioni di controllo (Capitolo 7, Sezione III);

- l'esternalizzazione di funzioni aziendali. Le banche che adottano scelte di *outsourcing* devono presidiare attentamente i relativi rischi, mantenendo la capacità di controllo e la responsabilità delle attività esternalizzate nonché le competenze essenziali per re-internalizzare le stesse in caso di necessità; disposizioni specifiche riguardano le condizioni per esternalizzare funzioni aziendali importanti o di controllo (Capitolo 7, Sezione IV);
- i controlli nei gruppi bancari, che delineano i compiti della capogruppo nell'ambito dell'attività di direzione e coordinamento delle entità appartenenti al proprio gruppo e le caratteristiche del sistema dei controlli del gruppo al fine di assicurare la coerenza delle scelte strategiche del gruppo e l'equilibrio gestionale delle singole componenti (Capitolo 7, Sezione V);
- le regole applicabili alle succursali di banche comunitarie e di banche extracomunitarie aventi sede nei paesi del Gruppo dei Dieci. È previsto che sia condotta una verifica di conformità della condotta aziendale rispetto alle norme italiane applicabili alla succursale (Capitolo 7, Sezione VIII);
- il sistema informativo. La disponibilità di risorse ICT sicure, adeguate alle esigenze del business e in grado di supportare le strategie aziendali e il controllo dei rischi si affianca e accresce l'efficacia dei controlli interni. Sono definiti i requisiti di base in materia di governance e organizzazione dell'ICT, gestione del rischio informatico, sicurezza informatica, sistema di gestione dei dati, esternalizzazione di sistemi e servizi ICT (Capitolo 8).

Coerentemente con l'impostazione del nuovo impianto disciplinare, che detta una disciplina di carattere generale del sistema dei controlli delle banche, vengono riportate, dopo essere state razionalizzate ed aggiornate, alcune previsioni normative dettate nel corso del tempo con riferimento ad aspetti particolari, rilevanti ai fini della individuazione dei requisiti di affidabili ed efficaci sistemi di controllo interno. Esse riguardano i controlli sulle filiali estere (Capitolo 7, allegato B) e le disposizioni in materia di continuità operativa (Capitolo 9). L'inclusione in questo pacchetto consente di avere un quadro completo e sistematico e di più agevole consultazione di tutta la materia.

Il Capitolo 9, recante le disposizioni in materia di continuità operativa, è stato predisposto avendo come riferimento oltre alle banche e ai gruppi bancari anche i sistemi di pagamento e i relativi fornitori di servizi tecnologici nonché i gestori di infrastrutture di trading e post-trading vigilate dalla Banca d'Italia, in modo da consolidare in un unico documento le disposizioni in materia di continuità operativa della Banca d'Italia. In sede di emanazione delle disposizioni definitive, il Capitolo potrebbe essere enucleato dal presente schema normativo e trasformato in disposizioni autonome in materia di continuità operativa applicabili non solo alle banche ma anche agli altri soggetti interessati.

3 Principali novità

Rispetto al vigente quadro normativo, i principali elementi di novità riguardano:

- l'introduzione di specifici principi generali di organizzazione che, oltre agli aspetti strettamente pertinenti al sistema dei controlli, riguardano altri profili, quali le politiche di gestione delle risorse umane e la prevenzione dei conflitti di interessi (cfr. Capitolo 7, Sezione I, par. 5);

- l'obbligo per le banche di definire processi e metodologie di valutazione, anche a fini contabili, delle attività aziendali in modo integrato con il processo di gestione del rischio (cfr. Capitolo 7, Sezione I, par 5);
- l'obbligo, da parte dell'organo con funzione di supervisione strategica, di definire il livello di rischio tollerato (c.d. "tolleranza al rischio" o "appetito per il rischio") (cfr. Capitolo 7, Sezione II, par. 2);
- l'approvazione, da parte dell'organo con funzione di supervisione strategica, di un codice etico a cui sono tenuti a uniformarsi i componenti degli organi aziendali e i dipendenti (cfr. Capitolo 7, Sezione II, par. 2);
- l'adozione di un approccio integrato alla gestione dei rischi (cfr., ad es., Capitolo 7, Sezione II, par. 3);
- l'obbligo da parte degli organi aziendali di definire il processo per l'approvazione di nuovi prodotti e servizi, l'avvio di nuove attività e l'inserimento in nuovi mercati (cfr. Capitolo 7, Sezione II, parr. 2 e 3);
- le disposizioni relative al coordinamento delle funzioni di controllo societarie (cfr. Capitolo 7, Sezione II, par. 5);
- le modalità di nomina e revoca dei responsabili delle funzioni di controllo (cfr. Capitolo 7, Sezione III, par. 1);
- con riferimento alla funzione di conformità alle norme, particolare attenzione è posta sul rispetto della normativa fiscale in virtù delle significative ripercussioni in termini di rischio di reputazione e conseguenti danni patrimoniali che la violazione o l'elusione di tale normativa, ivi incluse le situazioni di abuso del diritto, comportano (cfr. Capitolo 7, Sezione III, par. 3.2) ([2]);
- il rafforzamento dei poteri della funzione di controllo dei rischi (*risk management function*), che tra l'altro è tenuta a fornire pareri preventivi sulla coerenza con la politica aziendale di governo dei rischi delle operazioni di maggiore rilievo (cfr. Capitolo 7, Sezione III, par. 3.3);
- la previsione di una disciplina organica in materia di esternalizzazione di funzioni aziendali (cfr. Capitolo 7, Sezione IV), in linea con gli orientamenti definiti nelle sedi internazionali e con le disposizioni contenute nella disciplina organizzativa dei servizi di investimento ([3]); in particolare, è prevista la notifica preventiva alla Banca d'Italia e, in alcuni casi, la possibilità di vietare l'*outsourcing* di funzioni operative importanti o di controllo;
- l'obbligo dell'organo con funzioni di supervisione strategica di definire procedure di allerta interna (*internal alert*) volte a permettere la segnalazione da parte dei dipendenti di eventuali disfunzioni dell'assetto organizzativo o del sistema dei controlli interni nonché di ogni altra irregolarità nella gestione della banca o violazione delle norme disciplinanti l'attività bancaria (cfr. Capitolo 7, Sezione II, par. 2 e Sezione VII);

([2]) A tale proposito, si segnala che la disciplina della gestione e del controllo del rischio fiscale nell'ambito del sistema dei controlli interni è all'attenzione del legislatore e il relativo quadro normativo è destinato ad evolversi (cfr. in particolare l'articolo 6 del disegno di legge C. 5291, presentato il 15 giugno 2012 in materia di "delega al Governo recante disposizioni per un sistema fiscale più equo, trasparente e orientato alla crescita").

([3]) Cfr. CEBS, "*Guidelines on outsourcing*" e "Regolamento congiunto della Banca d'Italia e dalla CONSOB" cit.

- la disciplina organica e aggiornata in materia di sistema informativo, con particolare riferimento a: la governance e l'organizzazione dell'ICT, la gestione del rischio informatico, la sicurezza informatica, il sistema di gestione dei dati, l'esternalizzazione di sistemi e servizi ICT (cfr. Capitolo 8).
- tra i requisiti in tema di continuità operativa (cfr. Capitolo 9), è prevista la condivisione di informazioni tra il sistema di *incident management* e la struttura preposta alla dichiarazione dello stato di emergenza, in caso di eventi di elevata gravità.

4. Collocazione e abrogazioni

Il presente documento sarà inserito nella Circolare n. 263 del 27 dicembre 2006, "Nuove disposizioni di vigilanza prudenziale per le banche", in sostituzione della parte riguardante *"La gestione e il controllo dei rischi. Ruolo degli organi aziendali"* ([4]). In quanto ricomprese nella nuova disciplina, saranno abrogate le seguenti disposizioni:

- *Sistema dei controlli interni, compiti del collegio sindacale*, contenute nelle "Istruzioni di vigilanza per le banche", Circolare n. 229 del 21 aprile 1999, Titolo IV, Capitolo 11, ad eccezione della Sezione V (emissione e gestione di assegni bancari e postali);
- *La gestione e il controllo dei rischi. Ruolo degli organi aziendali*, contenute nelle "Nuove disposizioni di vigilanza prudenziale per le banche", Circolare n. 263 del 27 dicembre 2006, Titolo I, Capitolo I, Parte Quarta, Circolare n. 263 del *27* dicembre 2006;
- *Disposizioni di vigilanza - la funzione di controllo di conformità alle norme delle banche* (Comunicazione del 10 luglio 2007);
- *Disposizioni di vigilanza – Esternalizzazione del trattamento del contante* (Comunicazione del 7 maggio 2007);
- *Disposizioni di vigilanza – Continuità operativa in casi di emergenza* (Comunicazione del luglio 2004);
- *Disposizioni di vigilanza – Requisiti particolari per la continuità operativa dei processi di rilevanza sistemica* (Comunicazione del marzo 2007).

La presente consultazione si inquadra nell'obbligo di rivedere periodicamente gli atti normativi di vigilanza, secondo quanto previsto dal Regolamento 24 marzo 2010 recante la disciplina dell'adozione degli atti di natura normativa o di contenuto generale della Banca d'Italia nell'esercizio delle funzioni di vigilanza bancaria e finanziaria, ai sensi dell'articolo 23 della legge 28 dicembre 2005, n. 262.

*****

* *

([4]) Cfr. Titolo I, Capitolo I, Parte Quarta.

Si sollecitano, in generale, commenti e osservazioni sulla presente proposta di disciplina.

In particolare, sono apprezzati commenti specifici sulle seguenti questioni:

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

Box 1

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.

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)

Box 2

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

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

Box 3

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

Si sollecitano commenti per declinare nel concreto 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.

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

Box 4

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

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

Box 5

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*.

Schemi normativi

Titolo V – Capitolo 7
IL SISTEMA DEI CONTROLLI INTERNI

Sezione I
Disposizioni preliminari e principi di carattere generale

1. Premessa

Il sistema dei controlli interni è un elemento fondamentale del complessivo sistema di governo delle banche; esso assicura che l'attività aziendale sia in linea con le strategie e le politiche aziendali e sia improntata a canoni di sana e prudente gestione.

Le presenti disposizioni definiscono i principi e le linee guida cui il sistema dei controlli interni delle banche si deve uniformare; in quest'ambito, sono definiti i principi generali di organizzazione, indicati il ruolo e i compiti degli organi aziendali, delineate le caratteristiche e i compiti delle funzioni aziendali di controllo.

La presente disciplina:

- rappresenta la cornice generale del sistema dei controlli aziendali. In materia di istituti di vigilanza prudenziale, essa è integrata e completata dalle specifiche disposizioni previste in materia (tecniche di attenuazione del rischio di credito ed operazioni di cartolarizzazione, processo ICAAP, informativa al pubblico, concentrazione dei rischi, gestione e controllo del rischio di liquidità, obbligazioni bancarie garantite, partecipazioni detenibili, attività di rischio e conflitti di interesse nei confronti di soggetti collegati). Inoltre, alle banche che utilizzano, a fini prudenziali, sistemi interni di misurazione dei rischi diversi da quelli di base o standardizzati, si applicano anche le norme in materia di organizzazione e controlli interni previste dai rispettivi capitoli;
- forma parte integrante del complesso di norme concernenti gli assetti organizzativi, di governo e di controllo delle banche, quali: le disposizioni in materia di organizzazione e governo societario, di requisiti organizzativi in materia di *information and communication technology*, i controlli sugli assetti proprietari, i requisiti degli esponenti aziendali, gli obblighi di trasparenza e correttezza delle relazioni tra banche e clienti e delle norme organizzative relative alle attività e ai servizi di investimento ([1]), le disposizioni in materia di organizzazione, procedure e controlli interni volti a prevenire l'utilizzo degli intermediari e degli altri soggetti che svolgono attività finanziaria a fini di riciclaggio e di finanziamento del terrorismo, le disposizioni in materia di usura.

I presidi relativi al sistema dei controlli interni devono coprire ogni tipologia di rischio aziendale. La responsabilità primaria è rimessa agli organi aziendali, ciascuno secondo le rispettive competenze. L'articolazione dei compiti e delle responsabilità degli organi e delle funzioni aziendali deve essere chiaramente definita.

([1]) Alle banche che prestano servizi di investimento si applicano anche le disposizioni contenute nel Regolamento della Banca d'Italia e della CONSOB del 29 ottobre 2007 in materia di organizzazione e controlli degli intermediari che prestano servizi di investimento e di gestione collettiva.

Le banche applicano le disposizioni secondo il principio di proporzionalità, cioè tenuto conto della dimensione e complessità operative, della natura dell'attività svolta, della tipologia dei servizi prestati.

La Banca d'Italia, nell'ambito del processo di revisione e valutazione prudenziale, verifica l'efficienza e l'efficacia del sistema dei controlli interni delle banche.

2. Fonti normative

La materia è regolata:

- dalla direttiva xxxx/xx/UE del xx xxxxxx 2012 sull'accesso all'attività degli enti creditizi e sulla vigilanza prudenziale degli enti creditizi e delle imprese di investimento e che modifica la direttiva 2002/87/CE del Parlamento europeo e del Consiglio relativa alla vigilanza supplementare sugli enti creditizi, sulle imprese di assicurazione e sulle imprese di investimento appartenenti ad un conglomerato finanziario;
- dal Regolamento xxxx/xx/UE del xx xxxxxx 2012 sui requisiti prudenziali per gli enti creditizi e le imprese di investimento;
- dai seguenti articoli del TUB:
  a) art. 53, comma 1, lett. d), che attribuisce alla Banca d'Italia, in conformità delle delibere del CICR, il potere di emanare disposizioni di carattere generale in materia di organizzazione amministrativa e contabile e controlli interni delle banche;
  b) art. 67, comma 1, lett. d), che attribuisce alla Banca d'Italia, in conformità delle delibere del CICR, il potere di impartire alla capogruppo di un gruppo bancario disposizioni concernenti il gruppo complessivamente considerato o i suoi componenti aventi ad oggetto l'organizzazione amministrativa e contabile e i controlli interni;
- dalla delibera del CICR del 2 agosto 1996, come modificata dalla delibera del 23 marzo 2004, in materia di organizzazione amministrativa e contabile e controlli interni delle banche e dei gruppi bancari;
- dal decreto del Ministro dell'Economia e delle finanze, Presidente del CICR del 5 agosto 2004 in materia, tra l'altro, di compiti e poteri degli organi sociali delle banche e dei gruppi bancari;
- decisione della BCE del 16 settembre 2010 n. 14, relativa al controllo dell'autenticità e dell'idoneità delle banconote in euro e al loro ricircolo;
- si tiene anche conto dei seguenti documenti pubblicati da istituzioni comunitarie e organismi internazionali: EBA/CEBS: "*Guidelines on the Application of the Supervisory Review Process under Pillar 2*", 25 January 2006; "*Guidelines on outsourcing*", 14 December 2006; "*Guidelines on the management of operational risks in market-related activities"*, 12 October 2010; "*Guidelines on Internal Governance*", 27 September 2011; Basel Committee on Banking Supervision: "*Fair value measurement and modelling: An assessment of challenges and lessons learned from market stress*", June 2008; "*Principle for enhancing corporate governance*", October 2010; "*The internal audit function in banks*", Consultative document, December 2011; Financial Stability Forum, "*Enhancing Market and Institutional Resilience*", 7 April 2008.

3. Definizioni

Ai fini delle presenti disposizioni si intendono per:

a) *"Organo con funzione di supervisione strategica"*: l'organo aziendale cui - ai sensi del codice civile o per disposizione statutaria - sono attribuite funzioni di indirizzo della gestione dell'impresa, mediante, tra l'altro, esame e delibera in ordine ai piani industriali o finanziari ovvero alle operazioni strategiche;

b) *"Organo con funzione di gestione"*: 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 corrente, intesa come 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;

c) *"Organo con funzione di controllo"*: il collegio sindacale, il consiglio di sorveglianza o il comitato per il controllo sulla gestione;

d) *"Organi aziendali"*: il complesso degli organi con funzioni di supervisione strategica, di gestione e di controllo. La funzione di supervisione strategica e quella di gestione attengono, unitariamente, alla gestione dell'impresa e possono quindi essere incardinate nello stesso organo aziendale. Nei sistemi dualistico e monistico, in conformità delle previsioni legislative, l'organo con funzione di controllo può svolgere anche quella di supervisione strategica;

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

f) *"Funzione operativa importante"*: una funzione operativa per la quale risulta verificata almeno una delle seguenti condizioni:

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

g) *"Processo di gestione dei rischi"*: l'insieme delle regole, delle procedure e delle risorse volte a identificare, misurare o valutare, monitorare, attenuare e comunicare ai livelli appropriati i rischi, come specificato nel par. 5.

4. Destinatari della disciplina

Le presenti disposizioni si applicano, secondo quanto stabilito nel Titolo I, Capitolo 1, Parte Seconda:

- alle banche autorizzate in Italia, ad eccezione delle succursali di banche extracomunitarie aventi sede nei paesi del Gruppo dei Dieci ovvero in quelli inclusi in un apposito elenco pubblicato e periodicamente aggiornato dalla Banca d'Italia ([2]);
- alle capogruppo di gruppi bancari;
- alle imprese di riferimento, secondo quanto previsto dalla Sezione VI;
- alle succursali di banche comunitarie e alle succursali di banche extracomunitarie di paesi appartenenti al Gruppo dei Dieci o inclusi in un apposito elenco pubblicato e periodicamente aggiornato dalla Banca d'Italia, secondo quanto previsto dalla Sezione VIII.

5. Unità organizzative responsabili dei procedimenti amministrativi

Si indicano di seguito le unità organizzative responsabili dei procedimenti amministrativi di cui alla presente Parte, ai sensi dell'art. 9 del Regolamento della Banca d'Italia del 25 giugno 2008:

- *divieto dell'esternalizzazione di funzioni operative importanti o di controllo in altri paesi:* Servizio Supervisione gruppi bancari, Servizio Supervisione intermediari specializzati, Filiale competente per territorio.

6. Principi generali

Il sistema dei controlli interni è costituito dall'insieme delle regole, delle funzioni, delle strutture, delle risorse, dei processi e delle procedure che mirano ad assicurare, nel rispetto della sana e prudente gestione, il conseguimento delle seguenti finalità:

- verifica dell'attuazione delle strategie e delle politiche aziendali;
- contenimento del rischio entro il limite massimo accettato ("tolleranza al rischio" o "appetito per il rischio") ([3]);
- salvaguardia del valore delle attività e protezione dalle perdite;
- efficacia ed efficienza dei processi aziendali;
- affidabilità e sicurezza delle informazioni aziendali e delle procedure informatiche ([4]);
- prevenzione del rischio che la banca sia coinvolta, anche involontariamente, in attività illecite (con particolare riferimento a quelle connesse con il riciclaggio, l'usura ed il finanziamento al terrorismo);
- conformità delle operazioni con la legge e la normativa di vigilanza, nonché con le politiche, i regolamenti e le procedure interne.

Il sistema dei controlli interni riveste un ruolo centrale nell'organizzazione aziendale: rappresenta un elemento fondamentale di conoscenza per gli organi aziendali in modo da garantire piena consapevolezza della situazione ed efficace presidio dei rischi

([2]) Alle banche che prestano servizi di investimento si applicano anche le disposizioni contenute nel Regolamento della Banca d'Italia e della CONSOB del 29 ottobre 2007 in materia di organizzazione e controlli degli intermediari che prestano servizi di investimento e di gestione collettiva.

([3]) Cfr. Sezione II, par. 2.

([4]) Cfr. Capitolo 8.

aziendali e delle loro interrelazioni; orienta i mutamenti delle linee strategiche e delle politiche aziendali e di adattare in modo coerente il contesto organizzativo; presidia la funzionalità dei sistemi gestionali e il rispetto degli istituti di vigilanza prudenziale; favorisce la diffusione di una corretta cultura dei rischi, della legalità e dei valori aziendali.

Per queste caratteristiche, il sistema dei controlli interni ha rilievo strategico; la cultura del controllo deve avere una posizione di rilievo nella scala dei valori aziendali: non riguarda solo le funzioni di controllo, ma coinvolge tutta l'organizzazione aziendale (organi aziendali, strutture, livelli gerarchici, personale), nello sviluppo e nell'applicazione di metodi, logici e sistematici, per misurare, comunicare, gestire i rischi.

Per poter realizzare questo obiettivo, il sistema dei controlli interni deve in generale:

- consentire di identificare, misurare o valutare, monitorare, attenuare e riportare ai livelli gerarchici appropriati adeguatamente tutti i rischi assunti o assumibili (strategico, credito, controparte, concentrazione, mercato, tasso di interesse, operativi, liquidità, reputazione, ecc.) ([5]) nei diversi segmenti, a livello di portafoglio di impresa e di gruppo, cogliendone, in una logica integrata, anche le interrelazioni reciproche e con l'evoluzione del contesto esterno ("*processo di gestione dei rischi*"). Si riportano, nell'Allegato A, le linee guida riferite a specifiche categorie di rischio, fermo restando quanto previsto nelle specifiche discipline relative alle singole tipologie di rischio;
- prevedere attività di controllo diffuse a ogni segmento operativo e livello gerarchico ([6]);
- garantire che le anomalie riscontrate siano tempestivamente portate a conoscenza di livelli appropriati dell'impresa (agli organi aziendali, se significative) in grado di attivare tempestivamente gli opportuni interventi correttivi;
- incorporare specifiche procedure per far fronte all'eventuale violazione di limiti operativi.

A prescindere dalle strutture dove sono collocate, si possono individuare le seguenti tipologie di controllo:

- *controlli di linea* (c.d. "controlli di primo livello"), diretti ad assicurare il corretto svolgimento delle operazioni. Essi sono effettuati dalle stesse strutture operative (es. controlli di tipo gerarchico, sistematici e a campione), anche attraverso diverse unità che riportano ai responsabili delle strutture operative, ovvero eseguiti nell'ambito del *back office*; per quanto possibile, essi sono incorporati nelle procedure informatiche. Le strutture operative sono le prime responsabili del processo di gestione dei rischi: nel corso dell'operatività giornaliera tali strutture devono identificare, misurare o valutare, monitorare, attenuare e riportare i rischi derivanti dall'ordinaria attività aziendale in conformità con il processo di gestione dei rischi; esse devono assicurare il rispetto del livello di tolleranza al rischio stabilito e delle procedure in cui si articola il processo di gestione dei rischi;
- *controlli sui rischi e sulla conformità* (c.d. "controlli di secondo livello"), che hanno l'obiettivo di assicurare, tra l'altro:

  a) la corretta attuazione del processo di gestione dei rischi;

([5]) Devono altresì essere considerati i rischi derivanti dall'ambiente macroeconomico in cui la banca opera anche con riferimento all'andamento del ciclo economico.

([6]) Nell'Allegato B sono previsti specifici controlli per le succursali estere di banche italiane.

b) il rispetto dei limiti operativi assegnati alle varie funzioni;

c) la conformità alle norme dell'operatività aziendale.

