

Il presente documento è conforme all'originale contenuto negli archivi della Banca d'Italia

Firmato digitalmente da



BANCA D'ITALIA
EUROSISTEMA

Disposizioni di vigilanza per le banche

Circolare n. 285 del 17 dicembre 2013



RIEPILOGO DEGLI AGGIORNAMENTI

1° Aggiornamento del 6 maggio 2014

Parte Prima. Inserito un nuovo Titolo IV “Governo societario, controlli interni, gestione dei rischi” con il Cap. 1 “Governo societario”.

2° Aggiornamento del 21 maggio 2014

Parte Prima, Titolo I. Inseriti due nuovi capitoli: “Gruppi bancari” (Cap. 2) e “Albo delle banche e dei gruppi bancari” (Cap. 4). **Parte Terza, Capitolo 1.** Nella Sez. I, al paragrafo 5 è aggiunto un nuovo procedimento amministrativo. Nella Sez. V sono modificati il secondo e il terzo capoverso del paragrafo 2 ed è aggiunta una nota; al paragrafo 3 è modificato il quarto capoverso e sono inseriti due ultimi capoversi ed una nota.

3° Aggiornamento del 27 maggio 2014

Inserita una nuova Parte Quarta con il Capitolo 1 “Bancoposta”.

4° Aggiornamento del 17 giugno 2014

Ristampa integrale per incorporare i primi tre aggiornamenti nel testo iniziale; le pagine sono state rinumerate per capitolo. **Parte Prima, Titolo III.** Inserito un nuovo capitolo (Capitolo 2) “Informativa al pubblico Stato per Stato”. **Parte Seconda, Capitolo 4.** Nella Sezione III, par. 2 sono stati precisati i riferimenti temporali di efficacia della discrezionalità nazionale; nella Sezione IV, il par. 4 è stato coordinato con l’Allegato A. **Parte Seconda, Capitolo 10, Sezione IV, par. 1.** Precisate le linee di orientamento sulla verifica della connessione fra soggetti. **Parte Terza.** Inserito un nuovo capitolo (Capitolo 2) “Comunicazioni alla Banca d’Italia”. **Indice.** Modificato per includere i nuovi inserimenti. **Premessa.** Modificata per effetto dei nuovi inserimenti. **Disposizioni introduttive.** Inserito un nuovo paragrafo concernente i procedimenti amministrativi; modificate nel resto della Circolare le parti ad essi relative. **Ambito di applicazione.** Modificato per effetto dei nuovi inserimenti; nella Sezione II è stato precisato il par. 2.

5° Aggiornamento del 24 giugno 2014

Ristampa integrale. **Parte Terza.** Inserito un nuovo capitolo (Capitolo 3) “Obbligazioni bancarie garantite”. **Indice.** Modificato per includere il nuovo inserimento. **Ambito di applicazione.** Modificato per effetto del nuovo inserimento.

6° Aggiornamento del 4 novembre 2014

Ristampa integrale per adeguamento all’avvio del Meccanismo di vigilanza unico (4 novembre 2014). Pagine modificate: **Indice.**1,2,6,8; **Premessa.**1-4; **Disposizioni introduttive.**2,4,7-8,10,12,13,15,20,22; **Parte Prima.**I.1.1-2,7-14,17; **Parte Prima.**I.2.1-2; **Parte Prima.**I.3.1-2,4-8; **Parte Prima.**I.4.3; **Parte Prima.**I.5.1-5,7; **Parte Prima.**I.6.1,4-5; **Parte Prima.**II.1.2-3,6-7,15,17-18; **Parte Prima.**III.1.1-4,6-9,12-14,16-21; **Parte Prima.**III.2.1; **Parte Prima.**IV.1.2-5, 7, 18, 28; **Parte Seconda.**1.1-2,8, 11; **Parte Seconda.**2.1; **Parte Seconda.**1.3.1,4; **Parte Seconda.**1.4.1-3,5,8-10; **Parte Seconda.**5.1; **Parte Seconda.**1.6.1-2,11-12; **Parte Seconda.**1.7.1,4; **Parte Seconda.**1.8.1; **Parte Seconda.**1.9.1; **Parte Seconda.**1.10.1,10; **Parte Seconda.**1.11.1-2,4-5; **Parte Seconda.**1.12.1; **Parte Seconda.**1.13.1; **Parte Seconda.**1.14.1-2,7; **Parte Terza.**1.3.