Le funzioni preposte a tali controlli sono distinte da quelle produttive; esse concorrono alla definizione delle politiche di governo dei rischi e del processo di gestione dei rischi;

– *revisione interna* (c.d. "controlli di terzo livello"), volta a individuare andamenti anomali, violazione delle procedure e della regolamentazione nonché a valutare periodicamente la completezza, la funzionalità e l'adeguatezza, in termini di efficienza ed efficacia, del sistema dei controlli interni, inclusi quelli sul sistema informativo (ICT *audit*), con cadenza prefissata in relazione alla natura e all'intensità dei rischi.

Presupposto di un sistema dei controlli interni completo e funzionale è l'esistenza di una organizzazione aziendale adeguata per assicurare la sana e prudente gestione delle banche e l'osservanza delle disposizioni loro applicabili.

A tal fine, rileva, in primo luogo, il corretto funzionamento del governo societario, le cui caratteristiche devono essere in linea con quanto previsto nelle disposizioni di vigilanza in materia di organizzazione e governo societario delle banche ([7]).

Inoltre, le banche rispettano i seguenti principi generali di organizzazione:

– i processi decisionali e l'affidamento di funzioni al personale sono formalizzati e consentono l'univoca individuazione di compiti e responsabilità e sono idonei a prevenire i conflitti di interessi. In tale ambito, deve essere assicurata la necessaria separatezza tra le funzioni operative e quelle di controllo;

– le politiche e le procedure di gestione delle risorse umane assicurano che il personale sia provvisto delle competenze e della professionalità necessarie per l'esercizio delle responsabilità ad esso attribuite;

– i processi e le metodologie di valutazione, anche a fini contabili, delle attività aziendali sono affidabili e integrati con il processo di gestione del rischio. A tal fine: la definizione e la convalida delle metodologie di valutazione sono affidate a unità differenti; le metodologie di valutazione sono robuste, testate sotto scenari di stress e non fanno affidamento eccessivo su un'unica fonte informativa; la valutazione di uno strumento finanziario è affidata a un'unità indipendente rispetto a quella che negozia detto strumento;

– le procedure operative e di controllo devono: minimizzare i rischi legati a frodi o infedeltà dei dipendenti; prevenire e attenuare i potenziali conflitti d'interesse; evitare il coinvolgimento, anche inconsapevole, in fatti di riciclaggio, usura o di finanziamento al terrorismo;

– il sistema informativo rispetta la disciplina del Capitolo 8;

– i livelli di continuità operativa garantiti sono adeguati e conformi a quanto stabilito dal Capitolo 9.

([7]) Cfr. "Disposizioni di vigilanza in materia di organizzazione e governo societario delle banche" del 4 marzo 2008 e le relative linee applicative dell'11 gennaio 2012.

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.

Sezione II
Il ruolo degli organi aziendali

1. Premessa

Le banche formalizzano le politiche di governo dei rischi, istituiscono un processo di gestione dei rischi e procedono al loro riesame periodico al fine di assicurarne l'efficacia nel tempo. La responsabilità primaria è rimessa agli organi aziendali, ciascuno secondo le rispettive competenze.

Nei successivi paragrafi si forniscono indicazioni minime circa il ruolo di ciascun organo aziendale nell'ambito del sistema dei controlli interni, anche al fine di chiarire i relativi compiti e responsabilità.

Tali indicazioni non esauriscono, pertanto, le cautele che possono essere adottate dai competenti organi aziendali nell'ambito della loro autonomia gestionale.

2. Organo con funzione di supervisione strategica

L'organo con funzione di supervisione strategica: i) approva il modello di *business* avendo consapevolezza dei rischi cui tale modello espone la banca e comprensione delle modalità attraverso le quali i rischi sono rilevati e valutati; ii) assicura che la struttura della banca sia coerente con l'attività svolta e con il modello di *business* adottato, evitando la creazione di strutture complesse non giustificate da finalità operative.

Più in dettaglio tale organo:

– definisce e identifica il livello di rischio accettato (c.d. "tolleranza al rischio" o "appetito per il rischio");

Box 1

La tolleranza al rischio (*risk tolerance*) e l'appetito per il rischio (*risk appetite*) sono 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.

– definisce:

a) gli indirizzi strategici e le politiche di governo dei rischi e provvede al loro riesame periodico, in relazione all'evoluzione dell'attività aziendale e del contesto esterno, al fine di assicurarne l'efficacia nel tempo;

b) le linee di indirizzo del sistema dei controlli interni, verificando che esso sia coerente con il livello di rischio accettato e gli indirizzi strategici stabiliti nonché sia in grado di cogliere l'evoluzione dei rischi aziendali e l'interazione tra gli stessi;

c) i criteri per individuare le operazioni di maggiore rilievo da sottoporre al vaglio preventivo della funzione di controllo dei rischi (cfr. Sezione III, par. 3.3.),

indicando l'estensione, i limiti e le modalità di esercizio dei poteri di detta funzione;

Box 2

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

d) le procedure di allerta interna (*internal alert*), secondo quanto previsto dalla Sezione VII;

– approva:

a) la costituzione delle funzioni aziendali e societarie di controllo, i relativi compiti e responsabilità, le modalità di coordinamento e collaborazione, i flussi informativi tra tali funzioni e tra queste e gli organi aziendali (cfr. anche par. 5);

b) il processo di gestione del rischio e ne verifica la compatibilità con gli indirizzi strategici e le politiche di governo dei rischi;

c) le politiche, i processi e le metodologie di valutazione delle attività aziendali, e, in particolare, degli strumenti finanziari, assicurandone la costante adeguatezza; stabilisce altresì i limiti all'esposizione della banca verso strumenti o prodotti finanziari di incerta o difficile valutazione;

d) il processo per lo sviluppo e la convalida dei sistemi interni di misurazione dei rischi non utilizzati a fini regolamentari ([8]) e ne verifica periodicamente il corretto funzionamento.

e) la politica aziendale in materia di esternalizzazione di funzioni aziendali (cfr. Sezione IV);

f) al fine di attenuare i rischi operativi e di reputazione della banca e favorire la diffusione di una cultura dei controlli interni, un codice etico cui sono tenuti a uniformarsi i componenti degli organi aziendali e i dipendenti. Il codice definisce i principi di condotta (es. regole deontologiche e regole da osservare nei rapporti con i clienti) a cui deve essere improntata l'attività aziendale.

– assicura che:

a) sia definito il processo per l'approvazione di nuovi prodotti e servizi, l'avvio di nuove attività, l'inserimento in nuovi mercati;

b) la quantità e l'allocazione del capitale e della liquidità detenuti siano coerenti con il livello di rischio accettato, le politiche di governo dei rischi e il processo di gestione dei rischi;

– nel caso in cui la banca operi in giurisdizioni poco trasparenti o attraverso strutture particolarmente complesse, valuta i relativi rischi operativi, in particolare di natura legale, reputazionali e finanziari, individua i presidi per mitigarli e ne assicura il controllo effettivo;

– con cadenza almeno annuale, esamina il programma di attività e le relazioni annuali predisposti dalle funzioni aziendali di controllo compreso il piano di *audit* predisposto dalla funzione di revisione interna (cfr. Sezione III, par. 2).

([8]) Ai fini dell'utilizzo dei sistemi interni di misurazione dei rischi per la determinazione dei requisiti patrimoniali si applicano le specifiche disposizioni organizzative previste nei Capitoli che disciplinano le varie tipologie di rischio rilevanti a fini prudenziali.

L'organo con funzione di supervisione strategica si assicura, inoltre, che le funzioni aziendali di controllo possiedano i requisiti previsti nella Sezione III; e che il sistema dei controlli interni e l'organizzazione aziendale siano costantemente uniformate ai principi indicati nella Sezione I. In tale contesto, garantisce che il rispetto dei requisiti indicati nelle Sezione I e III e la completezza, funzionalità e adeguatezza del sistema dei controlli interni siano periodicamente verificati e i risultati di tali verifiche siano portati a conoscenza del medesimo organo con funzione di supervisione strategica. Nel caso emergano carenze o anomalie, promuove con tempestività l'adozione di idonee misure correttive e ne verifica l'efficacia.

Si indicano, infine, i compiti dell'organo con funzione di supervisione strategica con riguardo a taluni profili specifici:

– con riferimento al processo ICAAP, definisce e approva le linee generali del processo, ne assicura la coerenza con le politiche di appetito al rischio e l'adeguamento tempestivo in relazione a modifiche significative delle linee strategiche, dell'assetto organizzativo, del contesto operativo di riferimento, promuove il pieno utilizzo delle risultanze dell'ICAAP a fini strategici e nelle decisioni d'impresa;

– riguardo ai rischi di credito e di controparte, approva le linee generali del sistema di gestione delle tecniche di attenuazione del rischio che presiede all'intero processo di acquisizione, valutazione, controllo e realizzo degli strumenti di attenuazione del rischio utilizzati.

Nel caso di banche che adottano sistemi interni di misurazione dei rischi per la determinazione dei requisiti patrimoniali, l'organo con funzione di supervisione strategica svolge anche i seguenti compiti ([9]):

- approva l'adozione dei suddetti sistemi. In particolare, approva la scelta del sistema ritenuto idoneo e il relativo progetto in cui sono pianificate le attività connesse con la sua predisposizione e messa in opera, individuate le responsabilità, definiti i tempi di realizzazione, determinati gli investimenti previsti in termini di risorse umane, finanziarie e tecnologiche;
- verifica periodicamente che le scelte effettuate mantengano nel tempo la loro validità, approvando i cambiamenti sostanziali al sistema e provvedendo alla complessiva supervisione sul corretto funzionamento dello stesso;
- vigila, con il supporto delle competenti funzioni, sull'effettivo utilizzo dei sistemi interni a fini gestionali (*use test*) e sulla loro rispondenza agli altri requisiti previsti dalla normativa;
- con cadenza almeno annuale, esamina i riferimenti forniti dalla funzione di convalida e assume, col parere dell'organo con funzione di controllo, formale delibera con la quale attesta il rispetto dei requisiti previsti per l'utilizzo dei sistemi.

3. Organo con funzione di gestione

L'organo con funzione di gestione deve avere la comprensione di tutti i rischi aziendali, inclusi i possibili rischi di malfunzionamento dei sistemi interni di misurazione (c.d. "rischio di modello"), e, nell'ambito di una gestione integrata, delle loro interrelazioni

([9]) I compiti dell'organo con funzione di supervisione strategica relativi all'impiego da parte delle banche di sistemi interni di misurazione dei rischi per la determinazione dei requisiti patrimoniali, disciplinati nel presente paragrafo, potrebbero essere stralciati dalle disposizioni definitive tenuto conto della disciplina che sarà contenuta nel Regolamento comunitario sui requisiti prudenziali degli enti creditizi e delle imprese di investimento.

reciproche e con l'evoluzione del contesto esterno. In tale ambito, deve essere in grado di individuare e valutare i fattori, inclusa la complessità della struttura organizzativa, da cui possono scaturire rischi per la banca.

Tale organo, in attuazione degli indirizzi strategici e delle politiche di governo dei rischi definite dall'organo con funzione di supervisione strategica:

– è responsabile per l'adozione di tutti gli interventi necessari ad assicurare l'aderenza dell'organizzazione e del sistema dei controlli interni ai requisiti di cui alle Sezioni I e III;

  in tale contesto:

  a) coerentemente con le politiche di governo dei rischi, definisce il processo di gestione dei rischi. In particolare, stabilisce limiti operativi all'assunzione delle varie tipologie di rischio, coerenti con il livello di rischio accettato e tenendo esplicitamente conto dei risultati delle prove di stress e dell'evoluzione del quadro economico. Inoltre, nell'ambito della gestione dei rischi, limita l'affidamento sui rating esterni, assicurando che, per ciascuna tipologia di rischio, siano condotte adeguate e autonome analisi interne;

  b) nella definizione del processo di gestione dei rischi, agevola lo sviluppo e la diffusione a tutti i livelli di una cultura del rischio integrata in relazione alle diverse tipologie di rischi (di credito, di mercato, operativi, di liquidità, di concentrazione, di reputazione, di conformità, strategico, di modello ecc.) ed estesa a tutta la banca. In particolare, devono essere sviluppati e attuati programmi di formazione per sensibilizzare i dipendenti in merito alle responsabilità in materia di rischi in modo da non confinare il processo di gestione del rischio agli specialisti o alle funzioni di controllo;

  c) stabilisce le responsabilità delle strutture e delle funzioni aziendali coinvolte nel processo di gestione dei rischi, in modo che siano chiaramente attribuiti i relativi compiti e siano prevenuti potenziali conflitti d'interessi; 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;

  d) esamina le operazioni di maggior rilievo oggetto di parere negativo da parte della funzione di controllo dei rischi e, se del caso, le autorizza (cfr. Sezione III, par. 3.3.); di tali operazioni informa l'organo con funzione di supervisione strategica e l'organo con funzione di controllo;

  e) 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;

  f) pone in essere le iniziative e gli interventi necessari per garantire nel continuo la complessiva affidabilità del sistema dei controlli interni e porta i risultati delle verifiche effettuate a conoscenza dell'organo con funzione di supervisione strategica. Attua i necessari interventi correttivi o di adeguamento nel caso emergano carenze o anomalie, o a seguito dell'introduzione di nuovi prodotti, attività, servizi o processi rilevanti;

– definisce il processo (responsabili, procedure, condizioni) per approvare gli investimenti in nuovi prodotti, la distribuzione di nuovi prodotti o servizi ovvero l'avvio di nuove attività o l'ingresso in nuovi mercati. Il processo deve: a) assicurare che vengano pienamente valutati i rischi derivanti dalla nuova operatività, che detti

rischi siano coerenti con il livello di rischio accettato e che la banca sia in grado di gestirli; b) definire le fasce di clientela a cui si intendono distribuire nuovi prodotti o servizi in relazione alla complessità degli stessi e ad eventuali vincoli normativi esistenti; c) stimare gli impatti della nuova operatività in termini di costi e ricavi nonché di risorse umane, organizzative e informatiche; d) individuare le eventuali modifiche da apportare al sistema dei controlli interni.

- definisce e attua la politica aziendale in materia di esternalizzazione di funzioni aziendali (cfr. Sezione IV)
- assicura:
  a) la coerenza tra il livello di rischio accettato, la pianificazione aziendale, le politiche di governo dei rischi e il processo di gestione dei rischi avuta anche presente l'evoluzione delle condizioni interne ed esterne in cui opera la banca;
  b) l'adeguatezza delle funzioni aziendali di controllo;
  c) il corretto funzionamento dei processi e delle metodologie di valutazione delle attività aziendali, compresi gli strumenti finanziari, e promuove il loro costante aggiornamento;
  d) una corretta, tempestiva e sicura gestione delle informazioni a fini contabili, gestionali e di reporting.

Si indicano, infine, i compiti dell'organo con funzione di gestione con riguardo a taluni profili specifici:

- con riferimento al processo ICAAP, dà attuazione a tale processo curando che lo stesso sia rispondente agli indirizzi strategici e che soddisfi i seguenti requisiti: consideri tutti i rischi rilevanti; incorpori valutazioni prospettiche; utilizzi appropriate metodologie; sia conosciuto e condiviso dalle strutture interne; sia adeguatamente formalizzato e documentato; individui i ruoli e le responsabilità assegnate alle funzioni e alle strutture aziendali; sia affidato a risorse competenti, sufficienti sotto il profilo quantitativo, collocate in posizione gerarchica adeguata a far rispettare la pianificazione; sia parte integrante dell'attività gestionale;
- con specifico riferimento ai rischi di credito e di controparte, in linea con gli indirizzi strategici, approva specifiche linee guida volte ad assicurare l'efficacia del sistema di gestione delle tecniche di attenuazione del rischio e a garantire il rispetto dei requisiti generali e specifici di tali tecniche.

Nel caso di banche che adottano sistemi interni di misurazione dei rischi per la determinazione dei requisiti patrimoniali, l'organo con funzione di gestione svolge anche i seguenti compiti ([10]):

- è responsabile dell'impianto e del funzionamento del sistema prescelto; per svolgere tale compito i componenti dell'organo possiedono un'adeguata conoscenza degli aspetti rilevanti;
- impartisce le disposizioni necessarie affinché il sistema prescelto sia realizzato secondo le linee strategiche individuate, assegnando compiti e responsabilità alle

([10]) I compiti dell'organo con funzione di gestione relativi all'impiego da parte delle banche di sistemi interni di misurazione dei rischi per la determinazione dei requisiti patrimoniali, disciplinati nel presente paragrafo, potrebbero essere stralciati dalle disposizioni definitive tenuto conto della disciplina che sarà contenuta nel Regolamento comunitario sui requisiti prudenziali degli enti creditizi e delle imprese di investimento .

diverse funzioni aziendali e assicurando la formalizzazione e la documentazione delle fasi del processo di gestione del rischio;

- cura che i sistemi di misurazione dei rischi siano integrati nei processi decisionali e nella gestione dell'operatività aziendale (*use test*);
- tiene conto, nello svolgimento dei compiti assegnati, delle osservazioni emerse a seguito del processo di convalida e delle verifiche condotte dalla revisione interna.

4. Organo con funzione di controllo

L'organo con funzione di controllo ha la responsabilità di vigilare sulla completezza, funzionalità e adeguatezza del sistema dei controlli interni.

Nell'espletamento di tale compito, l'organo con funzione di controllo vigila sul rispetto delle previsioni di cui alla presente Sezione, di quelle di cui alle Sezioni I e III e di quelle che presiedono all'ICAAP. Per lo svolgimento delle proprie attribuzioni, tale organo dispone di adeguati flussi informativi da parte degli altri organi aziendali e delle funzioni di controllo interno.

L'organo con funzione di controllo svolge altresì le funzioni dell'organismo di vigilanza - previsto ai sensi della legge n. 231/2001, in materia di responsabilità amministrativa degli enti - che vigila sul funzionamento e l'osservanza dei modelli di organizzazione e di gestione di cui si dota la banca per prevenire i reati rilevanti ai fini della medesima legge ([11]). Ove vi siano particolari e motivate esigenze, le banche possono affidare tali funzioni a un organismo appositamente istituito.

Considerata la pluralità di funzioni aventi, all'interno dell'azienda, compiti e responsabilità di controllo, l'organo con funzione di controllo è tenuto ad accertare l'adeguatezza di tutte le funzioni coinvolte nel sistema dei controlli, il corretto assolvimento dei compiti e l'adeguato coordinamento delle medesime, promuovendo gli interventi correttivi delle carenze e delle irregolarità rilevate ([12]).

Nelle banche che adottano sistemi interni di misurazione dei rischi per la determinazione dei requisiti patrimoniali, l'organo con funzione di controllo, avvalendosi dell'apporto delle funzioni aziendali di controllo, valuta – nell'ambito della più generale attività di verifica del processo di gestione dei rischi – la funzionalità e adeguatezza dei sistemi stessi e la loro rispondenza ai requisiti previsti dalla normativa.

5. Il coordinamento delle funzioni di controllo (interne e societarie)

Il corretto funzionamento del sistema dei controlli interni si basa sulla proficua interazione nell'esercizio dei compiti (d'indirizzo, di attuazione, di verifica, di valutazione) fra gli organi aziendali, gli eventuali comitati costituiti all'interno di questi ultimi ([13]), i

([11]) In particolare, i citati modelli organizzativi e di gestione sono volti a: i) individuare le attività nel cui ambito possono essere commessi reati; ii) prevedere specifici protocolli diretti a programmare la formazione e l'attuazione delle decisioni dell'ente in relazione ai reati da prevenire; iii) individuare modalità di gestione delle risorse finanziarie idonee a impedire la commissione dei reati; iv) prevedere obblighi di informazione nei confronti dell'organismo di vigilanza; v) definire un sistema sanzionatorio per il mancato rispetto delle misure indicate nel citato modello.

([12]) Cfr. "Disposizioni di vigilanza in materia di organizzazione e governo societario delle banche" del 4 marzo 2008 e le relative linee applicative dell'11 gennaio 2012, cui si rimanda per la descrizione dettagliata dei compiti e poteri dell'organo con funzione di controllo.

([13]) Cfr. "Disposizioni di vigilanza in materia di organizzazione e governo societario delle banche" del 4 marzo 2008 e le relativa linee applicative dell'11 gennaio 2012, cui si rimanda per la descrizione dettagliata dei compiti e poteri dell'organo con funzione di controllo.

soggetti incaricati della revisione legale dei conti, le funzioni aziendali di controllo (*compliance*, *risk management*, *internal audit*).

L'ordinamento e le fonti di autoregolamentazione attribuiscono, poi, compiti di controllo a specifiche funzioni societarie di controllo o a comitati interni all'organo amministrativo, la cui attività va inquadrata in modo coerente nel sistema dei controlli interni.

In particolare, rilevano:

– l'organismo di vigilanza eventualmente istituito ai sensi della legge n. 231/2001;

– per le banche con azioni quotate, il dirigente preposto alla redazione dei documenti contabili societari (art. 154-*bis* del TUF), il quale, tra l'altro, ha il compito di stabilire adeguate procedure amministrative e contabili per la predisposizione del bilancio e di ogni altra comunicazione di carattere finanziario.

Inoltre, il Codice di autodisciplina della Borsa Italiana, a cui le banche quotate possono aderire su base volontaria, introduce principi e criteri applicativi riguardo al sistema di controllo interno e di gestione dei rischi, che prevedono, tra l'altro, la designazione di uno o più amministratori incaricati del sistema di controllo interno e di gestione dei rischi e l'istituzione, in seno all'organo amministrativo di un comitato controllo e rischi, composto da amministratori non esecutivi, in maggioranza indipendenti.

Per assicurare una corretta interazione tra tutte le funzioni e organi con compiti di controllo, evitando sovrapposizioni o lacune, l'organo con funzione di supervisione strategica approva un documento nel quale sono definiti i compiti e le responsabilità dei vari organi e funzioni (aziendali e societarie) di controllo, i flussi informativi tra le diverse funzioni/organi e tra queste/i e gli organi aziendali e, nel caso in cui gli ambiti di controllo presentino aree di potenziale sovrapposizione o permettano di sviluppare sinergie, le modalità di coordinamento e di collaborazione. A titolo esemplificativo, nell'attività dell'organismo di vigilanza, che attiene in generale all'adempimento di leggi e regolamenti, può essere proficuo uno stretto raccordo, in termini sia di suddivisione di attività che di condivisione di informazioni, con le funzioni di conformità alle norme e di revisione interna.

Nel definire le modalità di raccordo, ferme restando le attribuzioni previste dalla legge per le funzioni societarie di controllo, le banche prestano attenzione a non alterare, anche nella sostanza, le responsabilità primarie degli organi aziendali sul sistema dei controlli interni.

Sezione III
Funzioni aziendali di controllo

1. Istituzione delle funzioni aziendali di controllo

Ferma restando l'autonoma responsabilità aziendale per le scelte effettuate in materia di assetto dei controlli interni, le banche istituiscono, secondo quanto di seguito indicato, funzioni aziendali di controllo permanenti e indipendenti: i) di conformità alle norme (*compliance*); ii) di controllo dei rischi (*risk management function*); iii) di revisione interna (*internal audit*).

Le prime due funzioni attengono ai controlli di secondo livello, la revisione interna ai controlli di terzo livello.

Per assicurare l'indipendenza delle funzioni aziendali di controllo è necessario che:

a) tali funzioni dispongano dell'autorità, delle risorse e delle competenze necessarie per lo svolgimento dei loro compiti. Alle funzioni deve essere consentito di avere accesso ai dati aziendali e a quelli esterni necessari per svolgere in modo appropriato i propri compiti. Le risorse economiche, eventualmente attivabili in autonomia, devono, tra l'altro, permettere alle funzioni aziendali di controllo di ricorrere a consulenze esterne. Il personale deve essere adeguato per numero, competenze tecnico-professionali, aggiornamento, anche attraverso l'inserimento di programmi di formazione nel continuo. Al fine di garantire la formazione di competenze trasversali e di acquisire una visione complessiva e integrata dell'attività di controllo svolta dalla funzione, la banca incentiva, all'interno delle singole funzioni di controllo, programmi di rotazione delle risorse;

b) i responsabili:

   - possiedano requisiti di professionalità e siano collocati in posizione gerarchico - funzionale adeguata;
   - non abbiano responsabilità diretta di aree operative sottoposte a controllo né siano gerarchicamente subordinati ai responsabili di tali aree;
   - siano nominati e revocati (motivandone le ragioni) dall'organo con funzione di gestione, d'accordo con l'organo con funzione di supervisione strategica, sentito l'organo con funzione di controllo. Il responsabile di funzioni aziendali di controllo può essere un componente dell'organo amministrativo, purché non sia destinatario di altre deleghe operative. Per effetto dell'incarico di responsabile di una funzione di controllo l'amministratore è qualificato come amministratore esecutivo;
   - riferiscano direttamente agli organi aziendali.

c) il personale che partecipa alle funzioni aziendali di controllo non sia coinvolto in attività che tali funzioni sono chiamate a controllare. Nel rispetto di tale principio, nelle banche di dimensioni contenute o caratterizzate da una limitata complessità operativa, il personale incaricato di compiti attinenti al controllo di conformità alle norme o al controllo dei rischi, qualora non sia inserito nelle relative funzioni aziendali di controllo, può essere integrato in aree operative diverse; in questi casi, tale personale riferisce direttamente ai responsabili delle funzioni aziendali di controllo per le questioni attinenti ai compiti di tali funzioni;

d) le funzioni aziendali di controllo siano tra loro separate, sotto un profilo organizzativo. I rispettivi ruoli e responsabilità devono essere formalizzati;

e) i criteri di remunerazione del personale che partecipa alle funzioni aziendali di controllo non ne compromettano l'obiettività e concorrano a creare un sistema di incentivi coerente con le finalità della funzione svolta ([18]).

Se coerente con il principio di proporzionalità, le banche possono, a condizione che i controlli sulle diverse tipologie di rischio continuino ad essere efficaci:

- affidare lo svolgimento della funzione di conformità alle norme alle strutture incaricate della funzione di controllo dei rischi;
- affidare lo svolgimento delle funzioni aziendali di controllo all'esterno, secondo quanto previsto dalle disposizioni in materia di esternalizzazione previste nella Sezione IV, a soggetti terzi dotati di requisiti idonei in termini di professionalità e indipendenza. Le banche che ricorrono a tale facoltà nominano un referente interno per il soggetto incaricato di svolgere la funzione e quale incaricato della complessiva supervisione della specifica attività di controllo esternalizzata, posto che la responsabilità finale resta in capo alla banca.

Tenuto conto che l'adeguatezza ed efficacia delle funzioni di conformità alle norme e di controllo dei rischi devono essere sottoposte a verifica periodica da parte della funzione di revisione interna (controllo di terzo livello), per assicurare l'imparzialità delle verifiche, le funzioni di conformità alle norme e di gestione dei rischi non possono essere affidate alla funzione di revisione interna.

Box 3

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

Si sollecitano commenti per declinare nel concreto 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.

2. Programmazione e rendicontazione dell'attività di controllo

Per ciascuna funzione aziendale di controllo, la regolamentazione interna indica responsabilità, compiti, modalità operative, flussi informativi, programmazione dell'attività di controllo.

In particolare:

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

– la funzione di revisione interna presenta annualmente agli organi aziendali un piano di *audit*, che indica le attività di controllo pianificate, tenuto conto dei rischi delle

([18]) Cfr. "Disposizioni in materia di politiche e prassi di remunerazione e incentivazione nelle banche e nei gruppi bancari" del 30 marzo 2011.

varie attività e strutture aziendali; il piano contiene una specifica sezione relativa all'attività di revisione del sistema informativo (*ICT auditing*).

Al termine del ciclo gestionale, con cadenza quindi annuale, le funzioni aziendali di controllo:

- presentano agli organi aziendali una relazione dell'attività svolta, che illustra le verifiche effettuate, i risultati emersi, i punti di debolezza rilevati e propongono gli interventi da adottare per la loro rimozione;
- riferiscono, ciascuna per gli aspetti di rispettiva competenza, in ordine alla completezza, adeguatezza ed affidabilità del sistema dei controlli interni.

In ogni caso, le funzioni aziendali di controllo informano tempestivamente gli organi aziendali su ogni violazione o carenza rilevanti riscontrate (es. violazioni che possono comportare un alto rischio di sanzioni regolamentari o legali, perdite finanziarie di rilievo o significativi impatti sulla situazione finanziaria o patrimoniale, danni di reputazione, malfunzionamenti di procedure informatiche critiche).

3. Requisiti specifici delle funzioni aziendali di controllo

3.1 Premessa

Nei paragrafi seguenti si stabiliscono le responsabilità ed i principali compiti attribuibili, in via generale, a ciascuna delle funzioni aziendali di controllo ([19]).

Indicazioni più specifiche concernenti le responsabilità ed i compiti di tali funzioni relativamente a ciascuna singola categoria di rischio, ambiti operativi o attività particolari sono riportate nelle relative discipline (cfr. Sezione I, par. 1).

3.2 Funzione di conformità alle norme (compliance)

Il rischio di non conformità alle norme è il rischio di incorrere in sanzioni giudiziarie o amministrative, perdite finanziarie rilevanti o danni di reputazione in conseguenza di violazioni di norme imperative (leggi, regolamenti) ovvero di autoregolamentazione (es. statuti, codici di condotta, codici di autodisciplina).

Poiché il rischio di non conformità alle norme è diffuso a tutti livelli dell'organizzazione aziendale, soprattutto nell'ambito delle linee operative, l'attività di prevenzione deve svolgersi in primo luogo dove il rischio viene generato: è pertanto necessaria un'adeguata responsabilizzazione di tutto il personale.

In via generale, le norme più rilevanti ai fini del rischio di non conformità sono quelle che riguardano l'esercizio dell'attività bancaria e di intermediazione, la gestione dei conflitti di interesse, la trasparenza nei confronti della clientela e, più in generale, la disciplina posta a tutela del consumatore. Tuttavia, la funzione presiede alla gestione del rischio di non conformità alle norme, con riguardo a tutta l'attività aziendale.

Particolare attenzione deve essere posta anche nella verifica della conformità dell'attività aziendale alle normative di natura fiscale ([20]), al fine di evitare di incorrere in violazioni o elusioni di tale normativa ovvero in situazioni di abuso del diritto, che possono

([19]) Con esclusivo riferimento alla prestazione di servizi di investimento, si applica il riparto di competenze tra la funzione di conformità alle norme e la funzione di revisione interna previsto dalla Comunicazione congiunta Banca d'Italia – Consob dell'8 marzo 2011.

([20]) Le banche devono altresì tener conto dei rischi derivanti dal coinvolgimento in operazioni fiscalmente irregolari poste in essere dalla clientela.

determinare ripercussioni significative in termini di rischi operativi e di reputazione e conseguenti danni patrimoniali.

La funzione di conformità alle norme ha il compito di verificare che le procedure interne siano coerenti con l'obiettivo di prevenire la violazione di norme esterne (leggi e regolamenti) e di autoregolamentazione (codici di condotta, codici etici) applicabili alla banca.

I principali adempimenti che la funzione di conformità alle norme è chiamata a svolgere sono:

– l'ausilio alle strutture aziendali per la definizione delle metodologie di valutazione dei rischi di non conformità alle norme;

– l'individuazione di idonee procedure per la prevenzione del rischio rilevato con possibilità di richiederne l'adozione;

– l'identificazione nel continuo delle norme applicabili alla banca e la misurazione/valutazione del loro impatto su processi e procedure aziendali;

– la proposta di modifiche organizzative e procedurali finalizzate ad assicurare un adeguato presidio dei rischi di non conformità identificati;

– la predisposizione di flussi informativi diretti agli organi aziendali e alle strutture coinvolte (es.: gestione del rischio operativo e revisione interna);

– la verifica dell'efficacia degli adeguamenti organizzativi (strutture, processi, procedure anche operative e commerciali) suggeriti per la prevenzione del rischio di non conformità alle norme.

La funzione di conformità alle norme deve essere coinvolta nella valutazione *ex ante* della conformità alla regolamentazione applicabile di tutti i progetti innovativi (inclusa l'operatività in nuovi prodotti o servizi) che la banca intenda intraprendere nonché nella prevenzione e nella gestione dei conflitti di interesse sia tra le diverse attività svolte dalla banca, sia con riferimento ai dipendenti e agli esponenti aziendali.

Altre aree di intervento della funzione di conformità alle norme sono:

- la verifica della coerenza del sistema premiante aziendale (in particolare retribuzione e incentivazione del personale) con gli obiettivi di rispetto delle norme, dello statuto nonché di eventuali codici etici o altri standard di condotta applicabili alla banca;

- la consulenza e assistenza nei confronti degli organi aziendali della banca in tutte le materie in cui assume rilievo il rischio di non conformità nonché la collaborazione nell'attività di formazione del personale sulle disposizioni applicabili alle attività svolte, al fine di diffondere una cultura aziendale improntata ai principi di onestà, correttezza e rispetto dello spirito e della lettera delle norme.

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

Per svolgere efficacemente i propri compiti, è necessario che la funzione di conformità alle norme abbia accesso a tutte le attività della banca, centrali e periferiche, ed a qualsiasi informazione a tal fine rilevante, anche attraverso il colloquio diretto con il personale.

3.3 Funzione di controllo dei rischi (risk management function)

La funzione di controllo dei rischi ha la finalità di attuare le politiche di governo dei rischi, attraverso un adeguato processo di gestione dei rischi ([21]). Al fine di rafforzarne l'indipendenza, il responsabile della funzione può essere collocato alle dirette dipendenze del comitato controllo e rischi, ove costituito, o dell'organo con funzione di supervisione strategica ([22]).

La funzione di controllo dei rischi deve essere organizzata in modo da perseguire in maniera efficiente ed efficace tale obiettivo. Essa può essere variamente articolata, ad esempio in relazione ai singoli profili di rischio (di credito, di mercato, operativo, modello ecc.), purché la banca mantenga una visione d'insieme dei diversi rischi e della loro reciproca interazione. Le banche che adottano sistemi interni per la misurazione dei rischi, se coerente con la natura, la dimensione e la complessità dell'attività svolta, individuano all'interno della funzione di controllo dei rischi unità preposte alla convalida di detti sistemi indipendenti dalle unità responsabili dello sviluppo degli stessi.

Specie nelle banche più complesse, può essere prevista la costituzione di specifici comitati di gestione dei diversi profili di rischio (ad es. comitati per i rischi di credito e operativi, comitato di liquidità, comitato finanza, comitato per l'*asset and liability management*), definendo in modo chiaro le diverse responsabilità e le modalità di intervento e di partecipazione della funzione, in modo da garantirne la completa indipendenza dal processo di assunzione dei rischi; va inoltre evitato che l'istituzione di tali comitati possa depotenziare le prerogative della funzione di controllo dei rischi.

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

La funzione di controllo dei rischi:

- è coinvolta nella definizione del livello di rischio accettato e nell'elaborazione delle politiche 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;
- verifica nel continuo l'adeguatezza di tali politiche, processo e limiti;
- fermo restando quanto previsto nell'ambito della disciplina dei sistemi interni per il calcolo dei requisiti patrimoniali, è responsabile dello sviluppo, della convalida e del mantenimento dei sistemi di misurazione e controllo dei rischi assicurando che siano sottoposti a *backtesting* periodici, che vengano analizzati un appropriato numero di scenari e che siano utilizzate ipotesi conservative sulle dipendenze e sulle correlazioni; nella misurazione dei rischi tiene conto in generale del rischio di modello e dell'eventuale incertezza nella valutazione di alcune tipologie di strumenti finanziari e informa di queste incertezze l'organo con funzione di gestione;
- sviluppa e applica indicatori in grado di evidenziare situazioni di anomalia e di inefficienza dei sistemi di misurazione e controllo dei rischi;

([21]) La funzione di controllo dei rischi (*risk management function*) va tenuta distinta e indipendente dalle funzioni aziendali incaricate della "gestione operativa" dei rischi, che incidono sull'assunzione dei rischi da parte delle unità di business e modificano il profilo di rischio della banca.

([22]) Le banche classificate, a fini SREP, nelle macro-categorie 1 e 2 (cfr. Circolare 269 del 7 maggio 2008, "Guida per l'attività di vigilanza", Sezione I, Capitolo I.5) collocano obbligatoriamente la funzione di controllo dei rischi alle dirette dipendenze del comitato controllo e rischi, ove costituito, o dell'organo con funzione di supervisione strategica.

- analizza i rischi dei nuovi i prodotti e servizi e di quelli derivanti dall'ingresso in nuovi segmenti operativi e di mercato;
- dà pareri preventivi sulla coerenza con la politica di governo dei rischi delle operazioni di maggiore rilievo;
- monitora costantemente l'evoluzione dei rischi aziendali e il rispetto dei limiti operativi all'assunzione delle varie tipologie di rischio;
- verifica l'adeguatezza e l'efficacia delle misure prese per rimediare alle carenze riscontrate nel processo di gestione del rischio.

3.4 Funzione di revisione interna (internal audit)

La funzione di revisione interna è volta, da un lato, a controllare, in un'ottica di controlli di terzo livello, anche con verifiche in loco, il regolare andamento dell'operatività e l'evoluzione dei rischi, e, dall'altro, a valutare la completezza, funzionalità ed adeguatezza della struttura organizzativa e delle altre componenti del sistema dei controlli interni, portando all'attenzione degli organi aziendali i possibili miglioramenti, con particolare riferimento alle politiche di governo dei rischi, al processo di gestione dei rischi nonché agli strumenti di misurazione e controllo degli stessi. Sulla base dei risultati dei propri controlli formula raccomandazioni agli organi aziendali.

In tale ambito, coerentemente con il piano di *audit*, la funzione di revisione interna:

- valuta l'adeguatezza, in termini di efficacia ed efficienza, completezza ed affidabilità delle altre componenti del sistema dei controlli interni, avendo riguardo anche alla capacità di individuare errori ed irregolarità. In tale contesto, sottopone a verifica le funzioni aziendali di controllo dei rischi e di conformità alle norme;
- valuta la conformità dell'operatività aziendale al livello di tolleranza al rischio/appetito per il rischio approvato dall'organo con funzione di supervisione strategica e, in caso di strutture finanziarie particolarmente complesse, la conformità di queste alle strategie approvate dagli organi aziendali;
- verifica, anche attraverso accertamenti di natura ispettiva:
  a) la regolarità delle diverse attività aziendali, incluse quelle esternalizzate, e l'evoluzione dei rischi sia nella direzione generale della banca, sia nelle filiali. La frequenza delle ispezioni deve essere coerente con l'attività svolta;
  b) il rispetto delle norme da parte di tutti i livelli aziendali;
  c) il rispetto, nei diversi settori operativi, dei limiti previsti dai meccanismi di delega, e il pieno e corretto utilizzo delle informazioni disponibili nelle diverse attività;
  d) l'efficacia dei poteri della funzione di controllo dei rischi di fornire pareri preventivi sulla coerenza con la politica di governo dei rischi delle operazioni di maggior rilievo;
  e) l'adeguatezza e il corretto funzionamento dei processi e delle metodologie di valutazione delle attività aziendali e, in particolare, degli strumenti finanziari;
  f) l'adeguatezza, l'affidabilità complessiva e la sicurezza del sistema informativo (*ICT audit*);
  g) la rimozione delle anomalie riscontrate nell'operatività e nel funzionamento dei controlli (attività di "*follow-up*");

- effettua test periodici sul funzionamento delle procedure operative e di controllo interno;
- espleta compiti d'accertamento anche con riguardo a specifiche irregolarità, ove richiesto dagli organi aziendali;
- controlla regolarmente il piano aziendale di continuità operativa. In tale ambito, prende visione dei programmi di verifica, assiste alle prove e ne controlla i risultati, propone modifiche al piano sulla base delle mancanze riscontrate. La funzione di revisione interna è coinvolta nel controllo dei piani di emergenza degli *outsourcer* e dei fornitori critici; essa può decidere di fare affidamento sulle strutture di questi ultimi se ritenute professionali e indipendenti quanto ai risultati dei controlli ed esamina i contratti per accertare che il livello di tutela sia adeguato agli obiettivi e agli standard aziendali;
- nell'ambito della collaborazione e dello scambio di informazioni con il soggetto incaricato della revisione legale dei conti, individua le criticità emerse durante l'attività di revisione e si attiva affinché le competenti funzioni aziendali adottino i presidi necessari per superare tali criticità.

Con specifico riferimento al processo di gestione dei rischi, 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 alla'adeguatezza delle risorse a questa assegnate;
- l'adeguatezza del processo di gestione dei rischi;
- l'appropriatezza delle ipotesi utilizzate nelle analisi di scenario e negli stress test;
- l'allineamento con le *best practice* diffuse nel settore.

L'organizzazione della funzione di revisione interna deve essere coerente con l'articolazione ed il grado di complessità della banca. 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 ([23]). 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.

Indipendentemente dalle scelte organizzative, e fermo restando che i destinatari delle comunicazioni delle attività di verifica sono gli organi aziendali e le unità sottoposte a controllo, nella regolamentazione interna deve essere espressamene previsto il potere per la funzione di revisione interna di comunicare in via diretta i risultati degli accertamenti e delle valutazioni agli organi aziendali. Gli esiti degli accertamenti conclusisi con giudizi negativi o che evidenzino carenze di rilievo devono essere trasmessi integralmente, tempestivamente e direttamente agli organi aziendali.

Per svolgere adeguatamente i propri compiti, 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. In caso di attribuzione a soggetti terzi di attività rilevanti per il funzionamento del sistema dei controlli interni (ad esempio,

([23]) Le banche classificate, a fini SREP, nelle macro-categorie 1 e 2 (cfr. Circolare 269 del 7 maggio 2008, "Guida per l'attività di vigilanza", Sezione I, Capitolo I.5) collocano obbligatoriamente la funzione di revisione interna alle dirette dipendenze del comitato controllo e rischi, ove costituito, o dell'organo con funzione di supervisione strategica..

dell'attività di elaborazione dei dati), la funzione di revisione interna deve poter accedere anche alle attività svolte da tali soggetti.

3.5 Rapporti tra le funzioni aziendali di controllo e altre funzioni aziendali

Fermo restando la reciproca indipendenza e i rispettivi ruoli, le funzioni aziendali di controllo collaborano tra loro e con le altre funzioni (es. funzione legale, organizzazione, sicurezza informatica) allo scopo di sviluppare le proprie metodologie di controllo in modo coerente con le strategie e l'operatività aziendale.

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

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

Sezione IV
Esternalizzazione di funzioni aziendali (*outsourcing*)

1. Principi generali e requisiti particolari

Le banche che ricorrono all'esternalizzazione di funzioni aziendali devono presidiare i rischi derivanti dalle scelte effettuate, mantenendo la capacità di controllo e la responsabilità sulle attività esternalizzate nonché le competenze tecniche e gestionali essenziali per re-internalizzare, in caso di necessità, il loro svolgimento.

La decisione di ricorrere all'*outsourcing* per lo svolgimento di determinate funzioni aziendali (anche non importanti) deve essere coerente con la politica aziendale in materia di esternalizzazione.

In linea con il principio di proporzionalità, tale politica stabilisce almeno:

- il processo decisionale per esternalizzare funzioni aziendali (livelli decisionali; funzioni coinvolte; valutazione dei rischi, inclusi quelli connessi con potenziali conflitti di interesse dell'*outsourcer*, e l'impatto sulle funzioni aziendali; criteri per la scelta e la *due diligence* del fornitore);
- il contenuto minimo dei contratti di *outsourcing* e i livelli di servizio attesi delle attività esternalizzate;
- le modalità di controllo, nel continuo e con il coinvolgimento della funzione di revisione interna, delle funzioni esternalizzate;
- 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 relativi alle funzioni esternalizzate;
- i piani di emergenza (clausole contrattuali, piani operativi, ecc.) in caso di non corretto svolgimento delle funzioni esternalizzate da parte dell'*outsourcer*.

La banca, attraverso il ricorso all'esternalizzazione, non può:

– delegare le proprie responsabilità, né la responsabilità degli organi aziendali. In linea con questo principio, a titolo esemplificativo, non è ammessa l'esternalizzazione di attività che rientrano tra i compiti degli organi aziendali (cfr. Sezione II) o che riguardano aspetti nevralgici del processo di erogazione del credito (ad es. il processo di valutazione del merito di credito e di monitoraggio delle relazioni creditizie) nonché, per le banche di maggiori dimensioni e complessità, quella delle funzioni aziendali di controllo ([24]);

– alterare il rapporto e gli obblighi nei confronti dei suoi clienti;

– mettere a repentaglio la propria capacità di rispettare gli obblighi previsti dalla disciplina di vigilanza né mettersi in condizione di violare le riserve di attività previste dalla legge;

– pregiudicare la qualità del sistema dei controlli interni;

– ostacolare la vigilanza.

Ferma restando l'esigenza di assicurare, per ogni tipologia di esternalizzazione, il corretto svolgimento della stessa da parte del fornitore, il buon funzionamento del sistema dei controlli interni e il monitoraggio continuo dell'attività svolta dall'*outsourcer*, nel caso

([24]) E' ammessa l'esternalizzazione di tali funzioni all'interno del gruppo bancario (cfr. Sezione V).

in cui intendano esternalizzare funzioni operative importanti le banche assicurano che siano soddisfatte le seguenti condizioni:

– nell'accordo scritto tra la banca e l'*outsourcer* sono formalizzati e chiaramente definiti:

  a) i rispettivi diritti e obblighi; i livelli di servizio attesi, espressi in termini oggettivi e misurabili, nonché le informazioni necessarie per la verifica del loro rispetto; gli eventuali conflitti di interesse e le opportune cautele per prevenirli e attenuarli; le condizioni al verificarsi delle quali possono essere apportate modifiche all'accordo; la durata dell'accordo e le modalità di rinnovo nonché gli impegni reciproci connessi con l'interruzione del rapporto;

  b) i livelli di servizio assicurati in caso di emergenza e le soluzioni di continuità compatibili con le esigenze aziendali e coerenti con le prescrizioni dell'Autorità di vigilanza. Sono altresì stabilite le modalità di partecipazione, diretta o per il tramite di comitati utente, alle verifiche dei piani di emergenza dei fornitori.