7° Aggiornamento del 18 novembre 2014

Parte Prima, Titolo IV. Inserito un nuovo Capitolo 2 “Politiche e prassi di remunerazione e incentivazione”.

8° Aggiornamento del 10 marzo 2015

Ristampa integrale per incorporare il 7° aggiornamento (**Parte Prima, Titolo IV, Capitolo 2**). **Premessa:** pagine modificate: 2, 3. **Parte Seconda, Capitolo 6:** pagine modificate: 1-3, 5-12; inserita una nuova Sezione (Sezione V - Altre disposizioni); inserito un nuovo Allegato (Allegato A – Modulo informativo sul significativo trasferimento del rischio). **Parte Seconda, Capitolo 13:** modificata pagina 1; aggiunta pagina 2.

9° Aggiornamento del 9 giugno 2015

Parte Terza. Inserito un nuovo Capitolo 4 “Banche in forma cooperativa”.

10° Aggiornamento del 22 giugno 2015

Parte Prima, Titolo I, Capitolo 3: pagine modificate: I.3.1, I.3.4, I.3.6, Allegato A, eliminato Allegato B. **Parte Prima, Titolo I, Capitolo 5:** Modificato il titolo del Capitolo. Inserite due nuove Sezioni (Sezione IV – Succursali di banche in Stati extracomunitari; Sezione V – Uffici di rappresentanza). **Parte Prima, Titolo I, Capitolo 6:** Modificato il titolo del Capitolo. Sezione I: pagine modificate: I.6.1 e I.6.3. Sezione II: aggiunto un nuovo paragrafo (3. Prestazione di servizi senza stabilimento delle banche italiane in stati extracomunitari) e rinumerato e modificato il precedente paragrafo 3. **Parte Prima, Titolo I:** inserito un nuovo capitolo (Capitolo 7) “Banche extracomunitarie in Italia”. **Errata corrige** del 15 settembre 2015.

11° Aggiornamento del 21 luglio 2015

Parte Prima, Titolo IV. Inseriti nuovi capitoli: “Il sistema dei controlli interni” (Capitolo 3), “Il sistema informativo” (Capitolo 4), “La continuità operativa” (Capitolo 5) e “Governare e gestione del rischio di liquidità” (Capitolo 6).

12° Aggiornamento del 15 settembre 2015

Ristampa integrale comprensiva della sostituzione dei riferimenti ai capitoli della Circolare n. 229 e della Circolare n. 263 abrogati con riferimenti ai nuovi Capitoli introdotti nella Circolare n. 285. **Indice.** Modificato per includere il nuovo inserimento. **Disposizioni introduttive.** Modificata pagina 23. **Parte Prima, Titolo I, Capitolo 3.** Modificata pagina 5 e Allegato A. **Parte Prima, Titolo I, Capitolo 6.** Modificata pagina 4. **Parte Prima, Titolo I, Capitolo 7.** Modificate pagine I.7.13-17. **Parte Prima, Titolo III, Capitolo 1.** Modificate pagine: III.1.8, III.1.13, III.1.23. **Parte Prima, Titolo IV, Capitolo 1.** Modificate pagine: IV.1.4, IV.1.8-9, IV.1.11, IV.1.21. **Parte Prima, Titolo IV, Capitolo 3.** Modificate pagine: IV.3.5, IV.3.39-40. **Parte Seconda, Capitolo 3:** pagina modificata: 3.4. **Parte Seconda, Capitolo 10:** pagine modificate: 10.1, 10.2, 10.6, 10.8, 10.9. **Parte Terza.** Inseriti due nuovi capitoli: (Capitolo 5) “Vigilanza informativa su base individuale e consolidata” e (Capitolo 6) “Vigilanza ispettiva”. **Parte Terza, Capitolo 3.** Modificata pagina: 3.8. **Parte Quarta, Capitolo 1.** Modificate pagine: 1.14-16.

13° Aggiornamento del 13 ottobre 2015

Parte Terza, Capitolo 1. Aggiunta una nuova Sezione “Comunicazioni” (Sezione IX). Modificata pagina: Parte Terza.1.2.