  Sono inoltre previste clausole risolutive espresse che consentano alla banca di porre termine all'accordo di esternalizzazione in presenza di eventi che possano compromettere la capacità del fornitore di garantire il servizio oppure quando si verifichi il mancato rispetto del livello di servizio concordato;

– il fornitore di servizi:

  a) dispone della competenza, della capacità e delle autorizzazioni richieste dalla legge per esercitare, in maniera professionale e affidabile, le funzioni esternalizzate;

  b) informa la banca di qualsiasi evento che potrebbe incidere sulla sua capacità di svolgere le funzioni esternalizzate in maniera efficace e in conformità con la normativa vigente; in particolare, comunica tempestivamente il verificarsi di incidenti di sicurezza, anche al fine di consentire la pronta attivazione delle relative procedure di gestione o di emergenza;

  c) garantisce la sicurezza delle informazioni relative all'attività della banca, sotto l'aspetto della disponibilità, integrità e riservatezza; in particolare assicura il rispetto delle norme sulla protezione dei dati personali.

– la banca:

  a) conserva la competenza richiesta per controllare efficacemente le funzioni esternalizzate e per gestire i rischi connessi con l'esternalizzazione, inclusi quelli derivanti da potenziali conflitti di interessi dell'*outsourcer*; in tale ambito, individua, all'interno della propria organizzazione, un responsabile del controllo delle singole funzioni esternalizzate dotato di adeguati requisiti di professionalità ("referente per le attività esternalizzate");

  b) acquisisce i piani di emergenza dell'*outsourcer* o dispone di informazioni adeguate, al fine di valutare la qualità delle misure previste e di integrarle con le soluzioni di continuità realizzate all'interno;

– la banca, i suoi soggetti incaricati della revisione legale dei conti e le Autorità di vigilanza hanno effettivo accesso ai dati relativi alle attività esternalizzate e ai locali in cui opera il fornitore di servizi. Il diritto di accesso per l'Autorità di vigilanza deve risultare espressamente nel contratto, senza oneri aggiuntivi per l'intermediario;

– la sub-esternalizzazione (ovverosia la possibilità del fornitore di esternalizzare a sua volta una parte delle attività oggetto del contratto di esternalizzazione) non deve mettere a repentaglio il rispetto dei principi e delle condizioni per l'esternalizzazione previste nella presente disciplina; a tal fine, il contratto con l'*outsourcer* prevede che eventuali rapporti di sub-esternalizzazione siano preventivamente concordati con la banca e siano definiti in modo da consentire il pieno rispetto di tutte le condizioni sopra elencate relative al contratto primario, inclusa la possibilità per l'Autorità di vigilanza di avere accesso ai dati relativi alle attività esternalizzate e ai locali in cui opera il sub-fornitore di servizi.

In aggiunta a quanto sopra previsto ed a quanto disciplinato nella Sezione III, le banche di dimensioni contenute o caratterizzate da una limitata complessità operativa che intendono affidare a soggetti terzi ([25]), in tutto o in parte, le funzioni aziendali di controllo definiscono nell'accordo di esternalizzazione:

– gli obiettivi, la metodologia e la frequenza dei controlli;

– le modalità e la frequenza della reportistica dovuta al referente per l'attività esternalizzata e agli organi aziendali sulle verifiche effettuate. Resta fermo l'obbligo di dare riscontro tempestivamente a qualsiasi richiesta di informazioni e consulenza da parte di questi ultimi che in ogni caso rimangono responsabili del corretto espletamento delle attività di controllo esternalizzate;

– gli obblighi di riservatezza delle informazioni acquisite nell'esercizio della funzione;

– i collegamenti con le attività svolte dall'organo con funzione di controllo;

– la possibilità di richiedere specifiche attività di controllo al verificarsi di esigenze improvvise;

– la proprietà esclusiva della banca dei risultati dei controlli.

Nel rispetto delle medesime condizioni, inoltre, le banche, se in linea con il principio di proporzionalità, possono esternalizzare specifici controlli, che richiedono conoscenze professionali specializzate, in aree operative di contenute dimensioni e/o rischiosità.

Le banche che intendono esternalizzare, in tutto o in parte, lo svolgimento di funzioni operative importanti o di controllo sono tenute a informare preventivamente la Banca d'Italia, fornendo tutte le indicazioni utili a verificare il rispetto dei criteri sopra indicati. Nel caso di esternalizzazioni presso soggetti con sede in altri paesi la comunicazione alla Banca d'Italia deve essere effettuata almeno 30 giorni prima di conferire l'incarico, specificando le esigenze aziendali che hanno determinato la scelta. Entro 30 giorni dal ricevimento della comunicazione la Banca d'Italia può avviare un procedimento amministrativo d'ufficio di divieto dell'esternalizzazione che si conclude entro 60 giorni.

Qualora l'esternalizzazione riguardi sistemi informativi critici e, in genere, sistemi a supporto dell'operatività caratteristica dell'intermediario, si applicano anche le disposizioni di cui al Capitolo 8, Sezione VI, par. 2.

Entro il 30 aprile di ogni anno le banche trasmettono alla Banca d'Italia una relazione, redatta dalla funzione di revisione interna - o, se esternalizzata, dal referente aziendale - con le considerazioni dell'organo con funzione di controllo e approvata dall'organo con funzione di supervisione strategica, relativa ai controlli svolti sulle funzioni

([25]) Per soggetti terzi si intendono altre banche, società di revisione, ovvero gli organismi associativi di categoria (ad es. Federazioni regionali delle banche di credito cooperativo).

operative importanti esternalizzate, alle carenze eventualmente riscontrate e alle conseguenti azioni correttive adottate.

2. Esternalizzazione del trattamento del contante

Fatta salva l'applicazione delle disposizioni in materia di esternalizzazione di funzioni operative importanti di cui al paragrafo precedente e al fine di minimizzare i rischi operativi, in particolare di natura legale, e reputazionali connessi con l'eventuale erogazione alla clientela di banconote false o di qualità tale da non renderle idonee alla circolazione, le banche che esternalizzano l'attività di trattamento del contante adottano specifiche cautele nella gestione dei rapporti con i soggetti cui l'attività è esternalizzata sia all'atto della scelta del contraente, che deve fondarsi sull'accertamento della sua piena affidabilità, della correttezza della gestione e dell'adeguatezza delle strutture e dei processi organizzativi, 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.

In particolare, le funzioni aziendali di controllo effettuano, ciascuna per i profili di competenza, una specifica valutazione delle procedure seguite per l'allacciamento e la gestione dei rapporti con i soggetti cui è esternalizzata l'attività di trattamento del contante nonché del complessivo assetto dei controlli sulle attività esternalizzate. Inoltre, tali funzioni assicurano il rispetto degli obblighi previsti dalla Decisione della Banca Centrale Europea del 16 settembre 2010, n. 14 relativa al controllo dell'autenticità e idoneità delle banconote in euro e al loro ricircolo.

La banca che intende esternalizzare l'attività di trattamento del contante stipula con l'*outsourcer* un contratto concluso in forma scritta che, oltre a rispettare i requisiti previsti nel paragrafo precedente, prevede:

- l'obbligo di attenersi alle disposizioni comunitarie sopra richiamate, con particolare riguardo: (i) all'utilizzo esclusivo di apparecchiature conformi a detta disciplina; (ii) alle procedure di verifica delle apparecchiature; (iii) alle attività di monitoraggio che possono essere condotte dalla Banca d'Italia;
- il diritto per la banca di recedere, senza penalità, nel caso in cui la controparte violi reiteratamente gli obblighi contrattuali.

Sezione V
Il sistema dei controlli interni nei gruppi bancari

1. Ruolo della capogruppo

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

a) un *controllo strategico* sull'evoluzione delle diverse aree di attività in cui il gruppo opera e dei rischi incombenti sulle attività esercitate. Si tratta di un controllo sia sull'andamento delle attività svolte dalle società appartenenti al gruppo (crescita o riduzione per via endogena), sia sulle politiche di acquisizione e dismissione da parte delle società del gruppo (crescita o riduzione per via esogena);

b) un *controllo gestionale* volto ad assicurare il mantenimento delle condizioni di equilibrio economico, finanziario e patrimoniale sia delle singole società, sia del gruppo nel suo insieme. Queste esigenze di controllo vanno soddisfatte preferibilmente attraverso la predisposizione di piani, programmi e budget (aziendali e di gruppo), e mediante l'analisi delle situazioni periodiche, dei conti infra-annuali, dei bilanci di esercizio delle singole società e di quelli consolidati; ciò sia per settori omogenei di attività sia con riferimento all'intero gruppo;

c) un *controllo tecnico-operativo* finalizzato alla valutazione dei vari profili di rischio apportati al gruppo dalle singole controllate e dei rischi complessivi del gruppo.

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

2. Controlli interni di gruppo

La capogruppo dota il gruppo di un sistema unitario di controlli interni che consenta l'effettivo controllo sia sulle scelte strategiche del gruppo nel suo complesso sia sull'equilibrio gestionale delle singole componenti.

Per definire il sistema dei controlli interni del gruppo bancario, la capogruppo applica, per quanto compatibili, le disposizioni previste nella 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:

– procedure formalizzate di coordinamento e collegamento fra le società appartenenti al gruppo e la capogruppo per tutte le aree di attività;

– compiti e responsabilità delle diverse funzioni aziendali di controllo all’interno del gruppo, le procedure di coordinamento, i riporti organizzativi ed i raccordi di tipo tecnico-informatico. Nel caso dei gruppi bancari, la relazione che le funzioni aziendali di controllo della capogruppo devono presentare agli organi aziendali (cfr. Sezione III, par. 2) illustra le verifiche effettuate, i risultati emersi, i punti di debolezza rilevati con riferimento, oltre che alla capogruppo medesima, anche al gruppo bancario nel suo complesso e propone gli interventi da adottare per la rimozione delle carenze rilevate;

– meccanismi di integrazione dei sistemi informativi e dei processi di gestione dei dati (specie per le società appartenenti al gruppo aventi sede in paesi che adottano diversi

schemi/criteri contabili o di rilevazione), anche al fine di garantire l'affidabilità delle rilevazioni su base consolidata;

– flussi informativi periodici che consentano l'effettivo esercizio delle varie forme di controllo su tutte le componenti del gruppo;

– procedure che garantiscano, a livello accentrato, un efficace processo unitario di gestione dei rischi del gruppo a livello consolidato. In particolare, vi deve essere un'anagrafe unica, o più anagrafi che siano facilmente raccordabili, presso le diverse società del gruppo in modo da consentire l'univoca identificazione, da parte delle diverse entità, dei singoli clienti e controparti, dei gruppi di clienti connessi e dei soggetti collegati e rilevare correttamente, a livello consolidato, la loro esposizione complessiva ai diversi rischi.

– sistemi per monitorare i flussi finanziari, le relazioni di credito (in particolare le prestazioni di garanzie) e le altre relazioni fra i soggetti componenti il gruppo;

– controlli sul raggiungimento degli obiettivi di sicurezza informatica e di continuità operativa definiti per l'intero gruppo e le singole componenti.

L'organo con funzione di controllo della società capogruppo verifica anche il corretto esercizio delle attività di controllo svolte dalla capogruppo sulle società del gruppo.

La capogruppo formalizza e rende noti a tutte le società del gruppo i criteri che presiedono le diverse fasi che costituiscono il processo di gestione dei rischi. Essa, inoltre, convalida i processi di gestione dei rischi all'interno del gruppo. Per quanto riguarda in particolare il rischio di credito, la capogruppo fissa i criteri di valutazione delle posizioni e crea una base informativa comune che consenta a tutte le società appartenenti al gruppo di conoscere l'esposizione dei clienti nei confronti del gruppo nonché le valutazioni inerenti alle posizioni dei soggetti affidati.

Ciascuna società del gruppo si dota di un sistema dei controlli interni che sia coerente con la strategia e la politica del gruppo in materia di controlli, fermo restando il rispetto della disciplina eventualmente applicabile su base individuale.

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

- le decisioni strategiche in merito all'utilizzo di strutture accentrate sono riservate all'organo con funzione di supervisione strategica con il parere dell'organo con funzione di controllo della capogruppo;

- devono essere chiaramente valutati e documentati i costi, i benefici ed i rischi alla base della soluzione adottata; tale analisi deve essere periodicamente aggiornata;

- gli organi aziendali delle componenti del gruppo sono consapevoli delle scelte effettuate dalla capogruppo e sono responsabili, ciascuno secondo le proprie competenze, dell'attuazione, nell'ambito delle rispettive realtà aziendali, delle strategie e politiche perseguite in materia di controlli, favorendone l'integrazione nell'ambito dei controlli di gruppo;

- all'interno di tutte le banche del gruppo e delle altre entità che, a giudizio della capogruppo, assumono rischi considerati rilevanti per il gruppo nel suo complesso vengono individuati appositi referenti i quali: svolgono compiti di supporto per la funzione aziendale di controllo esternalizzata; riportano funzionalmente e

gerarchicamente a quest'ultima; provvedono tempestivamente a segnalare eventi o situazioni particolari, suscettibili di modificare i rischi generati dalla controllata ([26]);

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

La capogruppo che intende procedere all'esternalizzazione di funzioni operative importanti o di controllo delle componenti del gruppo, accentrandole presso di sé, presso un'altra componente del gruppo o presso un soggetto esterno, è tenuta ad informare preventivamente la Banca d'Italia, fornendo tutte le indicazioni utili a verificare il rispetto dei criteri sopra indicati. Nel caso di esternalizzazioni presso soggetti con sede in altri paesi, si applicano le previsioni della Sezione IV.

Nel caso di controllate estere, è necessario che la capogruppo, nel rispetto dei vincoli locali, adotti tutte le iniziative atte a garantire standard di controllo e presidi comparabili a quelli previsti dalle disposizioni di vigilanza italiane, anche nei casi in cui la normativa dei paesi in cui sono insediate le filiazioni non preveda analoghi livelli di attenzione.

Per verificare la rispondenza dei comportamenti delle società appartenenti al gruppo agli indirizzi della capogruppo, nonché l'efficacia del sistema dei controlli interni, la capogruppo si attiva affinché, nei limiti dell'ordinamento, la funzione di revisione interna a livello consolidato effettui periodicamente verifiche in loco sulle componenti del gruppo, tenuto conto della rilevanza delle diverse tipologie di rischio assunte dalle diverse entità.

La capogruppo invia annualmente alla Banca d'Italia una relazione riguardante gli accertamenti effettuati sulle società controllate, contenente anche le considerazioni dei propri organi aziendali.

([26]) A seconda della funzione aziendale di controllo esternalizzata può trattarsi di responsabili di unità di controllo del rischio locali, "compliance officer", responsabili di unità distaccate di internal audit.

Sezione VI
Imprese di riferimento

Le imprese di riferimento sono responsabili del calcolo dei requisiti patrimoniali e del rispetto delle disposizioni prudenziali applicabili su base consolidata ([27]); a tali fini, il sistema di controlli interni nel suo complesso assicura la correttezza, l'adeguatezza e la tempestività dei flussi informativi con le altre società bancarie, finanziarie e strumentali controllate dalla società di partecipazione finanziaria madre nell'UE necessari per rispettare gli obblighi imposti dalle disposizioni prudenziali.

([27]) Cfr. Titolo I, Capitolo 1, Sezione III, par. 1.

Sezione VII
Procedure di allerta interna

Le procedure di allerta interna sono volte a permettere la segnalazione da parte dei dipendenti di eventuali disfunzioni dell'assetto organizzativo o del sistema dei controlli interni nonché di ogni altra irregolarità nella gestione della banca o violazione delle norme disciplinanti l'attività bancaria.

Le procedure devono garantire in ogni caso la riservatezza e la protezione dei dati personali del soggetto che effettua le segnalazioni ([28]) e del soggetto eventualmente segnalato. Tali procedure devono altresì prevedere un canale separato e diverso dalle tradizionali linee di *reporting*.

Le informazioni fornite dai dipendenti, ove rilevanti, sono rese disponibili agli organi aziendali;

Le procedure di allerta interna stabiliscono, in particolare:

- i soggetti che le possono attivare;
- i fatti e le azioni che possono essere riportati;
- le modalità attraverso cui segnalare eventuali criticità individuate e i soggetti che devono essere informati;
- il procedimento che si instaura nel momento in cui viene effettuata una segnalazione;
- l'obbligo per il soggetto segnalante di dichiarare se ha un interesse privato collegato alla segnalazione; nel caso in cui sia corresponsabile di una criticità il soggetto segnalante deve, compatibilmente con la normativa applicabile, avere un trattamento privilegiato rispetto agli altri corresponsabili;
- l'obbligo per i soggetti che ricevono una segnalazione di garantire la confidenzialità delle segnalazioni ricevute e dell'identità del segnalante che in ogni caso deve essere opportunamente tutelato da condotte ritorsive, discriminatorie o comunque sleali conseguenti la segnalazione;
- le modalità attraverso cui il soggetto segnalante e il soggetto segnalato devono essere informati sugli sviluppi del procedimento.

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

([28]) Gli obblighi di riservatezza non possono essere opposti all'autorità di vigilanza o all'autorità giudiziaria quando le informazioni richieste sono necessarie per indagini o procedimenti relativi a violazioni sanzionate penalmente.

Sezione VIII
Succursali di banche comunitarie e di banche extracomunitarie aventi sede nei paesi del Gruppo dei Dieci o in quelli inclusi in un elenco pubblicato dalla Banca d'Italia

Nel caso delle succursali di banche comunitarie e delle succursali di banche extracomunitarie aventi sede nei paesi del Gruppo dei Dieci ovvero in quelli inclusi in un elenco pubblicato e periodicamente aggiornato dalla Banca d'Italia, il legale rappresentante attesta annualmente che è stata condotta una verifica di conformità della condotta aziendale rispetto alle norme italiane applicabili alla succursale e riferisce sinteticamente alla Banca d'Italia in merito all'esito di tale verifica.

A tal fine, la banca verifica che le procedure interne adottate dalla succursale stessa siano adeguate rispetto all'obiettivo di prevenire la violazione delle norme italiane applicabili alla succursale.

Sezione IX
Informativa alla Banca d'Italia

Le banche comunicano tempestivamente alla Banca d'Italia la nomina e l'eventuale revoca dei responsabili delle funzioni aziendali di controllo. Nel caso di gruppi bancari tale comunicazione è eseguita dalla capogruppo

Le banche non appartenenti a gruppi bancari trasmettono inoltre alla Banca d'Italia:

- tempestivamente, le relazioni sull'attività svolta redatte annualmente dalle funzioni di controllo dei rischi, di conformità alle norme e di revisione interna (cfr. Sezione III, par. 2). Se una o più di queste funzioni sono esternalizzate, la relazione è redatta dal referente aziendale;
- entro il 30 aprile di ogni anno, una relazione, redatta dalla funzione di revisione interna - o, se esternalizzata, dal referente aziendale - con le considerazioni dell'organo con funzione di controllo e approvata dall'organo con funzione di supervisione strategica, relativa ai controlli svolti sulle funzioni operative importanti esternalizzate, alle carenze eventualmente riscontrate e alle conseguenti azioni correttive adottate (cfr. Sezione IV, par. 1);
- qualora ve ne siano le condizioni, la relazione di cui al punto 2.1 dell'Allegato A.

Le banche non appartenenti a gruppi che intendono esternalizzare funzioni operative importanti o di controllo sono tenute a informare preventivamente la Banca d'Italia, fornendo tutte le indicazioni utili a verificare il rispetto dei requisiti richiesti (cfr. Sezione IV, par. 1). Nel caso di esternalizzazione presso soggetti con sede in un altro paese la comunicazione alla Banca d'Italia deve essere effettuata almeno 30 giorni prima di conferire l'incarico (cfr. Sezione IV, par. 1). Entro 30 giorni dal ricevimento della comunicazione la Banca d'Italia può avviare un procedimento amministrativo d'ufficio di divieto dell'esternalizzazione che si conclude entro 60 giorni (cfr. Sezione IV, par. 1);

Le capogruppo di gruppi bancari:

- che intendono procedere all'esternalizzazione delle funzioni operative importanti o di controllo delle componenti del gruppo, accentrandole presso di sé, presso un'altra componente del gruppo o presso un soggetto esterno, sono tenute ad informare preventivamente la Banca d'Italia, fornendo tutte le indicazioni utili a verificare il rispetto dei requisiti richiesti (cfr. Sezione V, par. 2). Nel caso di esternalizzazioni presso soggetti con sede in un altro paese si applicano le norme previste dalla Sezione IV, par. 1;
- inviano annualmente alla Banca d'Italia una relazione riguardante gli accertamenti effettuati sulle società controllate, contenente anche le considerazioni dei propri organi aziendali (cfr. Sezione V, par. 2).

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

Nel caso delle succursali di banche comunitarie e delle succursali di banche extracomunitarie aventi sede nei paesi del Gruppo dei Dieci ovvero in quelli inclusi in un elenco pubblicato e periodicamente aggiornato dalla Banca d'Italia, il legale rappresentante attesta annualmente che è stata condotta una verifica di conformità della condotta aziendale rispetto alle norme italiane applicabili alla succursale e riferisce sinteticamente alla Banca d'Italia in merito all'esito di tale verifica (cfr. Sezione VIII).

Sezione X
Disposizioni abrogate

Dall'entrata in vigore delle presenti disposizioni sono abrogate le seguenti disposizioni:

- *Sistema dei controlli interni, compiti del collegio sindacale*, contenute nelle "Istruzioni di vigilanza per le banche", Circolare n. 229 del 21 aprile 1999, Titolo IV, Capitolo 11, ad eccezione della Sezione V (emissione e gestione di assegni bancari e postali);
- *La gestione e il controllo dei rischi. Ruolo degli organi aziendali*, contenute nelle "Nuove disposizioni di vigilanza prudenziale per le banche", Circolare n. 263 del 27 dicembre 2006, Titolo I, Capitolo I, Parte Quarta, Circolare n. 263 del *27* dicembre 2006;
- *Disposizioni di vigilanza - la funzione di controllo di conformità alle norme delle banche* (Comunicazione del 10 luglio 2007);
- *Disposizioni di vigilanza – Esternalizzazione del trattamento del contante* (Comunicazione del 7 maggio 2007).

Allegato A
Disposizioni speciali relative a particolari categorie di rischio

1. Premessa

Vengono in questa sede individuate disposizioni speciali in materia di controlli interni, che assumono valenza per la generalità delle banche e dei gruppi bancari, relativamente a specifiche categorie di rischio. Nel caso in cui la banca utilizzi sistemi interni di misurazione dei rischi per la determinazione dei requisiti patrimoniali (credito, controparte, mercato, operativi), queste indicazioni devono essere integrate con i principi di carattere organizzativo previsti dalle rispettive discipline, i quali costituiscono una delle condizioni per il riconoscimento, a fini prudenziali, di tali sistemi.