14° Aggiornamento del 24 novembre 2015

Disposizioni introduttive. Modificate pagine: 15-24. **Parte Prima, Titolo I, Capitolo 3.** Modificate pagine: 3, 5, 7. **Parte Prima, Titolo I, Capitolo 7.** Modificate pagine: 7, 8, 11. **Parte Prima, Titolo III, Capitolo 1.** Modificata pagina 2. **Parte Seconda, Capitolo 11.** Modificate le Sezioni I, II e III. Aggiunto l'Allegato A. **Parte Seconda, Capitolo 12.** Modificate le Sezioni I, II e III.

15° Aggiornamento dell' 8 marzo 2016

Disposizioni introduttive. Modificate pagine: 18 e 20. **Parte Prima, Titolo I, Capitolo 3.** Modificato Allegato A. **Parte Prima, Titolo I, Capitolo 7.** Modificato Allegato A. **Parte Terza.** Inserito un nuovo capitolo: "Concessione di finanziamenti da parte di società veicolo per la cartolarizzazione ex legge 130/1999" (Capitolo 7).

16° Aggiornamento del 17 maggio 2016

Parte Prima, Titolo I, Capitolo 7. Modificato Allegato A. **Parte Prima, Titolo IV, Capitolo 4.** Modificate le Sezioni I e IV e aggiunta una nuova sezione "Principi organizzativi relativi a specifiche attività o profili di rischio" (Sezione VII).

17° Aggiornamento del 27 settembre 2016

Parte Prima, Titolo IV, Capitolo 3. Modificata Sez. I pagine: 2 e 3. Modificato l'Allegato A: modificate le pagine 41, 42, aggiunti i sottoparagrafi 2.2, 2.2.1, 2.2.2, 2.2.3.

18° Aggiornamento del 4 ottobre 2016 – Entrata in vigore: 1 gennaio 2017

Parte Prima, Titolo II, Capitolo 1. Modificata la Sezione II.

19° Aggiornamento del 2 novembre 2016

Parte Terza, Capitolo 5. Inserito un nuovo Capitolo 5 "Gruppo bancario cooperativo". Per effetto dell'inserimento i Capitoli 5, 6 e 7 sono stati così rinumerati: Capitolo 6 "Vigilanza informativa su base individuale e consolidata", Capitolo 7 "Vigilanza ispettiva", Capitolo 8 "Concessione di finanziamenti da parte di società veicolo per la cartolarizzazione ex legge 130/1999". Per effetto dell'inserimento sono state aggiornate le seguenti pagine: **Premessa**, pag. 4; **Disposizioni introduttive**, pagg. 18 e 20; **Parte prima, Titolo I, Capitolo 3**, pag. 9; **Capitolo 7**, pag. 15 e 16; **Parte Quarta, Capitolo 1**, pag. 16

20° Aggiornamento del 21 novembre 2017

Indice. Modificato per includere i nuovi inserimenti. **Disposizioni introduttive, Ambito di applicazione:** modificate le pagine 2, 16, 17, 19, 21. **Parte Prima, Titolo I, Capitolo 7:** modificata la Sezione VII. **Parte Prima, Titolo III, Capitolo 1:** modificate le Sezioni I, II, III; modificati gli Allegati C e D. **Parte Prima, Titolo IV, Capitolo 6:** modificata pag. 3. **Parte Seconda, Capitolo 7:** modificate le Sezioni I e II e aggiunta una nuova Sezione IV; **Capitolo 10:** modificate le Sezioni I e V; **Capitolo 12:** modificate le Sezioni I e III.

21° Aggiornamento del 22 maggio 2018

Parte Terza, Capitolo 5. Inserito un nuovo Capitolo 5 “**Banche di Credito Cooperativo**”. Per effetto dell’inserimento i Capitoli 6, 7 e 8 sono stati così rinumerati: Capitolo 6 “Gruppo Bancario Cooperativo”, Capitolo 7 “Vigilanza informativa su base individuale e consolidata”, Capitolo 8 “Vigilanza ispettiva”, Capitolo 9 “Concessione di finanziamenti da parte di società veicolo per la cartolarizzazione ex legge 130/1999”. Per effetto dell’inserimento sono state aggiornate le seguenti pagine: **Premessa**, pag. 4; **Disposizioni introduttive**, pagg. 19 e 21; **Parte prima, Titolo I, Capitolo 3**, pag. 9; **Capitolo 7**, pagg. 15 e 16; **Parte Terza, Capitolo 4**, Sez. I; **Parte Terza, Capitolo 6**, Sez. II; **Parte Quarta, Capitolo 1**, pag. 16. L’**Indice** è stato modificato per includere il nuovo inserimento e la rinumerazione dei capitoli.

22° aggiornamento del 12 giugno 2018

Parte Prima, Titolo III, Capitolo 1: modificate tutte le sezioni e gli Allegati A e D. **Parte Seconda, Capitolo 6:** modificate le Sezioni I e V; **Capitolo 7:** modificate le Sezioni I e III; **Capitolo 9:** modificate le Sezioni I e IV; **Capitolo 10:** modificate le Sezioni I e III; **Capitolo 11:** modificata la Sezione I; **Capitolo 13:** modificate entrambe le sezioni; **Capitolo 14:** modificate entrambe le sezioni. **Parte Terza, Capitolo 1:** modificate le Sezioni I e III. L’**Indice** è stato modificato per includere le modifiche.

23° aggiornamento del 25 settembre 2018

Parte terza, Capitolo 3: Modificata la Sezione I, paragrafi 1, 2 e 5; modificata la Sezione II, paragrafo 1.

24° aggiornamento del 16 ottobre 2018

Parte Terza, Capitolo 10. Inserito un nuovo Capitolo 10 “**Investimenti in immobili**”. L’**Indice** è stato modificato per includere il nuovo inserimento.

25° aggiornamento del 23 ottobre 2018

Parte Prima, Titolo IV. Interamente sostituito il **Capitolo 2 “Politiche e prassi di remunerazione e incentivazione”**. L’**Indice** è stato modificato di conseguenza.

26° aggiornamento del 5 marzo 2019

Parte Prima, Titolo IV, Capitolo 3 “Controlli interni” modificata la pagina 52 dell’Allegato A.

27° aggiornamento del 22 giugno 2019

Indice. Modificato per includere i nuovi inserimenti. **Parte Seconda, Capitolo 3 “Rischio di credito – Metodo standardizzato”**, Sezione I: modificata; Sezione III: aggiunto un nuovo paragrafo; Sezione IV: aggiunto un nuovo paragrafo. **Parte Seconda, Capitolo 4 “Rischio di credito – Metodo IRB”**, Sezione I: modificata; Sezione III: aggiunto un nuovo paragrafo; aggiunta la Sezione V.

28° aggiornamento del 23 luglio 2019

Indice. Modificato per includere i nuovi inserimenti. **Parte Prima, Titolo IV, Capitolo 4 “Il sistema informativo”**, Sezione I: modificata e aggiunto un nuovo paragrafo; Sezione II: modificato il paragrafo 7; modificate le Sezioni III, IV e VI; Sezione VII: modificata e aggiunti due nuovi paragrafi; Allegato A: modificato. **Parte Prima, Titolo IV, Capitolo 5 “La continuità operativa”**, Paragrafo 2: modificato; Allegato A: modificata la Sezione II.

29° aggiornamento del 17 settembre 2019

Indice. Modificato secondo le modifiche apportate. **Parte Seconda, Capitolo 1 “Fondi propri”:** modificate le Sezioni I e V; eliminata la Sezione VI; **Capitolo 6 “Operazioni di cartolarizzazione”:** modificata la Sezione IV; **Capitolo 7 “Rischio di controparte”:** eliminata la Sezione IV.

30° aggiornamento del 4 dicembre 2019

Indice. Modificato secondo le modifiche apportate. **Parte Prima, Capitolo 1 “Autorizzazione all’attività bancaria”:** modificate le Sezioni I, II, III, V, VI, VII e VIII. **Capitolo 3 “ Banche e società finanziarie comunitarie in Italia”:** eliminata la Sez. VI e modificate tutte le altre Sezioni; modificato l’Allegato A. **Capitolo 5:** il titolo è stato modificato in “**Stabilimento all’estero di banche e società finanziarie italiane**”; sono state modificate le Sezioni I, II, III e IV. **Capitolo 6 “Prestazione di servizi all’estero senza stabilimento delle banche e delle società finanziarie italiane”:** modificate entrambe le Sezioni. **Capitolo 7 “Banche extracomunitarie in Italia”:** modificate tutte le Sezioni; la Sez. VII “Vigilanza”, anch’essa modificata, è stata rinumerata come Sez. VIII per effetto dell’inserimento di una nuova Sez. VII “Autorizzazione all’esercizio di servizi e attività di investimento tramite stabilimento di succursale”; l’Allegato B è stato eliminato e l’Allegato C è stato rinominato allegato B.