2. Rischio di credito e di controparte

L'intero processo di gestione del rischio di credito e di controparte (misurazione del rischio, istruttoria, erogazione, controllo andamentale e monitoraggio delle esposizioni, revisione delle linee di credito, classificazione delle posizioni di rischio, interventi in caso di anomalia, criteri di classificazione, valutazione e gestione delle esposizioni deteriorate) deve risultare dal regolamento interno ed essere periodicamente sottoposto a verifica.

Nel definire i criteri per l'erogazione dei crediti, il regolamento interno assicura che la diversificazione dei vari portafogli esposti al rischio di credito sia coerente con gli obiettivi di mercato e la strategia complessiva della banca.

La corretta misurazione del rischio di credito presuppone che le banche abbiano in ogni momento conoscenza della propria esposizione verso ciascun cliente e verso ciascun gruppo di clienti connessi (con rilevanza sia delle connessioni di carattere giuridico sia di quelle di tipo economico-finanziario). A tale fine, è indispensabile la disponibilità di basi dati complete ed aggiornate, di un sistema informativo che ne consenta lo sfruttamento ai fini richiesti, di un'anagrafe clienti attraverso cui generare ed aggiornare, a livello individuale e, nel caso di un gruppo bancario, consolidato, i dati identificativi della clientela, le connessioni giuridiche ed economico-finanziarie tra clienti diversi, le forme tecniche da cui deriva l'esposizione, il valore aggiornato delle tecniche di attenuazione dei rischi.

La corretta rilevazione e gestione di tutte le informazioni necessarie riveste particolare importanza nelle procedure per l'assunzione di grandi rischi. A tal fine, le banche sono tenute al rispetto della disciplina dettata nel Titolo V, Capitolo 1, Sezione V.

Nella fase istruttoria, le banche acquisiscono tutta la documentazione necessaria per effettuare un'adeguata valutazione del merito di credito del prenditore, sotto il profilo patrimoniale e reddituale, ed una corretta remunerazione del rischio assunto. La documentazione deve consentire di valutare la coerenza tra importo, forma tecnica e progetto finanziato; essa deve inoltre permettere l'individuazione delle caratteristiche e della qualità del prenditore, anche alla luce del complesso delle relazioni intrattenute. Nel caso di affidamenti ad imprese, sono acquisiti i bilanci (individuali e, se disponibili, consolidati), le altre informazioni desumibili dalla Centrale dei Bilanci e ogni altra informazione, significativa e rilevante, per valutare la situazione aziendale attuale e prospettica dell'impresa, anche di carattere qualitativo (validità del progetto imprenditoriale, assetti proprietari, esame della situazione del settore economico di appartenenza, situazione dei mercati di sbocco e di fornitura). Le procedure di sfruttamento delle informazioni devono fornire indicazioni circostanziate sul livello di affidabilità del cliente (ad esempio, attraverso sistemi di credit scoring e/o di rating). Nel caso in cui l'affidato faccia parte di un gruppo, la valutazione tiene conto anche della situazione e delle prospettive del gruppo nel suo

complesso. Al fine di conoscere la valutazione degli affidati da parte del sistema bancario le banche utilizzano, anche nella successiva fase di controllo andamentale e monitoraggio delle esposizioni, le informazioni fornite dalla Centrale dei Rischi.

Le deleghe in materia di erogazione del credito devono risultare da apposita delibera dell'organo con funzione di supervisione strategica e devono essere commisurate alle caratteristiche dimensionali della banca. Nel caso di fissazione di limiti "a cascata" (quando, cioè, il delegato delega a sua volta entro i limiti a lui attribuiti), la griglia dei limiti risultanti deve essere documentata. Il soggetto delegante deve inoltre essere periodicamente informato sull'esercizio delle deleghe, al fine di poter effettuare le necessarie verifiche.

Il controllo andamentale e il monitoraggio delle singole esposizioni devono essere svolti con sistematicità, avvalendosi di procedure efficaci in grado di segnalare tempestivamente l'insorgere di anomalie e di assicurare l'adeguatezza delle rettifiche di valore e degli accantonamenti.

I criteri di classificazione, valutazione e gestione delle esposizioni deteriorate ([29]), nonché le relative unità responsabili devono essere stabiliti con apposita delibera da parte dell'organo con funzione di supervisione strategica, nella quale vanno anche indicate le modalità di raccordo tra tali criteri e quelli previsti per le segnalazioni di vigilanza. Devono essere altresì stabilite procedure atte a individuare, in dettaglio, gli interventi da attuare in presenza di deterioramento delle posizioni di rischio e le strutture e funzioni cui spetta attuare tali interventi. Gli organi aziendali devono essere regolarmente informati sull'andamento delle esposizioni deteriorate e delle relative procedure di recupero.

Il sistema dei controlli interni deve, infine, garantire che l'intero processo di gestione del rischio ricomprenda l'esposizione al rischio di credito derivante dall'operatività diversa dalla tipica attività di finanziamento, costituita dai derivati finanziari e di credito, dalle operazioni SFT ("*securities financing transactions*") e da quelle con regolamento a lungo termine, così come definite nella disciplina relativa al trattamento prudenziale dei rischi di controparte.

A tal fine, le banche sono tenute anche al rispetto dei requisiti organizzativi per l'operatività in derivati di credito ([30]).

Nel caso di partecipazione ad accordi di compensazione, su base bilaterale o multilaterale, che misurano il rischio di controparte sulla base dell'esposizione netta anziché lorda, le banche verificano che gli accordi siano giuridicamente fondati. Nel caso in cui intendano riconoscere anche a fini prudenziali l'effetto di riduzione del rischio devono attenersi al rispetto dei criteri previsti dalla normativa (cfr. Titolo II, Capitolo 3, Sezione II, par. 10).

L'esigenza di assicurare idonei presidi non viene meno nei casi in cui i finanziamenti sono concessi nella forma del rilascio di garanzie, posto che il credito di firma concesso espone la banca al rischio di dover successivamente intervenire con una erogazione per cassa, attivando conseguentemente le azioni di recupero. Ciò in particolare quando il rilascio di garanzie costituisce l'attività esclusiva o prevalente della banca.

I presidi organizzativi devono pertanto assicurare anche:

- l'approfondita conoscenza - sin dall'inizio della relazione e per tutta la durata della stessa - della capacità dei garantiti di adempiere le proprie obbligazioni (incluse quelle di fare);

([29]) Nei gruppi bancari i criteri di classificazione, valutazione e gestione devono essere applicati in maniera omogenea.

([30]) Cfr. Bollettino di vigilanza n. 4 - Aprile 2006.

- il costante monitoraggio degli impegni assunti con riferimento sia al volume sia al grado di rischiosità degli stessi, specie in situazioni di elevata rotazione delle garanzie rilasciate.

Una particolare attenzione va inoltre posta nella definizione della contrattualistica, al fine di prevenire o limitare l'insorgere di contenziosi con riferimento sia all'attivazione delle garanzie rilasciate, sia alle successive eventuali azioni di rivalsa nei confronti dei garantiti.

Le banche evitano di sottoscrivere i contratti relativi alle garanzie rilasciate prima che siano stati definiti tutti gli elementi essenziali del rapporto (in particolare: indicazione del beneficiario, prestazione dovuta dal garantito, ammontare e durata della garanzia, modalità di liberazione dall'obbligo di garanzia o di rinnovo della stessa).

Al fine di assicurare il monitoraggio dell'esposizione, anche per il rispetto dei requisiti prudenziali in presenza elevata rotazione delle garanzie, il sistema delle rilevazioni contabili aziendali deve consentire di ricostruire la successione temporale delle operazioni effettuate.

2.1 Valutazione del merito di credito

Le disposizioni in materia di determinazione dei requisiti patrimoniali a fronte del rischio di credito nel metodo standardizzato, prevedono l'applicazione di coefficienti di ponderazione diversificati in funzione delle valutazioni del merito creditizio rilasciate dalle ECAI.

Il riconoscimento di un'ECAI, effettuato dalla Banca d'Italia mediante la procedura di cui al Titolo II, Capitolo 1, sezione VIII, non implica una valutazione di merito sulla validità dei giudizi attribuiti o un supporto alle metodologie utilizzate, di cui le ECAI restano le uniche responsabili; esso è volto a consentire alle banche l'utilizzo dei rating esterni ai fini del calcolo dei requisiti patrimoniali.

L'utilizzo dei rating esterni non esaurisce il processo di valutazione del merito di credito che le banche devono svolgere nei confronti della clientela sovvenuta; esso rappresenta soltanto uno degli elementi che possono contribuire alla definizione del quadro informativo sulla qualità creditizia del cliente.

Le banche si dotano, pertanto, di metodologie interne che consentano una valutazione del rischio di credito derivante da esposizioni nei confronti di singoli prenditori, titoli, posizioni verso le cartolarizzazioni nonché del rischio di credito a livello di portafoglio. Tali metodologie non devono basarsi meccanicamente sulle valutazioni espresse dalle ECAI.

La valutazione del merito di credito svolta dalla banca in base alle risultanze dell'attività istruttoria e delle sue metodologie interne può discostarsi da quelle effettuate dalle ECAI.

Divergenze frequenti nella valutazione del merito di credito possono essere indice di incompletezza e scarsa accuratezza del sistema di valutazione dell'agenzia esterna e costituiscono utili informazioni ai fini della periodica valutazione che la Banca d'Italia effettua sulla permanenza dei presupposti per il riconoscimento delle ECAI.

Le banche, oltre ad analizzare l'analisi della qualità dei singoli prenditori nell'ambito del processo di gestione del rischio, sono tenute ad effettuare, con periodicità almeno annuale, una specifica valutazione della complessiva coerenza dei rating delle ECAI con le valutazioni elaborate in autonomia. I risultati dell'esame sono formalizzati in un documento approvato dall'organo con funzione di gestione e portato a conoscenza dell'organo di

controllo. Ove dall'esame emergano frequenti e significativi disallineamenti fra valutazioni interne ed esterne, copia della citata relazione è trasmessa alla Banca d'Italia.

3. Rischi derivanti dall'utilizzo di tecniche di attenuazione del rischio di credito

Requisiti organizzativi specifici per la gestione dei rischi derivanti dall'utilizzo di tecniche di attenuazione del rischio di credito sono contenute nel Titolo II, Capitolo 2, Parte I, Sezione II.

4. Concentrazione dei rischi

Regole organizzative specifiche in materia di grandi rischi sono contenute nel Titolo V, Capitolo 1, Sezione V.

Inoltre, il sistema dei controlli interni assicura la gestione e il controllo, anche attraverso specifiche politiche e procedure aziendali, dei rischi di concentrazione derivanti dalle esposizioni nei confronti di clienti, incluse le controparti centrali, gruppi di clienti connessi, clienti operanti nel medesimo settore economico, nella medesima regione geografica o che esercitano la stessa attività o trattano la stessa merce nonché dall'applicazione di tecniche di attenuazione del rischio di credito, compresi in particolare i rischi derivanti da esposizioni indirette come, ad esempio, nei confronti di singoli fornitori di garanzie (cfr. Titolo III, Capitolo 1, Allegato B).

5. Rischi derivanti da operazioni di cartolarizzazione

Regole organizzative specifiche in materia di operazioni di cartolarizzazione sono contenute nel Titolo II, Capitolo 2, Parte II, Sezione VII.

In particolare, il sistema dei controlli interni assicura che i rischi derivanti da tali operazioni inclusi i rischi reputazionali derivanti, ad esempio, dall'utilizzo di strutture o prodotti complessi, siano gestiti e valutati attraverso adeguate politiche e procedure volte a garantire che la sostanza economica di dette operazioni sia pienamente in linea con la loro valutazione di rischiosità e con le decisioni degli organi aziendali.

6. Rischi di mercato

I principali requisiti relativi al processo di gestione dei rischi di mercato sono riportati nel Titolo II, Capitolo 4.

Il sistema di controlli interni, in particolare, assicura l'attuazione di politiche e procedure volte a identificare, misurare e gestire tutte le fonti e gli effetti derivanti dall'esposizione a rischi di mercato.

Nei casi in cui una posizione corta abbia scadenza inferiore rispetto alla relativa posizione lunga, la banca adotta adeguati presidi volti a prevenire il rischio di liquidità.

In ogni caso, le banche che non sono in grado di misurare e gestire correttamente i rischi associati a strumenti finanziari sensibili a più fattori di rischio devono astenersi dalla negoziazione di tali strumenti (cfr. Titolo II, Capitolo 4, Parte Seconda, Sezione II).

7. Rischio tasso di interesse derivante da attività non appartenenti al portafoglio di negoziazione a fini di vigilanza

Le banche predispongono adeguati sistemi volti a identificare, valutare e gestire i rischi derivanti da potenziali variazioni del livello dei tassi di interesse riguardanti attività

non appartenenti al portafoglio di negoziazione a fini di vigilanza (cfr. Titolo III, Capitolo 1, Allegato C).

8. Rischi operativi

Diversamente dagli altri rischi di "primo pilastro", per i quali la banca, in base alla sua propensione al rischio, assume consapevolmente posizioni creditizie o finanziarie per raggiungere il desiderato profilo di rischio/rendimento, l'assunzione di rischi operativi risulta implicita nella decisione di intraprendere un determinato tipo di attività e, più in generale, nello svolgimento dell'attività d'impresa.

In tale contesto, il sistema dei controlli interni deve costituire il presidio principale per la prevenzione ed il contenimento di tali rischi. In particolare, devono essere approvare e attuare politiche e procedure aziendali volte a definire, identificare, valutare e gestire l'esposizione ai rischi operativi, inclusi quelli derivanti da eventi caratterizzati da bassa frequenza e particolare gravità.

Le disposizioni in materia di governo e gestione dei rischi operativi sono riportati nel Titolo II, Capitolo 5. Essi si differenziano in relazione al tipo di trattamento prudenziale adottato dalla banca.

Le banche, inoltre, applicano le linee guida del CEBS/EBA in materia di gestione dei rischi operativi derivanti dall'attività di trading (cfr. CEBS/EBA GL35, "*Guidelines on management of operational risks in market-related activities*") ([31]).

9. Rischio di liquidità

Considerata l'importanza crescente che il rischio di liquidità ha assunto nel corso del tempo, i principi e le linee guida del sistema dei controlli interni sono trattati nel più ampio contesto dei presidi organizzavi da predisporre a fronte di questa categoria di rischio (Titolo V, Capitolo 2, Sezione V).

10. Rischio di leva finanziaria eccessiva

Le banche si dotano di politiche e procedure aziendali volte a identificare, gestire e monitorare il rischio di eccessiva leva finanziaria. Indicatori di tale tipologia di rischio sono l'indice di leva finanziaria e i disallineamenti tra attività e passività.

Le banche gestiscono conservativamente il rischio di eccessiva leva finanziaria considerando i potenziali incrementi di tale rischio dovuti alle riduzioni dei fondi propri della banca causate da perdite attese o realizzate derivanti dalle regole contabili applicabili. A tal fine, le banche devono essere in grado di far fronte a diverse situazioni di stress con riferimento al rischio di leva finanziaria eccessiva.

11. Rischi connessi con l'emissione di obbligazioni bancarie garantite

Regole di dettaglio in materia di responsabilità degli organi aziendali e controlli sulle banche che emettono obbligazioni bancarie garantite sono riportate nel Titolo V, Capitolo 3, Sezione II, par. 5.

([31]) Tali linee guida potranno essere incorporate nella versione definitiva del presente schema di disposizioni.

12. Rischi connessi con l’assunzione di partecipazioni

Al fine di gestire i rischi specifici connessi con l’assunzione di partecipazioni da parte di banche e gruppi bancari, specifiche regole organizzative e di governo societario sono contenute nel Titolo V, Capitolo 4, Sezione VII.

13. Attività di rischio e conflitti di interesse nei confronti di soggetti collegati

Con specifico riferimento alle operazioni con parti correlate si applicano specifiche disposizioni in materia di controlli interni e responsabilità degli organi aziendali contenute nel Titolo V, Capitolo 5, Sezione IV.

14. Rischi connessi con l’attività di banca depositaria di OICR e fondi pensione

Le banche che assumono l’incarico di depositaria rispettano le regole specifiche in materia di controlli interni contenute nel Titolo V, Capitolo 6, Sezioni II e IV.

Allegato B
Controlli sulle succursali estere

Le succursali estere di banche italiane presentano peculiari esigenze di controllo. Vengono di seguito formulate alcune indicazioni di carattere minimale cui le banche devono attenersi nell'orientare le proprie scelte in materia di controlli interni.

In particolare, le banche devono:

- verificare la coerenza dell'attività di ciascuna succursale o gruppo di succursali estere con gli obiettivi e le strategie aziendali;
- adottare procedure informative e contabili uniformi o comunque pienamente raccordabili con il sistema centrale, in modo da assicurare flussi informativi adeguati e tempestivi nei confronti degli organi aziendali;
- conferire poteri decisionali secondo criteri rapportati alle potenzialità delle succursali e attribuire le competenze tra le diverse unità operative di ciascuna succursale in modo da assicurare la necessaria dialettica nell'esercizio dell'attività;
- prevedere l'esercizio dei poteri di firma in forma congiunta; qualora le caratteristiche e la rischiosità delle operazioni lo richiedano, deve essere previsto l'intervento di dirigenti della succursale capo-area, ove esistente, o dell'organo con funzione di gestione. Eventuali deroghe per operazioni di importo e rischiosità limitati devono essere disciplinate con apposito regolamento;
- assoggettare le succursali estere ai controlli dell'*internal audit*, che devono essere effettuati da personale in possesso della necessaria specializzazione;
- istituire presso le succursali con una operatività significativa un'unità incaricata dei controlli di secondo livello e un’unità avente funzioni di revisione interna. Gli addetti a tali unità, di norma gerarchicamente dipendenti dalle funzione aziendali di controllo centrali, riferiscono, oltre che ai responsabili di tali funzioni, attraverso specifiche relazioni direttamente al dirigente preposto alla succursale capo-area, ove esistente, e all'organo con funzione di gestione;
- 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; l'esito delle verifiche va sottoposto all'organo con funzione di gestione, che curerà, almeno una volta all'anno, uno specifico riferimento all'organo con funzione di supervisione strategica.

L'organo con funzione di gestione deve avere cura di intensificare, a fini di controllo sulla propria struttura periferica, i rapporti con le parallele strutture centrali delle principali banche corrispondenti, concordando tra l'altro idonee procedure per la verifica delle posizioni reciproche.

Nella selezione dei dirigenti da preporre alla guida delle filiali estere, gli organi aziendali devono tenere conto della capacità degli interessati di adeguarsi alla logica dell'organizzazione aziendale e alle regole di comportamento applicabili in generale alle banche italiane.

Vanno previste verifiche, la cui frequenza deve essere coerente con la tipologia di rischi assunti dalla succursale estera, da parte dell’organo con funzione di controllo, della funzione di revisione interna e delle società di revisione esterne. Le verifiche in loco

condotte dalla funzione di revisione interna devono essere estese e riguardare almeno i rischi assunti, l'affidabilità delle strutture operative, i sistemi informativi, il funzionamento dei controlli interni, l'inserimento sul mercato. La periodicità minima delle verifiche, fissata dall’organo con funzione di gestione, è graduata in relazione all'operatività svolta e ai mercati di insediamento. I risultati delle verifiche sono portati tempestivamente a conoscenza degli organi aziendali.

TITOLO V - Capitolo 8
SISTEMA INFORMATIVO

Sezione I
Disposizioni di carattere generale

1. Premessa

Il sistema informativo (*hardware*, *software*, dati, documenti elettronici, reti telematiche) rappresenta uno strumento fondamentale per il conseguimento degli obiettivi strategici ed operativi degli intermediari. Infatti:

- dal punto di vista strategico, un'architettura flessibile dei sistemi informativi e un efficiente processo di sviluppo e gestione consentono di sfruttare le opportunità offerte dalla tecnologia per offrire migliori prodotti e servizi per la clientela e per accrescere la qualità dei processi di lavoro, facilitando lo scambio di informazioni e la creazione di sinergie anche con operatori esterni; inoltre la disponibilità di idonei strumenti informativi per l'analisi della propria operatività e del mercato costituisce il presupposto per l'assunzione di decisioni consapevoli e tempestive;
- nell'ottica della sana e prudente gestione, i sistemi informativi consentono al management di disporre di informazioni dettagliate, accurate e aggiornate per un regolare monitoraggio dei rischi aziendali;
- con riguardo al contenimento del rischio operativo, il regolare svolgimento dei processi interni e dei servizi forniti alla clientela, l'integrità, la riservatezza e la disponibilità delle informazioni trattate nonché la sicurezza dei valori custoditi fanno affidamento in misura rilevante sull'adeguatezza e funzionalità dei controlli automatizzati;
- con riferimento alla compliance, ai sistemi informativi è affidato il compito di registrare, conservare e rappresentare correttamente i fatti di gestione e gli eventi rilevanti per le finalità previste da norme di legge nonché da regolamenti interni ed esterni.

Le informazioni e i sistemi ICT aziendali degli intermediari costituiscono un patrimonio da salvaguardare, in considerazione da una parte, della criticità dei processi aziendali che dipendono da essi, dall'altra, della progressiva dematerializzazione dei valori custoditi e virtualizzazione dei servizi bancari.

I principi contenuti nel presente Capitolo rappresentano requisiti di carattere generale per lo sviluppo e la gestione dei sistemi informativi da parte degli intermediari, con riguardo ai profili sopraelencati. Le concrete misure da adottare possono essere individuate tenendo conto, oltre che degli specifici obiettivi strategici, anche, sulla base del principio di proporzionalità, delle dimensioni dell'intermediario, del tipo e della complessità della sua operatività, dal livello di automazione dei suoi processi e servizi. In tale ambito, gli intermediari fanno riferimento agli standard e *best practices* definiti a livello internazionale in materia di governo, controllo e sicurezza dei sistemi informativi.

2. Fonti normative

La materia è regolata:

- dalla direttiva xxxx/xx/UE del xx xxxxxx 2012 sull'accesso all'attività degli enti creditizi e sulla vigilanza prudenziale degli enti creditizi e delle imprese di investimento e che modifica la direttiva 2002/87/CE del Parlamento europeo e del Consiglio relativa alla vigilanza supplementare sugli enti creditizi, sulle imprese di assicurazione e sulle imprese di investimento appartenenti ad un conglomerato finanziario;
- dai seguenti articoli del TUB:
  a) art. 53, comma 1, lett. d), che attribuisce alla Banca d'Italia, in conformità delle delibere del CICR, il potere di emanare disposizioni di carattere generale in materia di organizzazione amministrativa e contabile e controlli interni delle banche;
  b) art. 67, comma 1, lett. d), che attribuisce alla Banca d'Italia, in conformità delle delibere del CICR, il potere di impartire alla capogruppo di un gruppo bancario disposizioni concernenti il gruppo complessivamente considerato o i suoi componenti aventi ad oggetto l'organizzazione amministrativa e contabile e i controlli interni;
- dalla delibera del CICR del 2 agosto 1996, come modificata dalla delibera del 23 marzo 2004, in materia di organizzazione amministrativa e contabile e controlli interni delle banche e dei gruppi bancari;
- dal decreto del Ministro dell'Economia e delle finanze, Presidente del CICR del 5 agosto 2004 in materia, tra l'altro, di compiti e poteri degli organi sociali delle banche e dei gruppi bancari;
- si tiene anche conto dei seguenti documenti pubblicati da organismi internazionali: *Information technology -- Security techniques -- Code of practice for information security management* (ISO/IEC 272002); *Control Objectives for Information and related Technology* (COBIT); *Information Technology Infrastructure Library* (ITIL); documento di consultazione della Banca Centrale Europea *Recommendations for the security of internet payments* e del Comitato di Basilea *Principles for effective risk data aggregation and risk reporting*.