31° aggiornamento del 24 marzo 2020

Indice. Modificato secondo le modifiche apportate. **Parte Seconda, Capitolo 13 “Informativa al pubblico”:** Sezione I: modificata pag. 2; Sezione II: aggiunto un nuovo paragrafo 5 “Informativa sulle esposizioni deteriorate e oggetto di misure di correzione”.

32° aggiornamento del 21 aprile 2020

Indice. Modificato secondo le modifiche apportate. **Parte Prima, Titolo III, Capitolo 1 “Processo di controllo prudenziale”:** modificate le Sezioni I e III; modificati gli allegati A e C e aggiunto un nuovo Allegato C *bis*. **Parte Prima, Titolo IV, Capitolo 3 “Il sistema dei controlli interni”:** modificate le Sezioni I, II e III; modificati gli Allegati A e C. **Parte Prima, Titolo IV, Capitolo 6 “Governare e gestione del rischio di liquidità”:** modificate le Sezioni I e III.

33° aggiornamento del 23 giugno 2020

Parte Terza, inserito un nuovo **Capitolo 11 “Attività di rischio e conflitti di interessi nei confronti di soggetti collegati”.** **Indice.** Modificato per includere il nuovo Capitolo 11.

34° aggiornamento del 22 settembre 2020

Ristampa integrale per integrare il 33° aggiornamento e nuove modifiche normative. **Parte Prima, Titolo I, Capitolo 1 “Autorizzazioni all’attività bancaria”,** Allegato A, Parte II: modificato punto 4; Allegato B, Sezione A: modificato punto 2. **Parte Prima, Titolo I, Capitolo 7 “Banche extracomunitarie in Italia”,** Sez. VIII: modificata la nota 1; Allegato A modificato per eliminare i riferimenti a disposizioni abrogate e inserire i riferimenti a disposizioni vigenti. **Parte Prima, Titolo III, Capitolo 1 “Processo di controllo prudenziale”,** Sez. I: modificato il par. 4; Sez. III: inserita correzione di errore materiale in sottoparagrafo 2.2. **Parte Prima, Titolo IV, Capitolo 3 “Il sistema dei controlli interni”:** modificate Sezioni I, II, III, IV, V, VIII, IX; Allegato A: modificati par. 13 e par. 14 per aggiornare rinvii a disposizioni normative. **Parte Prima, Titolo IV Capitolo 4 “Il sistema informativo”,** Sez. I: modificato il par. 3.; Sez. II: modificata la nota 5; Sez. III: modificata la nota 3; modificata la Sez. VI. **Parte Prima Titolo IV**

Capitolo 5 “La continuità operativa”: modificato il par. 3. **Parte Seconda, Capitolo 2 “Requisiti patrimoniali**, Sez. I modificata; Sez. III: modificato par. 1. **Parte Seconda, Capitolo 3 “Rischio di credito – metodo standardizzato”**, Sez. III: modificato il par. 4; Sez. IV: modificato il par. 2. **Parte Seconda, Capitolo 4, “Rischio di credito – metodo IRB”**, Sez. III: modificato il par. 3; Sez. V modificata. **Parte Terza, Capitolo 1 “Partecipazioni detenibili dalle banche e dai gruppi bancari”**, Sez. I par. 3: modificata la nota 4; Sez. II: modificato il par. 2. **Parte Terza, Capitolo 5 “Banche di credito cooperativo”**, Sez. III par. 2: modificata la nota 6. **Parte Terza, Capitolo 6 “Gruppo bancario cooperativo”**, Sez. II: modificato il par. 2; Sez. III: modificato sottoparagrafo 1.3 e eliminata la nota 5. **Parte Terza, Capitolo 10 “Investimenti in immobili”**, Sez. III: modificata la nota 1. **Parte Quarta, Capitolo 1 “Bancoposta”**, Sez. I: modificato il par. 5; Sez. II: modificato il par. 5; Sezione III: eliminato il sottoparagrafo 2.2 e modificati i sottoparagrafi 2.3 e 2.4 rinumerati 2.2 e 2.3.

35° aggiornamento del 30 giugno 2021

Parte Prima, Titolo IV. Interamente sostituito il **Capitolo 1 “Governo societario”**.

36° aggiornamento del 20 luglio 2021

Parte Prima, Titolo IV, Capitolo 3 “Il sistema dei controlli interni”: modificate la Sezione I e l’Allegato A.

37° aggiornamento del 24 novembre 2021

Parte Prima, Titolo IV. Interamente sostituito il **Capitolo 2 “Politiche e prassi di remunerazione e incentivazione”**.

38° aggiornamento del 15 febbraio 2022

Parte Prima, Titolo I, Capitolo 1 “Banche extracomunitarie in Italia”. Modificate Sez. VII, par. 2 e l’Allegato A.

Parte Prima, Titolo II, Capitolo 1 “Riserve di capitale”. Modificate Sez. I, paragrafi 2, 4 e 5; Sez. I-bis; Sez. IV, par. 1; Sez. V, par. 2.

Parte Terza. Inserito il **Capitolo 12 “Misure basate sulle caratteristiche dei clienti o dei finanziamenti”**.

39° aggiornamento del 12 luglio 2022

Parte Prima, Titolo I. Interamente sostituito il **Capitolo 2 “Gruppi bancari e vigilanza consolidata”**.

Parte Prima, Titolo I. Interamente sostituito il **Capitolo 4 “Albo delle banche e dei gruppi bancari”**.

Parte Prima, Titolo III, Capitolo 1 “Processo di controllo prudenziale”. Modificate le Sezioni I-V e l’Allegato D.

40° aggiornamento del 2 novembre 2022

Parte Prima, Titolo IV. Modificata la Sezione I del **Capitolo 3 “Il sistema dei controlli interni”**.

Parte Prima, Titolo IV, Capitolo 4 “Il sistema informativo”. Modificate le Sezioni I, II, III, IV, VI, VII e l’Allegato A e inserita una nuova Sezione IV *bis*.

Parte Prima, Titolo IV. Interamente sostituito il **Capitolo 5 “La continuità operativa”**.

INDICE

RIEPILOGO DEGLI AGGIORNAMENTI

INDICE

PREMESSA

DISPOSIZIONI INTRODUTTIVE

SIGLE E ABBREVIAZIONI

DEFINIZIONI

MECCANISMO DI VIGILANZA UNICO E PROCEDIMENTI AMMINISTRATIVI

AUTORIZZAZIONE ALL'UTILIZZO DEI SISTEMI INTERNI DI MISURAZIONE DEI RISCHI

SEZIONE I - FONTI NORMATIVE

SEZIONE II - PROCEDIMENTI AMMINISTRATIVI

SEZIONE III - PROCEDURE AUTORIZZATIVE

1. Premessa
2. Procedura autorizzativa

AMBITO DI APPLICAZIONE

SEZIONE I - DISPOSIZIONI A CARATTERE GENERALE

1. Premessa
2. Fonti normative
3. Definizioni

SEZIONE II - DISCIPLINA SU BASE INDIVIDUALE

1. Banche italiane
2. Succursali in Italia di banche extracomunitarie
3. Succursali in Italia di banche comunitarie

SEZIONE III - DISCIPLINA SU BASE CONSOLIDATA

1. Capogruppo di gruppi bancari e imprese di riferimento
2. Componenti del gruppo sub-consolidanti

SEZIONE IV - ALTRE DISPOSIZIONI

1. Autorizzazione all'attività bancaria (Parte Prima, Tit. I, Cap. 1)
2. Gruppi bancari (Parte Prima, Tit. I, Cap. 2)
3. Albo delle banche e dei gruppi bancari (Parte Prima, Tit. I, Cap. 4)
4. Succursali estere di banche e società finanziarie italiane (Parte Prima, Tit. I, Cap. 5)
5. Prestazione di servizi all'estero senza stabilimento delle banche e delle società finanziarie italiane (Parte Prima, Tit. I, Cap. 6)
6. Governo societario (Parte Prima, Tit. IV, Cap. 1)

7. Comunicazioni alla Banca d'Italia (Parte Terza, Cap. 2)
8. Banche in forma cooperativa (Parte Terza, Cap. 4)
9. Bancoposta (Parte Quarta, Cap. 1)