3. Destinatari della disciplina

Le presenti disposizioni si applicano, secondo quanto stabilito nel Titolo I, Capitolo 1, Parte Seconda:

- alle banche autorizzate in Italia, ad eccezione delle succursali di banche extracomunitarie aventi sede nei paesi del Gruppo dei Dieci ovvero in quelli inclusi in un apposito elenco pubblicato e periodicamente aggiornato dalla Banca d'Italia ([1]);
- alle capogruppo di gruppi bancari;
- alle imprese di riferimento, secondo quanto previsto dalla Sezione VI del Capitolo 7.

4. Definizioni

Ai fini della presente disciplina si definiscono:

([1]) Alle banche che prestano servizi di investimento si applicano anche le disposizioni contenute nel Regolamento della Banca d'Italia e della CONSOB del 29 ottobre 2007 in materia di organizzazione e controlli degli intermediari che prestano servizi di investimento e di gestione collettiva.

- "*accountability*", l'assegnazione della responsabilità di un'attività o processo aziendale, con il conseguente compito di rispondere delle operazioni svolte e dei risultati conseguiti, a una figura aziendale ben determinata; in ambito tecnico, si intende la garanzia di poter attribuire le operazioni effettuate nei sistemi a enti (utenti o elaboratori) univocamente identificabili;
- "*autenticazione*", la procedura di riconoscimento di un utente da parte di un sistema o applicazione;
- "*ICT (Information and Communications Technology)*", la disciplina che comprende l'insieme delle conoscenze, dei metodi e degli strumenti utilizzati per il trattamento elettronico delle informazioni;
- "*operazioni critiche*", le operazioni di modifica effettuate da parte di personale tecnico nei sistemi informativi critici in ambiente di produzione (con riferimento a dati, programmi o alla configurazione del sistema) nonché l'utilizzo di funzioni applicative che comportano la possibilità, diretta o indiretta, di movimentare fondi;
- "*rischio informatico (o tecnologico)*", il complessivo livello di rischio cui sono soggetti i processi e i beni aziendali in relazione all'utilizzo di un dato sistema informatico. Tale tipologia di rischio rappresenta un sottoinsieme dei rischi operativi e come tale è trattato nell'ambito degli istituti di vigilanza prudenziale e della generale rappresentazione dei rischi aziendali;
- "*rischio informatico residuo*", il rischio informatico cui il sistema è comunque esposto una volta applicate le misure di sicurezza individuate mediante il processo di analisi dei rischi;
- "*risorsa informatica*", un bene dell'azienda afferente alla tecnologia ICT (cfr. ICT infra); comprende le risorse elaborative, di memorizzazione e trasmissive. Rientrano tra le risorse informatiche sottoposte a tutela anche le informazioni;
- "*segregazione dei compiti (segregation of duties)*", il principio stabilisce che l'esecuzione di operazioni di particolare criticità deve essere svolta attraverso la cooperazione di più utenti o amministratori di un sistema le cui responsabilità siano state formalmente ripartite;
- "*sistemi informativi critici*" ([2]), le applicazioni o infrastrutture che, per la rilevanza dei danni conseguenti a eventuali attacchi, malfunzionamenti o indisponibilità, richiedono elevati livelli di sicurezza e continuità;
- "*utente responsabile (system owner)*", la figura aziendale identificata o identificabile per ciascun sistema che ne assume la generale responsabilità amministrativa in rappresentanza degli utenti, in rapporto con le funzioni preposte allo sviluppo e alla gestione tecnica;
- "*verificabilità*", la garanzia di poter ricostruire, all'occorrenza, anche a distanza di tempo, eventi connessi all'accesso a sistemi ICT, all'utilizzo di servizi e al trattamento di informazioni.

([2]) Tali sistemi sono equiparati alle funzioni operative importanti di cui al Capitolo 7, Sezione I, par. 3.

Sezione II
Governo e organizzazione dell'ICT

Nell'ambito della generale disciplina dell'organizzazione e dei controlli interni, sono attribuiti agli organi e funzioni aziendali ruoli e responsabilità relativi allo sviluppo e alla gestione dei sistemi informativi, nel rispetto del principio della separazione delle funzioni di controllo da quelle di supervisione e gestione.

1. Compiti dell'organo con funzione di supervisione strategica

L'organo con funzione di supervisione strategica assume la generale responsabilità di indirizzo e controllo dei sistemi informativi, nell'ottica di un ottimale impiego della variabile tecnologica a sostegno delle strategie aziendali (*ICT governance*). In tale ambito esso:

- delibera in ordine al modello di riferimento per l'architettura dei sistemi informativi, in considerazione dell'articolazione in essere e a tendere dei settori di operatività, dei processi e dell'organizzazione aziendale; inoltre, delibera la policy di sicurezza in materia di trattamento di informazioni, di sviluppo di applicazioni e sistemi, nonché di esercizio e utilizzo di risorse e servizi tecnologici da parte del personale interno, di terze parti e della clientela;
- emana linee di indirizzo in materia di approvvigionamento delle risorse: modalità di selezione del personale tecnico e di acquisizione di sistemi, software e servizi, incluso il ricorso a fornitori esterni (cfr. Sezione V);
- promuove strumenti e modalità organizzative per lo sviluppo, la condivisione e l'aggiornamento di conoscenze in materia di ICT all'interno dell'azienda;
- è informato con cadenza almeno annuale sul valore fornito all'azienda dai sistemi informativi, in termini di adeguatezza dei servizi erogati e del supporto prestato all'evoluzione del business, in rapporto ai costi sostenuti; è inoltre informato tempestivamente in caso di gravi problemi per l'attività aziendale derivanti da incidenti e malfunzionamenti rilevanti del sistema informativo.

Con specifico riguardo all'esercizio della responsabilità di supervisione della gestione del rischio informatico (cfr. sezione III), lo stesso organo:

- approva il quadro di riferimento organizzativo e metodologico per l'analisi del rischio informatico, volto ad assicurare che tale categoria di rischio sia regolarmente identificata, valutata e trattata nei vari settori operativi nonché opportunamente aggregata e comunicata attraverso i livelli di management e gli organi aziendali, secondo criteri uniformi;
- approva il livello di tolleranza al rischio informatico dell'intermediario con riguardo sia ai servizi interni che a quelli offerti alla clientela, in raccordo con il quadro di riferimento generale della gestione del rischio aziendale;
- è informato con cadenza almeno annuale sulla situazione di rischio informatico rispetto al livello accettato di tolleranza al rischio.

Nell'allegato A, vengono riportati i documenti che l'organo con funzione di supervisione strategica deve approvare nell'ambito del suo ruolo e responsabilità nella materia.

Box 4

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

2. Compiti dell'organo con funzione di gestione

L'efficacia e il regolare funzionamento dei sistemi informativi sono sotto la responsabilità dell'organo con funzione di gestione. In particolare, tale organo:

- definisce la struttura organizzativa della funzione ICT assicurandone la rispondenza alle strategie e ai modelli architetturali definiti dall'organo con funzione di supervisione strategica, garantendo il corretto dimensionamento quali-quantitativo delle risorse umane assegnate;
- disegna e segue l'implementazione dei processi di gestione dell'ICT – incluso in particolare il processo di analisi del rischio informatico – 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 robustezza dei controlli, alla validità del supporto metodologico e procedurale;
- approva gli standard di *data governance*, le procedure di gestione dei cambiamenti e degli incidenti e, di norma con cadenza annuale, il piano operativo delle iniziative informatiche, verificandone la coerenza con le esigenze informative e di automazione delle linee di business nonché con le strategie aziendali;
- valuta almeno annualmente le prestazioni della funzione ICT rispetto alle strategie e agli obiettivi fissati, in termini di rapporto costi / benefici, ovvero con riferimento a sistemi integrati di misurazione delle prestazioni ([3]), assumendo opportuni interventi e iniziative di miglioramento.
- fornisce con periodicità almeno annuale all'organo con funzione di supervisione strategica flussi informativi sulla situazione del rischio tecnologicononché sul valore e costi dei servizi ICT; provvede a fornire all'organo con funzione di supervisione strategica tempestive informazioni in caso di gravi problemi per l'attività aziendale derivanti da incidenti e malfunzionamenti rilevanti del sistema informativo.

Nell'ambito dei suoi compiti di gestione nel continuo dei rischi informatici, in rapporto alla tolleranza al rischio definita, l'organo con funzione di gestione:

- verifica regolarmente la complessiva situazione del rischio informatico sulla base di idonei flussi informativi – concernenti, come minimo, il livello di rischio residuo valutato per le diversi risorse informatiche, lo stato di avanzamento degli eventuali piani di implementazione dei presidi di sicurezza (cfr. Sez. III) nonché gli incidenti registratisi nel periodo di riferimento;

([3]) I sistemi integrati di misurazione e *reporting* delle prestazioni sono sistemi automatizzati, di norma basati su specifiche metodologie (ad es. *balanced scorecards*), volti a tracciare un profilo integrato del complessivo andamento dell'azienda o di una specifica funzione aziendale, attraverso il ricorso ad indicatori di prestazione (*KPI – key performance indicators*) e valori di riferimento (*benchmark*) opportunamente individuati.

– pone in atto opportune azioni correttive;

– assume decisioni tempestive in merito a gravi incidenti (cfr. Sez. IV).

Indipendentemente dall'articolazione organizzativa dell'intermediario e dalle strategie di *sourcing* adottata per l'ICT, l'organo con funzione di gestione deve essere dotato di competenze tecnico – manageriali coerenti con le responsabilità ed i compiti menzionati.

Nell'allegato A, vengono riportati i documenti che l'organo con funzione di gestione deve approvare nell'ambito del suo ruolo e responsabilità nella materia.

3. Organizzazione della funzione ICT

L'articolazione organizzativa della funzione ICT dipende da diversi fattori, quali la complessità della struttura societaria, la dimensione, i settori di attività, le strategie di business e gestionali. Essa deve ispirarsi a criteri di funzionalità, efficienza e sicurezza, definendo chiaramente compiti e responsabilità e contemplando in particolare:

– la previsione, nelle realtà più complesse, di un organo ("Direttore dei sistemi informativi" o equivalente) che assume la generale responsabilità della funzione, con linea di riporto diretta verso l'organo con funzione di gestione ([4]), a garanzia dell'unitarietà della visione gestionale e del rischio informatico nonché dell'uniformità di applicazione delle norme riguardanti i sistemi informativi;

– la chiara attribuzione di responsabilità per la pianificazione e il controllo unitario del portafoglio dei progetti informatici; si colloca in tale ambito il governo dell'evoluzione dell'architettura e dell'innovazione tecnologica;

– la realizzazione degli opportuni meccanismi di raccordo con le linee di business, con particolare riguardo alle attività propedeutiche all'individuazione e pianificazione delle iniziative informatiche (raccolta della domanda di servizi informatici e promozione delle opportunità tecnologiche offerte dall'evoluzione dei sistemi ICT);

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

([4]) Eventuali unità di sviluppo decentrato sotto il controllo delle linee di business devono comunque inquadrarsi nel più generale disegno architetturale ed agire nell'ambito di regole definite a livello aziendale.

Sezione III
La gestione del rischio informatico

Il processo di analisi del rischio informatico costituisce un importante strumento aziendale a garanzia dell'efficacia ed efficienza dei sistemi di protezione, permettendo di graduare la misure di sicurezza in funzione degli specifici rischi ravvisati nei diversi ambienti; inoltre esso riveste un fondamentale ruolo di raccordo tra i processi di governo dei sistemi informativi (Sezione II) e le attività tecnico – gestionali della sicurezza informatica (Sezione IV).

Il processo di analisi deve essere svolto dall'utente responsabile ([5]) con la partecipazione del personale tecnico, secondo una metodologia definita dall'organo con funzione di gestione. Esso si compone di due fasi successive:

– la valutazione del rischio potenziale cui sono soggette le risorse informatiche esaminate, prima dell'applicazione degli opportuni presidi di sicurezza; l'attività deve interessare tutte le iniziative informatiche per la realizzazione di nuovi sistemi e di rilevanti modifiche ai sistemi esistenti ([6]).

  Tale fase prende l'avvio con la classificazione delle risorse informatiche, sulla base di criteri documentati ed uniformi, ad esempio assegnando un livello di criticità in relazione al potenziale impatto di un'eventuale violazione per ciascuno dei profili di riservatezza, integrità, disponibilità ([7]);

– il trattamento del rischio, volto all'individuazione delle misure di sicurezza – di tipo tecnico e organizzativo - idonee a conseguire il contenimento del rischio individuato; le modalità di svolgimento possono variare in dipendenza delle risultanze della fase precedente, ma in ogni caso deve essere determinato il rischio residuo da sottoporre ad accettazione formale dell'utente responsabile ([8]). In tale ambito l'utente responsabile, che sarà in generale vincolato all'osservanza del livello di tolleranza al rischio definito a livello aziendale, potrà eventualmente considerare l'adozione di misure alternative o ulteriori di trattamento del rischio ([9]).

  Per i sistemi già in esercizio, gli eventuali presidi in aggiunta a quelli già operativi devono formare oggetto di uno specifico piano di implementazione, con l'indicazione dei tempi di realizzazione. Nelle more dell'attuazione del piano, il rischio residuo deve essere trattato con presidi compensativi, ad esempio di tipo organizzativo o procedurale, anch'essi documentati e sottoposti all'accettazione formale dell'utente responsabile.

([5]) Nel caso di sistemi informativi critici l'utente responsabile deve essere individuato ad un adeguato livello gerarchico.

([6]) In sede di valutazione dei rischi di sistemi esistenti si dovrà tenere opportunamente conto dei dati disponibili in merito agli incidenti di sicurezza verificatisi che abbiano coinvolto detti sistemi (cfr. Sezione IV, par. 4).

([7]) La classificazione delle risorse informatiche va opportunamente raccordata con il trattamento delle informazioni aziendali in formato diverso da quello elettronico, onde conseguire uniformi livelli di protezione indipendentemente dalle modalità di trattamento delle informazioni.

([8]) Nel documento approvato dall'utente responsabile, il rischio residuo deve essere espresso indicando un livello qualitativo e una descrizione in termini non tecnici degli eventi dannosi che potrebbero comunque verificarsi in determinate circostanze.

([9]) Ad esempio potrebbe essere deciso di non abilitare funzioni od operazioni considerate troppo rischiose (*risk avoidance*), ovvero di acquisire una polizza assicurativa in relazione alla fornitura dei servizi informatici in esame (*risk transfer*).

I risultati del processo (livelli di classificazione, rischi potenziali e residui, lista delle minacce considerate, elenco dei presidi individuati e testati), ogni loro aggiornamento successivo, le assunzioni operate e le decisioni assunte devono essere documentati.

L'analisi del rischio va rivista con periodicità adeguata alla tipologia dei sistemi e dei rischi e alla presenza di situazioni che possono influenzare il livello di rischio informatico ([10]).

([10]) Tra le situazioni suscettibili di modificare il livello di rischio informatico valutato – e che quindi richiedono la revisione dell'analisi del rischio – ci sono il verificarsi di gravi incidenti, la rilevazione di carenze nei controlli, la diffusione di notizie su nuove vulnerabilità o minacce che potrebbero interessare propri sistemi.

Sezione IV
Il sistema di gestione della sicurezza informatica

Il sistema di gestione della sicurezza ha l'obiettivo di garantire a ciascun insieme individuato di informazioni o servizio applicativo una protezione, – in termini di riservatezza, integrità, disponibilità, verificabilità e *accountability* – appropriata e coerente lungo l'intero ciclo di vita.

Obiettivo del sistema è anche di contribuire alla conformità delle risorse informatiche alle norme di legge e regolamenti interni ed esterni.

La struttura dei processi e l'intensità dei presidi da porre in atto dipende dalle risultanze dell'analisi dei rischi (cfr. Sezione III), processo attorno al quale gravitano tutte le attività che concorrono a realizzare il sistema di sicurezza.

Le disposizioni contenute nella presente Sezione sono da intendersi come requisiti minimi, nel rispetto del principio di proporzionalità, non esaurendo le opportune misure e cautele che gli intermediari sono chiamati a porre in atto in relazione alle caratteristiche e ai rischi specifici dei propri sistemi informativi.

1. Policy di sicurezza

La policy di sicurezza informatica deve essere approvata dall'organo con funzione di supervisione strategica e comunicata a tutto il personale nonché alle terze parti esterne coinvolte nella gestione di informazioni e sistemi. Essa deve riportare:

- gli obiettivi del sistema di gestione della sicurezza delle informazioni, in linea con la tolleranza al rischio informatico definita a livello aziendale, espressi in termini di esigenze di protezione e di controllo del rischio tecnologico;
- i principi generali sull'utilizzo e la gestione dei sistemi informatici da parte dei diversi profili aziendali;
- i ruoli e le responsabilità delle funzioni aziendali deputate alla sicurezza informatica nonché all'aggiornamento e verifica delle policy;
- il quadro di riferimento organizzativo e metodologico dei processi di gestione dell'ICT deputati a garantire l'appropriato livello di protezione;
- le linee di indirizzo per le attività di comunicazione, training e sensibilizzazione delle diverse classi di utenti in materia di sicurezza;
- un richiamo alle norme interne che disciplinano le conseguenze di violazioni rilevate della policy da parte del personale.

La policy di sicurezza può fare riferimento ad ulteriore documentazione di carattere più specifico, ad esempio linee guida o manuali operativi in tema di configurazioni e procedure di sicurezza per particolari sistemi e applicazioni, ovvero di norme per il corretto utilizzo di applicazioni aziendali trasversali, quali la posta elettronica e la navigazione internet.

2. La sicurezza dei dati e il controllo degli accessi

Il controllo degli accessi ad applicazioni, dati e sistemi viene realizzato attraverso presidi e procedure di sicurezza a livello fisico e logico, la cui intensità di applicazione deve

essere graduata in relazione alle risultanze della valutazione del rischio (classificazione delle informazioni, rischi potenziali). Tali misure comprendono:

- i presidi fisici di difesa e le procedure di autorizzazione e controllo per l'accesso fisico a sistemi e dati (ad es. barriere perimetrali con punti di ingresso vigilati, locali ad accesso controllato con registrazione degli ingressi e delle uscite);
- la regolamentazione dell'accesso logico ai sistemi, sulla base delle effettive esigenze operative (principio del *need to know*); i diritti di accesso devono essere accordati, mediante ricorso ad opportuni profili abilitativi, previa formale autorizzazione; l'elenco degli utenti abilitati deve essere sottoposto a verifica con periodicità definita;
- la procedura di autenticazione per l'accesso alle applicazioni e ai sistemi informatici; in particolare devono essere garantite l'univoca associazione a ciascun utente delle proprie credenziali di accesso, il presidio della riservatezza dei fattori di autenticazione ([11]), l'osservanza di policy e standard definiti all'interno nonché delle normative applicabili ([12]) (ad es. in materia di composizione e gestione della password, di limiti ai tentativi di accesso, di lunghezza di chiavi crittografiche);
- la segmentazione della rete di telecomunicazione, con controllo dei flussi scambiati, in particolare tra domini connotati da diversi livelli di sicurezza (ad es. sistemi e utenti interni, applicazioni *core*, sistemi e utenti esterni); i collegamenti di sistemi critici con la rete internet (ad es. nel caso dell'*e-banking*) devono essere presidiati attraverso specifici sistemi e procedure di sicurezza, in grado di fornire un livello di protezione adeguato ai rischi da fronteggiare;
- la separazione degli ambienti di sviluppo, collaudo e produzione, con adeguata formalizzazione del passaggio di moduli software dal primo, al secondo, al terzo (par. 3), al fine di evitare l'accesso a dati riservati e sistemi critici da parte del personale addetto allo sviluppo e di esercitare un più stretto controllo degli accessi e delle modifiche nell'ambiente di produzione;
- le procedure per lo svolgimento delle operazioni critiche, con riguardo ai principi del minimo privilegio ([13]) e della segregazione dei compiti (ad esempio specifiche procedure di abilitazione e di autenticazione, controlli di tipo *four eyes* [14], o di verifica giornaliera ex-post);
- il monitoraggio di accessi, operazioni ed altri eventi che occorrono nei sistemi e nelle applicazioni, in base alle risultanze del processo di analisi dei rischi, previa individuazione dei casi che configurano un'anomalia e delle conseguenti procedure di gestione; in particolare, vanno sottoposti a stretto controllo le attività degli amministratori di sistema ed altri utenti privilegiati;
- la verifica periodica delle vulnerabilità tecniche di sistema e applicative;

([11]) La procedura di generazione e di gestione dei fattori di autenticazione (ad es. *password, smart card, token*) garantisce che essi siano unici e nella sola disponibilità del legittimo utente assegnatario.

([12]) Si fa riferimento in particolare al "Codice in materia di protezione dei dati personali" (D.lgs. 196/3003) – All. B.

([13]) Il principio di minimo privilegio (*least privilege*) stabilisce che vengano assegnati a ciascun utente o amministratore di sistema le abilitazioni strettamente necessarie allo svolgimento dei propri compiti;

([14]) Si fa riferimento a controlli applicativi che richiedono l'inserimento di una stessa transazione da parte di due diversi utenti per procedere alla sua esecuzione.

– le regole di tracciabilità delle azioni svolte, finalizzate a consentire la verifica a posteriori delle operazioni critiche, con l'archiviazione dell'autore, data e ora ([15]), contesto operativo e altre caratteristiche salienti della transazione. Il periodo di conservazione per le tracce elettroniche in discorso non deve essere inferiore a cinque anni ([16]).

Disposizioni specifiche per la sicurezza delle applicazioni telematiche fornite alla clientela (*e-banking*) sono riportate nell'Allegato B.

3. La gestione dei cambiamenti

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

– la valutazione dell'impatto sui sistemi e dei rischi correlati con tutte le proposte di modifica;

– l'effettuazione del collaudo e dei test di sicurezza nell'ambiente deputato;

– l'autorizzazione formale di ogni cambiamento in ambiente di produzione ([17]);

– il ricorso ad un idoneo sistema di registrazione, conservazione e gestione della configurazione del sistema (hardware, software, procedure di gestione ed utilizzo, modalità di interconnessione), per il controllo dell'implementazione dei cambiamenti, inclusa la possibilità di ripristino della situazione ex ante;

– nei casi di maggior rilievo, individuati dalla normativa interna, lo svolgimento o l'aggiornamento dell'analisi dei rischi e l'accettazione formale del sistema introdotto o modificato da parte dell'utente responsabile.

Fanno eccezione le modifiche in caso di emergenza, che possono essere gestite con presidi adeguati alla particolare situazione. Va comunque previsto il tracciamento delle operazioni nonché la notifica ex post all'utente responsabile.

Le iniziative di ampio impatto sui sistemi informativi critici e sui sistemi a supporto dell'operatività caratteristica (ad es. adeguamento dei sistemi in conseguenza di fusioni o scissioni, migrazione ad altre piattaforme) – che si inseriscono di norma in piani strategici all'attenzione dell'organo con funzione di supervisione strategica - devono essere preventivamente comunicate alla Banca d'Italia e prevedere, in aggiunta a quanto sopra specificato, tutte le idonee misure, tecniche, organizzative e procedurali, volte a garantire un avvio in esercizio controllato e con limitati impatti sui servizi forniti alla clientela (ad es. implementazione per stadi successivi, periodi di esercizio in parallelo con la precedente procedura, procedure di *fallback* [18] e *contingency* [19]). Il puntuale monitoraggio

([15]) Ai fini della possibilità di una corretta ed agevole ricostruzione di eventi ed operazioni che coinvolgono più sistemi, inclusi eventualmente sistemi esterni, è opportuno che l'intermediario si doti di un sistema unificato di riferimento temporale, ad esempio basato sul protocollo standard NTP e sincronizzato con un segnale orario di riferimento ufficiale.

([16]) L'intermediario deve altresì fare riferimento alla normativa in materia di protezione dei dati personali per gli obblighi di tracciamento di operazioni – anche in sola consultazione – inerenti informazioni appartenenti a tale fattispecie.

([17]) Il livello autorizzativo deve essere adeguato ai rischi correlati.

([18]) Una procedura di *fallback* è volta a fornire modalità alternative per lo svolgimento delle funzioni applicative offerte da un sistema di nuova implementazione.

dell'avanzamento del progetto deve comprendere adeguati flussi informativi per i vari livelli manageriali e verso gli organi aziendali.

4. La gestione degli incidenti di sicurezza

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);

La gestione degli incidenti di sicurezza segue procedure formalmente definite ([20]), con l'obiettivo di minimizzare l'impatto di eventi avversi e garantire il tempestivo ripristino del regolare funzionamento dei servizi e dei sistemi coinvolti. Vanno individuate le funzioni a cui va comunicato l'accadere dell'incidente, secondo un'opportuna procedura di *escalation*; i casi più gravi che comportino rischi di interruzione della continuità operativa devono essere segnalati alla struttura preposta a dichiarare lo stato di emergenza (cfr. Capitolo 9 - Paragrafo 6.2).

Il processo deve raccordarsi con la gestione dei malfunzionamenti e della segnalazioni di problemi da parte degli utenti, al fine di consentire una visione organica dei fenomeni, favorendo l'assunzione di iniziative di prevenzione.

Gli incidenti che causino perdite economiche elevate o prolungati disservizi all'intermediario o alla clientela, anche in conseguenza del ripetuto verificarsi di incidenti di minore entità, devono essere comunicati senza indugio alla Banca d'Italia, attraverso un rapporto sintetico recante, oltre al tempo di rilevazione e alla descrizione delle azioni intraprese, i seguenti dati, accertati o presunti: data e ora dell'accadimento o dell'inizio della manifestazione dell'incidente, sistemi e servizi coinvolti, cause, impatti, tempi e modalità previsti per il pieno ripristino dei livelli di disponibilità e sicurezza definiti e per il completo accertamento dei fatti connessi..

5. La disponibilità delle informazioni e dei servizi ICT

La disponibilità dell'accesso a dati e dei servizi telematici deve essere garantita agli utenti autorizzati negli orari definiti dai livelli di servizio concordati. A tal fine, va tenuto conto delle seguenti indicazioni per tutti i processi interessati (definizione dei modelli architetturali, gestione dei problemi tecnici, monitoraggio e pianificazione della capacità elaborativa e trasmissiva, sviluppo di infrastrutture e sistemi, gestione dei fornitori):

– con riguardo alle applicazioni di maggiore criticità (elevato livello di classificazione per il profilo disponibilità) e ai servizi ICT rivolti alla clientela sono formalmente definiti i livelli di servizio che l'intermediario si impegna ad osservare; le prestazioni dei sistemi rispetto a tali livelli devono essere regolarmente monitorate e formare oggetto di sintetici rapporti da rendere disponibili periodicamente a tutte le parti interessate; è assicurata la congruità tra i livelli definiti per sistemi in rapporto di dipendenza operativa;

([19]) Una procedura di *contingency* prevede il ricorso a strumenti semplificati, che possono contemplare anche il ricorso ad attività manuali, per effettuare un nucleo individuato di operazioni di particolare criticità in caso di indisponibilità o grave malfunzionamento della piattaforma applicativa utilizzata di norma.

([20]) Nel caso delle banche AMA il processo è integrato con la rilevazione delle perdite operative.

- in relazione alle esigenze di disponibilità delle singole applicazioni, sono definite procedure di backup (di dati, software e configurazione) e di ripristino su sistemi alternativi individuati;
- le architetture dei sistemi sono disegnate in considerazione degli obiettivi di disponibilità delle applicazioni ospitate, tenendo conto di tutte le risorse ICT e di supporto interessate (alimentazione elettrica, impianti di condizionamento, ecc.); a tale riguardo, l'intermediario può considerare l'opportunità di predisporre una specifica piattaforma volta a garantire l'alta disponibilità delle applicazioni maggiormente critiche ([21]), in sinergia con le procedure e i sistemi utilizzati per il *disaster recovery*;
- in funzione della criticità delle comunicazioni e delle applicazioni accedute, i collegamenti tra sedi, centri elaborativi, articolazioni territoriali e con i punti di accesso a internet per la fornitura di servizi telematici sono opportunamente ridondati;
- la gestione dei sistemi ICT è opportunamente automatizzata e si avvale di procedure standardizzate; le operazioni di manutenzione ordinaria e straordinaria sono pianificate e comunicate con congruo anticipo agli utenti interessati;
- le informazioni raccolte attraverso il processo di monitoraggio dei sistemi e delle reti - coerente con il livello di rischio attribuito – devono alimentare il regolare processo di *capacity planning* ([22]) ed essere utilizzate nella progettazione dell'evoluzione dei sistemi informativi.

([21]) L'alta disponibilità può essere ottenuta mediante architetture particolarmente robuste e completamente ridondate (in osservanza del principio del *no single point of failure*, secondo il quale l'eventuale guasto di un qualsiasi singolo componente di un sistema non deve compromettere il regolare funzionamento di quest'ultimo).

([22]) Si intende per *capacity planning* il processo di gestione dell'ICT volto a stimare la quantità di risorse informatiche necessarie a fronteggiare le esigenze delle applicazioni aziendali nell'arco di un determinato periodo futuro.

Sezione V
Il sistema di gestione dei dati

Il sistema di registrazione e reporting è deputato a tracciare tempestivamente tutte le operazioni aziendali e i fatti di gestione al fine di fornire informazioni adeguate e aggiornate sulla gestione del business e sull'evoluzione dei rischi. Esso deve assicurare nel continuo l'integrità, completezza e correttezza dei dati conservati e delle informazioni rappresentate; inoltre deve garantire l'*accountability* e l'agevole verificabilità (ad esempio da parte delle funzioni di controllo) delle operazioni registrate.

In particolare, il sistema deve soddisfare i seguenti requisiti:

- la registrazione dei fatti aziendali deve essere completa, corretta e tempestiva, al fine di consentire la ricostruzione dell'attività svolta ([23]);
- è definito uno standard aziendale di *data governance*, che individua ruoli e responsabilità delle funzioni coinvolte nel trattamento dell'informazione nonché le misure atte a garantire la qualità dei dati (in termini di completezza e accuratezza) ([24]), sia operativi che gestionali ([25]);
- l'utilizzo di procedure settoriali (contabilità, segnalazioni, antiriciclaggio, ecc.) non deve compromettere la qualità e la coerenza complessiva dei dati aziendali; a livello consolidato, va garantita l'integrazione tra le informazioni provenienti da tutte le componenti del gruppo;
- nel caso di ricorso ad uno specifico sistema aziendale di *datawarehouse* a fini di analisi e reporting le procedure di estrazione dai sistemi operazionali, di trasformazione e caricamento nel nuovo sistema – così come le funzioni di sfruttamento dei dati – devono essere dettagliatamente documentate, al fine di consentire la verifica della qualità dei dati forniti;
- le procedure di gestione dei dati sono documentate, con specifica previsione delle circostanze in cui è ammessa l'immissione o la rettifica manuale di dati aziendali: in tali casi, va tenuta traccia della data, ora e motivo dell'intervento, l'ambiente operativo interessato, i dati precedenti la modifica, l'utente che effettua l'intervento;
- i dati devono essere conservati con una granularità adeguata a consentire le diverse analisi ed aggregazioni richieste dalle procedure di sfruttamento;
- i rapporti prodotti devono esporre le principali assunzioni e gli eventuali criteri di stima adottati (ad esempio, nell'ambito del monitoraggio dei rischi aziendali);
- il sistema di reporting deve consentire di produrre informazioni tempestive e di qualità elevata per l'Autorità di vigilanza e per il mercato.

([23]) I controlli sulle registrazioni contabili verificano, tra l'altro, le procedure per l'individuazione e sistemazione delle divergenze tra saldi dei sottosistemi sezionali e quelli della contabilità generale, i processi di quadratura tra i documenti di *front-office* e le registrazioni giornaliere; la conferma periodica dei rapporti con controparti e clienti.

([24]) La completezza è garantita dalla registrazione di tutti gli eventi, operazioni ed informazioni – con i pertinenti attributi – necessarie per le elaborazioni da effettuare, mentre l'accuratezza dei dati viene assicurata dalla verifica dell'assenza di distorsione nei processi di registrazione o raccolta dei dati, nonché in fase di successivo trattamento.

([25]) Le banche classificate, a fini SREP, nelle macro-categorie 1 e 2 (cfr. Circolare 269 del 7 maggio 2008, "Guida per l'attività di vigilanza", Sezione I, Capito I.5) individuano uno o più responsabili della qualità dei dati rilevanti (informazione al mercato, segnalazioni all'OdV, valutazione dei rischi, ecc).

Sezione VI
L'esternalizzazione di sistemi e servizi ICT

1. Tipologie di esternalizzazione

L'esternalizzazione dei sistemi e servizi ICT può assumere diverse forme, a seconda delle caratteristiche funzionali e della flessibilità architetturale: dall'outsourcing verticale – relativo a determinati processi operativi - a varie forme di outsourcing orizzontale di servizi, concernenti ad esempio gli apparati hardware (*facility management*), del parco applicativo (*application management*), dei collegamenti di rete, di alcuni processi di gestione dell'ICT (ad es. help desk, interventi tecnici di riparazione e manutenzione, sviluppo applicativo).

L'intermediario deve essere consapevole dei rischi che le scelte di esternalizzazione comportano e mettere in atto misure adeguate per il loro contenimento.

Nell'elaborazione del modello architetturale e delle strategie di *sourcing* (Sezione II), vanno considerate soluzioni tese a contenere il grado di dipendenza da fornitori e partner tecnologici (c.d. *vendor lock-in*), salvaguardando la possibilità di sostituire la fornitura con un'altra funzionalmente equivalente (ad es. privilegiando il ricorso a standard aperti per le connessioni, lo scambio di dati, la cooperazione applicativa) e prevedendo opportune *exit strategies* ([26]).

Nella scelta del fornitore l'intermediario deve esercitare un'appropriata *due diligence*, con specifico riguardo alla solidità finanziaria, all'economicità della fornitura nonché alla maturità e diffusione, in un adeguato orizzonte temporale, del prodotto in esame. Il mantenimento nel tempo da parte del fornitore delle condizioni necessarie a fornire un servizio adeguato e conforme alle norme va assicurato attraverso idonei strumenti contrattuali e procedure di controllo.

2. Accordi con i fornitori e altri requisiti

All'esternalizzazione di sistemi e servizi ICT si applicano, per quanto non diversamente disposto dal presente paragrafo, le disposizioni in materia di outsourcing di funzioni aziendali contenute nel Capitolo 7, Sezione IV.

La comunicazione preventiva deve inoltre essere effettuata almeno 30 giorni prima di conferire l'incarico anche in tutti i casi in cui un fornitore ha sede in Italia ma utilizzi, anche attraverso subfornitori, *data center* in paesi diversi da quest'ultimo. Entro 30 giorni dal ricevimento della comunicazione la Banca d'Italia può avviare un procedimento amministrativo d'ufficio di divieto dell'esternalizzazione che si conclude entro 60 giorni.

Nei contratti con i fornitori di sistemi e servizi ICT, in aggiunta alle richiamate disposizioni, devono essere disciplinati i seguenti aspetti:

– l'obbligo per l'outsourcer di osservare la policy di sicurezza informatica aziendale, per quanto di pertinenza; nello specifico, il fornitore deve provvedere al trattamento dei dati in accordo con il loro livello di classificazione - con particolare riferimento al profilo della riservatezza;

([26]) Anche l'acquisizione di licenze software per prodotti installati sui propri sistemi, a supporto ad importanti processi aziendali trasversali, può introdurre forme di dipendenza dal fornitore, a seguito di vincoli tecnologici o contrattuali che rendano necessario avvalersi del fornitore o di società collegate per la manutenzione o rendano molto dispendiosa la sostituzione del prodotto. Di tali aspetti va tenuto conto nel processo di selezione delle soluzioni software.

- la proprietà di dati, software e altre risorse informatiche, con esclusiva per l'intermediario dei dati inerenti la clientela e i servizi ad essa forniti;
- la periodica produzione e messa a disposizione dell'intermediario delle opportune copie di backup di dati (database, transazioni, log applicativi e di sistema);
- la ripartizione dei compiti e delle responsabilità attinenti i presidi di sicurezza necessari per la tutela di dati, applicazioni e sistemi, con particolare riferimento ai rischi di attacchi interni ed esterni, anche attraverso Internet;
- la definizione di livelli di servizio in coerenza con le esigenze di sicurezza delle applicazioni e dei processi aziendali che si avvalgono dei servizi esternalizzati, anche con riferimento agli eventuali livelli di servizio definiti dall'intermediario per dette applicazioni e servizi;
- la possibilità per l'intermediario di conoscere la localizzazione dei *data center* e l'elenco del personale che ha accesso ai propri dati ed applicazioni, con obbligo per l'outsourcer di tempestiva notifica di qualsiasi variazione a riguardo ([27]);
- l'obbligo per l'outsourcer, una volta concluso il rapporto contrattuale, di eliminare – facendo uso di opportuni strumenti e capacità tecniche, debitamente documentati - qualsiasi copia o stralcio di dati riservati di proprietà dell'intermediario presente su propri sistemi o supporti, in modo da escludere la possibilità tecnica di accessi successivi a dati dell'intermediario da parte del proprio personale o di terzi.

3. Indicazioni particolari

L'intermediario deve porre particolare cautela nella valutazione di offerte di servizi in outsourcing erogati secondo il modello del *cloud computing*, che prevede la fruizione delle risorse informatiche nella forma di servizi accessibili via rete e configurabili in modo flessibile.

Sono presenti diverse tipologie di implementazione:

- *privato:* si tratta di ambienti interni a una società o gruppo che permettono la condivisione delle risorse tra più aree aziendali e il mantenimento dei dati all'interno della struttura; questo caso non rientra nella definizione di servizio esternalizzato;
- community*:* i servizi sono utilizzati da un ristretto numero di organizzazioni clienti che condividono analoghe necessità e obiettivi. La condivisione delle risorse informatiche è ristretta a dette organizzazioni;
- *pubblico:* i servizi sono erogati a un vasto numero di utenti e le funzionalità sono offerte in maniera aperta e condivisa. I fornitori in genere sfruttano la possibilità di condividere in modo flessibile le proprie risorse tra i diversi utenti e applicano di norma tariffe proporzionali all'utilizzo (approccio *pay-per-use*).

Nel caso dell'acquisizione di servizi in *community* o pubblici i maggiori rischi potenziali possono richiedere una più elevata complessità del sistema di controlli da predisporre. Va valutata nello specifico la capacità del fornitore di garantire il rispetto dei requisiti richiesti e di assicurare la piena ricostruzione degli accessi e delle modifiche effettuate sui dati, anche nel contesto di verifiche ispettive.

([27]) Cfr. il Provvedimento del Garante per la protezione dei dati personali del 27 novembre 2008 "Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema"**.**

Box 5

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*.

Allegato A
Documenti aziendali per la gestione e il controllo dell'ICT

Documento	*Approvazione*	*Aggiornamento*	*Note*
DOCUMENTI DI POLICY E STANDARD AZIENDALI			
Documento di indirizzo strategico per l'ICT	Organo con funzione di supervisione strategica	In dipendenza della periodicità dei piani strategici aziendali (3 – 5 anni)	Contiene (cfr. Sezione II par. I): - modello di riferimento architetturale; - strategie di *sourcing* - livello di tolleranza al rischio informatico
Metodologia di analisi del rischio informatico	Organo con funzione di supervisione strategica	In base alle necessità	
Policy di sicurezza ICT	Organo con funzione di supervisione strategica	In base alle necessità	
Organigramma della funzione ICT	Organo con funzione di supervisione strategica	In base alle necessità	Include il disegno dei processi di gestione dell'ICT (cfr. Sezione II par. 2)
Standard di data governance	Organo con funzioni di gestione	Periodicità definita	
ALTRI DOCUMENTI ESSENZIALI PER LA GESTIONE E LO SVILUPPO DEI SISTEMI ICT			
Procedura di gestione dei cambiamenti	Organo con funzione di gestione	In base alle necessità	
Procedura di gestione degli incidenti	Organo con funzione di gestione	In base alle necessità	
Piano operativo	Organo con funzione di gestione	Annuale	
VALUTAZIONI AZIENDALI			
Rapporto sintetico su valore e costi dell'ICT	Organo con funzione di supervisione strategica	Annuale	
Rapporto sintetico sulla situazione rischio informatico	Organo con funzione di supervisione strategica	Annuale	
Rapporti dell'internal audit e delle altre funzioni responsabili della valutazione della sicurezza	Organo con funzione di supervisione strategica	Almeno annuale	

Allegato B
Misure in materia di servizi telematici per la clientela

(e-banking e altri servizi elettronici di pagamento)

I servizi telematici di consultazione e gestione dei conti da parte della clientela e i servizi di pagamento elettronico via internet sono particolarmente esposti al rischio di frodi informatiche.

Per prevenire e monitorare tali rischi, in aggiunta a quanto specificato alla Sezione III del presente capitolo, gli intermediari devono tenere conto delle seguenti indicazioni.

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

Al fine di attenuare i rischi di frodi e abusi commessi attraverso falsi siti web che replicano l'apparenza di siti di intermediari, devono essere resi disponibili ai clienti appropriati strumenti per riconoscere i siti web utilizzati per l'erogazione di servizi telematici e per verificarne l'autenticità (ad es. nomi di dominio che rispecchiano la denominazione dell'intermediario, certificati digitali emessi da una riconosciuta autorità di certificazione a nome dell'intermediario). Il canale di comunicazione telematica tra intermediario e cliente deve essere cifrato – mediante robuste soluzioni tecnologiche – senza soluzione di continuità (modalità *end-to-end*), ogni qualvolta siano scambiati dati personali o comunque riservati, ovvero si acceda a funzioni dispositive.

2. Procedura di autenticazione del cliente

Per minimizzare i rischi di furto di identità ([28]), l'accesso del cliente a funzionalità di consultazione o l'attivazione di operazioni su rapporti in essere con l'intermediario devono essere soggetti ad una idonea procedura di autenticazione; almeno con riferimento all'operatività a carattere dispositivo, tale procedura deve fare ricorso a sistemi di autenticazione a più fattori tra loro indipendenti ("autenticazione forte").

L'autenticazione forte (o multi fattore) prevede l'utilizzo, insieme a un codice identificativo (userID), di non meno di due fattori indipendenti individuati tra "qualcosa che si conosce" (ad es. un PIN o una password), "qualcosa che si possiede" (ad es. una smart card o un token che genera password non riutilizzabili) e "qualcosa che si è" (ad es. caratteristiche biometriche). L'indipendenza dei fattori deve garantire che un'eventuale vulnerabilità o violazione di sicurezza di uno di essi non influenzi l'efficacia degli altri.

3. Autorizzazione e monitoraggio delle transazioni di pagamento

L'intermediario deve disporre di procedure per assicurare che ogni transazione di pagamento sia eseguita solo previa autorizzazione da parte dell'utente.

Inoltre, sulla base dei rischi ravvisati, le transazioni devono essere soggette a idonee procedure (assistite da sistemi di monitoraggio) in modo che l'intermediario sia in grado di rilevare tempestivamente anomalie rispetto al normale comportamento dell'utente e al regolare funzionamento del sistema, assumendo prontamente eventuali iniziative di contrasto.

([28]) Per "furto di identità" si intende il comportamento fraudolento di chi, con varie tecniche ed espedienti, sottrae le credenziali di accesso o altre informazioni personali di un utente per spacciarsi per questi nell'ambito di un'applicazione informatica.

4. Sensibilizzazione della clientela

I clienti devono essere posti in grado di utilizzare gli strumenti di autenticazione, eseguire la procedura di accesso e avvalersi delle funzionalità di e-banking e di pagamento elettronico in modo sicuro. L'intermediario, oltre a informare correntemente la clientela sugli strumenti e procedure di sicurezza disponibili, valuta l'opportunità di avviare programmi di sensibilizzazione ed educazione all'utilizzo degli strumenti informatici.

Titolo V – Capitolo 9
DISPOSIZIONI IN MATERIA DI CONTINUITÀ OPERATIVA

1. Destinatari della disciplina

I soggetti destinatari, indicati nel testo con il nome collettivo di “intermediari”, sono:

- le banche e i gruppi bancari;
- i sistemi di pagamento e i relativi fornitori di servizi tecnologici; le controparti centrali, le società di gestione accentrata di strumenti finanziari, i gestori di sistemi di riscontro e rettifica giornaliera e società che forniscono servizi di compensazione e liquidazione su strumenti finanziari; i mercati regolamentati all’ingrosso su titoli di Stato, i sistemi multilaterali all’ingrosso su titoli di Stato e i sistemi multilaterali di scambio di depositi in euro.

2. Premessa

La crescente complessità dell'attività finanziaria, l'intenso utilizzo della tecnologia dell'informazione e i nuovi scenari di rischio hanno messo in evidenza l'esigenza che gli intermediari, nell’ambito della gestione dei rischi operativi, adeguino le strategie in tema di sicurezza e rafforzino i presidi di emergenza in modo da garantire adeguati livelli di continuità operativa.

I piani di emergenza devono prevedere soluzioni, non solo basate su misure tecnico-organizzative finalizzate alla salvaguardia degli archivi elettronici e al funzionamento dei sistemi informativi, ma che considerino anche ipotesi di crisi estesa e blocchi prolungati delle infrastrutture essenziali in modo da assicurare la continuità operativa dell'azienda in caso di eventi disastrosi.

In relazione a ciò, gli intermediari devono adottare un approccio esteso che, partendo dalla identificazione dei processi aziendali critici, definisca per ciascuno di essi presidi organizzativi e misure di emergenza commisurati ai livelli di rischio.

Per prevenire l'insorgere di rischi sistemici occorre inoltre elevare e uniformare la qualità delle soluzioni di emergenza dei maggiori operatori, in particolare nei comparti dei servizi di pagamento e dell'accesso ai mercati finanziari, anche attraverso iniziative di cooperazione tra intermediari.

Per la prevenzione del rischio sistemico la Banca d’Italia si riserva di chiedere ad alcuni intermediari l'attivazione di misure di emergenza più rigorose.

3. Definizioni

La gestione della continuità operativa comprende tutte le iniziative volte a ridurre a un livello ritenuto accettabile i danni conseguenti a incidenti e catastrofi che colpiscono direttamente o indirettamente un'azienda.

Il piano aziendale di continuità operativa, nel seguito denominato anche piano di emergenza, è il documento che formalizza i principi, fissa gli obiettivi e descrive le procedure per la gestione della continuità operativa dei processi aziendali critici.

Il piano di *disaster recovery* stabilisce le misure tecniche e organizzative per fronteggiare eventi che provochino la indisponibilità dei centri di elaborazione dati. Il piano, finalizzato a consentire il funzionamento delle procedure informatiche rilevanti in siti

alternativi a quelli di produzione, costituisce parte integrante del piano di continuità operativa.

4. Ambito del piano di continuità operativa

Gli intermediari definiscono un piano di continuità operativa per la gestione di situazioni critiche conseguenti sia a incidenti di portata settoriale sia a catastrofi estese che colpiscono l'azienda o le sue controparti rilevanti (altre società del gruppo; principali fornitori; clientela primaria; specifici mercati finanziari; istituzioni di regolamento, compensazione e garanzia).

Per i gruppi bancari, i piani di continuità possono essere definiti e gestiti in modo accentrato per l'intero gruppo o decentrato per singola società; in ogni caso la capogruppo assicura che tutte le controllate siano dotate di piani di continuità operativa e verifica la coerenza degli stessi con gli obiettivi strategici del gruppo in tema di contenimento dei rischi.

Laddove alcuni processi critici siano svolti da soggetti specializzati appartenenti al gruppo (ad es. allocazione della funzione informatica o del *back-office* presso una società strumentale), i relativi presidi di emergenza costituiscono parte integrante dei piani di continuità degli intermediari.

Il piano si inquadra nella complessiva politica aziendale sulla sicurezza e tiene conto delle vulnerabilità esistenti e delle misure preventive poste in essere per garantire il raggiungimento degli obiettivi aziendali.

Il piano prende in considerazione almeno i seguenti scenari di crisi:

- distruzione o inaccessibilità di strutture nelle quali sono allocate unità operative o apparecchiature critiche;
- indisponibilità di personale essenziale per il funzionamento dell'azienda;
- interruzione del funzionamento delle infrastrutture (tra cui energia elettrica, reti di telecomunicazione, reti interbancarie, mercati finanziari);
- alterazione dei dati o indisponibilità dei sistemi a seguito di attacchi perpetrati dall'esterno attraverso reti telematiche;
- danneggiamenti gravi provocati da dipendenti.

5. Correlazione ai rischi

L'analisi di impatto, preliminare alla stesura del piano di emergenza e periodicamente aggiornata, individua il livello di rischio relativo ai singoli processi aziendali e pone in evidenza le conseguenze della interruzione del servizio. I rischi residui, non gestiti dal piano, sono documentati ed esplicitamente accettati dall’intermediario. L'allocazione delle risorse e le priorità di intervento sono correlate al livello di rischio.

L'analisi di impatto tiene conto dei parametri caratteristici della struttura organizzativa e dell'operatività aziendale, tra cui:

- le specificità – in termini di probabilità di catastrofe – connesse con la localizzazione dei siti rilevanti (ad es. sismicità dell'area, dissesto idrogeologico del territorio, vicinanza ad insediamenti industriali pericolosi, prossimità ad aeroporti o a istituzioni con alto valore simbolico);

- i profili di concentrazione geografica (ad es. presenza di una pluralità di operatori nei centri storici di grandi città);
- la complessità dell'attività tipica o prevalente e il grado di automazione raggiunto;
- le dimensioni aziendali e l'articolazione territoriale dell'attività;
- il livello di esternalizzazione di funzioni rilevanti (ad es. *outsourcing* del sistema informativo o del *back-office*);
- l'assetto organizzativo in termini di accentramento o decentramento di processi critici;
- i vincoli derivanti da interdipendenze, anche tra e con fornitori, clienti, altri intermediari.

L'analisi di impatto prende in considerazione, oltre ai rischi operativi, anche gli altri rischi (ad es. di mercato e di liquidità).

6. Definizione del piano e gestione dell'emergenza

6.1 I processi critici

Gli intermediari identificano in modo circostanziato i processi che, per la rilevanza dei danni conseguenti alla loro indisponibilità, necessitano di elevati livelli di continuità operativa da conseguire mediante misure di prevenzione e con soluzioni di emergenza da attivare in caso di incidente.

A tal fine vengono considerati con particolare attenzione i processi che attengono alla gestione dei rapporti con la clientela, ivi incluse imprese e pubbliche amministrazioni, e alla registrazione dei fatti contabili.

Per ciascun processo critico sono individuati il responsabile, le procedure informatiche di supporto, il personale addetto, le strutture logistiche interessate, le infrastrutture tecnologiche e di comunicazione utilizzate.

Il responsabile del processo 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.

6.2 La responsabilità del piano

La responsabilità dello sviluppo, della manutenzione e delle verifiche del piano di emergenza è affidata a un esponente aziendale con posizione gerarchico – funzionale adeguata.

Il piano attribuisce l'autorità di dichiarare lo stato di emergenza e stabilisce la catena di comando incaricata di gestire l'azienda in circostanze eccezionali. La policy aziendale in tema di *incident management* prevede la comunicazione degli incidenti e dei fatti anomali rilevanti alle strutture preposte alla dichiarazione dello stato di emergenza.

Sono esplicitamente individuati i membri della struttura preposta alla gestione della crisi (ad es. comitato di crisi), il responsabile della stessa struttura, le modalità interne di comunicazione e le responsabilità attribuite alle funzioni aziendali interessate.

Le unità operative coinvolte nei processi critici individuano i responsabili di settore del piano di emergenza. Essi coordinano, per gli aspetti di competenza, i lavori per la definizione del piano, per l'attuazione delle misure previste nello stesso e per la conduzione delle verifiche.

Prima della attivazione di nuovi sistemi o processi operativi, i responsabili di settore definiscono le opportune modifiche del piano.

6.3 Il contenuto del piano

Il piano di continuità documenta le modalità per la dichiarazione dello stato di emergenza, l'organizzazione e le procedure da seguire in situazione di crisi, l'iter per la ripresa della normale operatività.

Il piano stabilisce il tempo massimo accettabile di ripartenza di sistemi e processi critici.

Il piano individua i siti alternativi, prevede spazi e infrastrutture logistiche e di comunicazione adeguate per il personale coinvolto nell'emergenza, stabilisce le regole di conservazione delle copie dei documenti importanti (ad es. contratti) in luoghi remoti rispetto ai documenti originali.

Con riferimento ai sistemi informativi centrali e periferici, il piano fornisce indicazioni su modalità e frequenza di generazione delle copie degli archivi di produzione e sulle procedure per il ripristino presso i sistemi secondari.

La frequenza dei *back-up* è correlata al volume di operatività dell'intermediario; gli archivi di produzione sono duplicati almeno giornalmente. Sono assunte cautele per il tempestivo trasporto e la conservazione delle copie elettroniche in siti ad elevata sicurezza fisica posti in luoghi remoti rispetto ai sistemi di produzione.

Nel caso di sistemi secondari *off-line*, in cui non siano presenti archivi di dati ovvero questi non siano allineati in tempo reale ai dati di produzione, sono definite modalità e tempi di allineamento alla situazione corrente al momento dell'interruzione.

Il piano definisce le modalità di comunicazione con la clientela, le controparti rilevanti, le Autorità e i media.

Gli intermediari che ricorrono a terzi per i servizi di continuità operativa definiscono con i fornitori livelli di servizio adeguati al conseguimento degli obiettivi aziendali. Nel caso in cui il fornitore abbia impegnato le stesse risorse per fornire analoghi servizi ad altre aziende, in particolare se situate nella stessa zona, sono stabilite cautele contrattuali per evitare il rischio che, in caso di esigenze concomitanti di altre organizzazioni, le prestazioni degenerino o il servizio si renda di fatto indisponibile.

Il contratto stipulato con il fornitore consente all'intermediario di utilizzare il sito secondario per periodi prolungati, fino al pieno ripristino del sito primario.

6.4 Le verifiche

Le verifiche delle misure di emergenza sono correlate ai rischi e alle criticità dei processi; di conseguenza sono 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 viene svolta una verifica complessiva, il più possibile realistica, del ripristino della operatività in 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.

In particolare, le verifiche annuali dei sistemi informativi devono prevedere l'attivazione dei collegamenti di rete presso il sito secondario, l'esecuzione delle procedure *batch* e – per le banche - l'operatività *on-line* di almeno una succursale.

I risultati delle verifiche sono documentati per iscritto, portati all'attenzione dell'organo con funzione di gestione e inviati, per le parti di competenza, alle unità operative coinvolte e alla funzione di audit. A fronte di carenze riscontrate nelle prove sono tempestivamente avviate le opportune azioni correttive.

6.5 Le risorse umane

Il piano individua il personale essenziale per assicurare la continuità dei processi critici e fornisce allo stesso indicazioni sulle località da raggiungere e sulle attività da porre in essere in caso di emergenza.

Le procedure di emergenza sono chiare e dettagliate, in modo da poter essere eseguite anche da risorse non esperte.

Il personale coinvolto nel piano è addestrato sulle misure di emergenza, dispone della lista di contatto e della documentazione necessaria per operare in situazione di crisi, ha dimestichezza con i siti secondari e con le apparecchiature in essi contenute, partecipa alle sessioni di verifica delle misure di emergenza.

Va valutata l'opportunità di frazionare l'attività connessa con i processi critici in più siti ovvero di organizzare il lavoro del personale su turni.

6.6 Infrastrutture e controparti rilevanti

Il piano di continuità considera l'eventualità che le principali infrastrutture tecnologiche e finanziarie e le controparti rilevanti siano colpiti da un evento calamitoso e stabilisce le misure per gestire i problemi conseguenti; la capacità di comunicare con i siti secondari di tali soggetti è verificata periodicamente.

Per i servizi essenziali all'operatività dell’intermediario, va valutata la possibilità di ricorrere a fornitori alternativi.

6.7 Controlli

Fermo restando quanto stabilito con riguardo ai controlli di competenza della funzione di revisione interna, gli intermediari considerano l'opportunità di sottoporre il piano di emergenza alla revisione da parte di competenti terze parti indipendenti.

6.8 Comunicazioni alla Banca d’Italia

In caso di incidente grave che ne comprometta il normale funzionamento, l'intermediario informa tempestivamente la Banca d'Italia e fornisce valutazioni circa l'impatto dell'evento sulla operatività delle strutture centrali e periferiche e sui rapporti con la clientela e le controparti.

7. Requisiti particolari

L'operatività del sistema finanziario nel suo complesso si basa sul corretto funzionamento delle infrastrutture tecnologiche e finanziarie e sulla capacità dei maggiori operatori di erogare i servizi essenziali nei comparti dei sistemi di pagamento e dell'accesso ai mercati finanziari.

A tali soggetti la Banca d'Italia può chiedere il rispetto di requisiti di continuità operativa più stringenti rispetto a quelli previsti per la generalità degli intermediari, in

particolare con riferimento ai tempi massimi di ripristino dei processi a rilevanza sistemica, alla localizzazione dei siti secondari, alle risorse previste per gestire le situazioni di emergenza.

La Banca d'Italia individua nominativamente i soggetti ai quali si applicano i requisiti particolari, concorda con loro gli adeguamenti dei piani di continuità operativa, verifica le soluzioni adottate.

I requisiti particolari per la continuità operativa previsti dalle presenti disposizioni si applicano a:

a) Gruppi bancari e banche non appartenenti a gruppi con una quota di mercato, calcolata sui fondi intermediati, superiore al 5 per cento del totale del sistema bancario. Nell'ambito dei gruppi bancari, i requisiti particolari si applicano alla capogruppo, alle controllate bancarie italiane con fondi intermediati superiori a 5 miliardi di euro e alle altre controllate bancarie, finanziarie e strumentali che, indipendentemente dalla dimensione e localizzazione (quindi anche estera), svolgono in misura rilevante o danno un supporto essenziale ai processi a rilevanza sistemica; altri intermediari, incluse le succursali italiane di banche estere, con una quota di mercato superiore al 5 per cento in almeno uno dei seguenti segmenti del mercato finanziario italiano: Target 2, Express II, servizi di controparte centrale, e-Mid, aste BCE, operazioni di finanziamento del Tesoro effettuate tramite asta, MTS (comparto pronti contro termine), pagamento delle pensioni sociali, bollettini postali.

   Nel caso di soggetti appartenenti a gruppi bancari, vengono identificate le società del gruppo alle quali si applicano i requisiti particolari; la capogruppo coordina le iniziative necessarie per il raggiungimento degli obiettivi concordati con la Vigilanza.

b) Sistemi di pagamento e relativi fornitori di servizi tecnologici che forniscono: servizi di regolamento lordo del contante (Target 2); servizi di erogazione del contante tramite terminale ATM (Bancomat); servizi di gestione delle infrastrutture telematiche di supporto ad applicazioni e servizi rientranti nell'ambito della "Convenzione per la partecipazione al Sistema per la trasmissione telematica di dati" (SITRAD).

c) Controparti centrali, società di gestione accentrata di strumenti finanziari, gestori di sistemi di riscontro e rettifica giornaliera e società che forniscono servizi di compensazione e liquidazione su strumenti finanziari.

d) Mercati regolamentati all'ingrosso su titoli di Stato, sistemi multilaterali all'ingrosso su titoli di Stato e sistemi multilaterali di scambio di depositi in euro.

In relazione a ciò, sono: individuati i processi ad alta criticità da proteggere ("processi a rilevanza sistemica"); definite le misure aggiuntive per la loro continuità operativa ("requisiti particolari"); stabiliti i parametri di riferimento per l'individuazione degli intermediari soggetti a tali requisiti particolari.

7.1 Processi a rilevanza sistemica

I processi ad alta criticità nel sistema finanziario italiano che, per un "effetto domino", possono provocare il blocco dell'operatività dell'intera piazza finanziaria nazionale si concentrano nei sistemi di pagamento e nelle procedure per l'accesso ai mercati finanziari.

Tali processi vengono denominati, ai fini delle presenti disposizioni, "processi a rilevanza sistemica" per la continuità operativa del sistema finanziario italiano. Si tratta di un complesso strutturato di attività finalizzate all'erogazione dei seguenti servizi:

- servizi connessi con i sistemi di regolamento lordo in moneta di banca centrale e con i sistemi di gestione accentrata, compensazione, garanzia e liquidazione degli strumenti finanziari. Sono inclusi: Target 2, Express II, gestione accentrata di strumenti finanziari, sistemi di riscontro e rettifica giornalieri, servizi di controparte centrale;
- servizi connessi con l'accesso ai mercati rilevanti per regolare la liquidità del sistema finanziario. Sono inclusi: mercato interbancario dei depositi (e-Mid), aste BCE, operazioni di finanziamento del Tesoro effettuate tramite asta, MTS (comparto pronti contro termine);
- servizi di pagamento al dettaglio a larga diffusione tra il pubblico. Sono inclusi: bollettini postali, pagamento delle pensioni sociali, erogazione del contante;
- servizi strettamente funzionali al soddisfacimento di fondamentali esigenze di liquidità degli operatori economici, il cui blocco ha rilevanti effetti negativi sull'operatività degli stessi. Sono inclusi: servizi di gestione delle infrastrutture telematiche per l'erogazione del contante tramite terminale ATM (Bancomat) e di supporto ad applicazioni e servizi rientranti nell'ambito della "Convenzione per la partecipazione al Sistema per la trasmissione telematica di dati" (SITRAD).

7.2 Responsabilità

Per i gruppi bancari, la capogruppo promuove e coordina l'attuazione degli interventi di adeguamento dei piani di continuità operativa relativi ai processi a rilevanza sistemica e garantisce nel continuo il rispetto dei requisiti particolari da parte di tutte le controllate interessate. Nomina un responsabile unico di tali attività, con competenze estese all'intero gruppo.

Per le succursali italiane di banche estere, il coordinamento del piano di continuità operativa relativo ai processi a rilevanza sistemica è assicurato dalle succursali stesse, in stretto raccordo con le strutture che gestiscono la continuità operativa a livello centrale o di area geografica.

Per sistemi di pagamento e relativi fornitori di servizi tecnologici, controparti centrali, società di gestione accentrata di strumenti finanziari, gestori di sistemi di riscontro e rettifica giornaliera e società che forniscono servizi di compensazione e liquidazione su strumenti finanziari, mercati regolamentati all'ingrosso su titoli di Stato, sistemi multilaterali all'ingrosso su titoli di Stato e sistemi multilaterali di scambio di depositi in euro, l'intermediario promuove e coordina l'attuazione degli interventi di adeguamento dei piani di continuità operativa relativi ai processi a rilevanza sistemica e garantisce nel continuo il rispetto dei requisiti particolari e nomina un responsabile unico di tali attività.

7.3 Scenari di rischio

Gli scenari di rischio rilevanti per la continuità operativa dei processi a rilevanza sistemica sono documentati e costantemente aggiornati; essi includono ipotesi di distruzioni fisiche su larga scala, a dimensione metropolitana o superiore, di infrastrutture essenziali dell'intermediario e di terzi nonché situazioni di crisi gravi anche non connesse ad eventi con distruzioni materiali (ad es. pandemie, attacchi biologici).

7.4 Siti di recovery

I siti di recovery dei processi a rilevanza sistemica sono situati a congrua distanza dai siti primari in modo da assicurare un elevato grado di indipendenza tra i due insediamenti.

In generale, i siti di recovery sono ubicati all'esterno dell'area metropolitana nella quale sono presenti i siti primari; inoltre, essi utilizzano servizi (telecomunicazioni, energia, acqua, ecc.) distinti da quelli impiegati in produzione. Laddove ciò non avvenga è necessaria una valutazione rigorosa, supportata da pareri di parti terze qualificate (ad es. Protezione Civile, accademici, professionisti) e compiutamente documentata, che il rischio di indisponibilità contemporanea dei siti primari e secondari è trascurabile.

I siti di recovery dei sistemi informativi sono configurati con capacità adeguata, all'occorrenza, a gestire volumi di attività attestati sui picchi massimi riscontrati nel corso dell'operatività ordinaria.

7.5 Tempi di ripristino e percentuali di disponibilità

Il tempo di ripristino dei processi a rilevanza sistemica in caso di incidente è contenuto:

a) per banche e gruppi bancari: entro 4 ore dalla dichiarazione dello stato di crisi;

b) per sistemi di pagamento e relativi fornitori di servizi tecnologici: entro 2 ore dalla dichiarazione dello stato di crisi;

c) per controparti centrali, società di gestione accentrata di strumenti finanziari, gestori di sistemi di riscontro e rettifica giornaliera e società che forniscono servizi di compensazione e liquidazione su strumenti finanziari: entro 2 ore dalla dichiarazione dello stato di crisi;

d) per mercati regolamentati all'ingrosso su titoli di Stato, sistemi multilaterali all'ingrosso su titoli di Stato e sistemi multilaterali di scambio di depositi in euro: entro 4 ore dalla dichiarazione dello stato di crisi.

Per i processi a rilevanza sistemica, di concerto con le Autorità, gli intermediari stabiliscono parametri obiettivo relativi alla disponibilità dei servizi.

Con riferimento ai sistemi informativi, sono considerate adeguate le soluzioni basate su architetture tecnologiche che effettuano la duplicazione in linea dei dati operativi in modo da eliminare o ridurre al minimo la perdita di informazioni (cioè *recovery point objective* pari o prossimo a zero).

Nel caso in cui il disastro comporti un blocco dei servizi essenziali ovvero si registri una situazione di gravi danni o di serio pericolo sul lato umano, è possibile che gli obiettivi sopra enunciati subiscano un adattamento, in via straordinaria, sulla base delle indicazioni fissate nelle sedi nazionali di coordinamento della crisi. É importante che sia prevista, anche in queste situazioni estreme, una ripartenza più immediata possibile dei processi a rilevanza sistemica, anche attraverso procedure d'emergenza a bassa integrazione nei processi aziendali (ad es. mediante l'utilizzo di PC offline, fax, contatti telefonici con controparti selezionate) per gestire le esigenze essenziali di liquidità. In ogni caso, anche le citate soluzioni di emergenza devono essere adeguatamente presidiate dal punto di vista della sicurezza. L'eventuale perdita di dati, in questi casi eccezionali, va contenuta indicativamente entro le quattro ore precedenti la dichiarazione dello stato di crisi e devono essere predisposti adeguati meccanismi procedurali, atti a consentire la tempestiva ripresa delle transazioni perse e a minimizzare il rischio di elaborazioni duplicate o errate.

7.6 Risorse

Sono individuate e documentate le risorse – umane, tecnologiche e logistiche – necessarie per l'operatività dei processi a rilevanza sistemica. Occorre garantire – con misure organizzative, mediante accordi con terzi, con la duplicazione del personale o con altri provvedimenti documentati – la presenza nei siti di *recovery*, all'occorrenza, del personale necessario per l'operatività dei processi a rilevanza sistemica. Va evitata la concentrazione, nello stesso luogo e allo stesso tempo, del personale chiave.

7.7 Verifiche

Sono effettuate, con frequenza almeno annuale, verifiche accurate dei presidi di continuità operativa dei processi a rilevanza sistemica. Viene assicurata la partecipazione attiva ai test di sistema organizzati o promossi dalle Autorità, dai mercati e dalle principali infrastrutture finanziarie.

8. Comunicazioni alla Banca d'Italia

Il piano di continuità operativa dei processi a rilevanza sistemica, inclusi gli adeguamenti e le integrazioni, viene prontamente trasmesso alla Banca d'Italia.

9. Disposizioni abrogate

Dall'entrata in vigore delle presenti disposizioni sono abrogate le seguenti disposizioni:

– *Disposizioni di vigilanza – Continuità operativa in casi di emergenza* (Comunicazione del luglio 2004);

– *Disposizioni di vigilanza – Requisiti particolari per la continuità operativa dei processi di rilevanza sistemica* (Comunicazione del marzo 2007).