SEZIONE V - ESERCIZIO DELLE DISCREZIONALITÀ NAZIONALI

Allegato A

PARTE PRIMA - RECEPIMENTO IN ITALIA DELLA CRD IV

TITOLO I – ACCESSO AL MERCATO E STRUTTURA

TITOLO I – Capitolo 1

AUTORIZZAZIONE ALL'ATTIVITÀ BANCARIA

SEZIONE I - DISPOSIZIONI DI CARATTERE GENERALE

1. Premessa
2. Fonti normative
3. Definizioni
4. Destinatari della disciplina
5. Procedimenti amministrativi

SEZIONE II - CAPITALE MINIMO

1. Ammontare del capitale iniziale
2. Caratteristiche e movimentazione del conto corrente indisponibile

SEZIONE III - PROGRAMMA DI ATTIVITÀ

1. Contenuto del programma di attività
2. Tutoring
3. Valutazioni della Banca centrale europea e della Banca d'Italia

SEZIONE IV - ASSETTO PROPRIETARIO

1. Partecipanti
2. Strutture di gruppo

SEZIONE V - AUTORIZZAZIONE ALL'ATTIVITÀ BANCARIA PER LE SOCIETÀ DI NUOVA COSTITUZIONE

1. Domanda di autorizzazione
2. Istruttoria e valutazioni della Banca centrale europea e della Banca d'Italia
3. Rilascio dell'autorizzazione
4. Iscrizione all'albo e altri adempimenti
5. Decadenza e revoca dell'autorizzazione

SEZIONE VI - AUTORIZZAZIONE ALL'ATTIVITÀ BANCARIA PER LE SOCIETÀ GIÀ ESISTENTI

1. Procedura di autorizzazione
2. Programma di attività
3. Accertamento dell'esistenza del patrimonio e altre verifiche

SEZIONE VII - AUTORIZZAZIONE ALL'ESERCIZIO DI SERVIZI E ATTIVITÀ DI INVESTIMENTO

1. Premessa
2. Domanda di autorizzazione
3. Istruttoria e rilascio dell'autorizzazione
4. Domanda di autorizzazione, o di estensione della stessa, all'esercizio di servizi e attività di investimento successivamente al rilascio dell'autorizzazione bancaria
5. Decadenza e revoca dell'autorizzazione
6. Obblighi informativi

SEZIONE VIII - FILIAZIONI DI BANCHE ESTERE

1. Filiazioni di banche comunitarie
2. Filiazioni di banche extracomunitarie

Allegato A - SCHEMA DELLA RELAZIONE SUL GOVERNO SOCIETARIO E SULLA STRUTTURA ORGANIZZATIVA

Allegato B – SCHEMA DELLA RELAZIONE ILLUSTRATIVA SULL'ESERCIZIO DI SERVIZI E ATTIVITÀ DI INVESTIMENTO

TITOLO I – Capitolo 2

GRUPPI BANCARI E VIGILANZA CONSOLIDATA

SEZIONE I - DISPOSIZIONI DI CARATTERE GENERALE

1. Premessa
2. Fonti normative
3. Definizioni
4. Destinatari della disciplina
5. Procedimenti amministrativi

SEZIONE II - GRUPPO BANCARIO

1. Composizione del gruppo e individuazione della capogruppo
2. Società del gruppo

SEZIONE III – AUTORIZZAZIONE DELLE SOCIETÀ DI PARTECIPAZIONE FINANZIARIA O DI PARTECIPAZIONE FINANZIARIA MISTA CAPOGRUPPO

1. Autorizzazione delle società di partecipazione finanziaria o di partecipazione finanziaria mista capogruppo
2. Condizioni per l'autorizzazione e relativi criteri di valutazione

3. Rilascio dell'autorizzazione
4. Revoca dell'autorizzazione
5. Coordinamento con l'autorizzazione di cui all'art. 19 TUB
6. Coordinamento con l'autorizzazione di cui all'art. 14 TUB

SEZIONE IV – ESENZIONE DELLE SOCIETÀ DI PARTECIPAZIONE FINANZIARIA O DI PARTECIPAZIONE FINANZIARIA MISTA

1. Soggetti ammessi a presentare l'istanza di esenzione
2. Condizioni per l'esenzione e relativi criteri di valutazione
3. Concessione dell'esenzione
4. Coordinamento con l'autorizzazione di cui all'art. 19 TUB
5. Coordinamento con l'autorizzazione di cui all'art. 14 TUB

SEZIONE V – POTERI DELLA CAPOGRUPPO E OBBLIGHI DELLE CONTROLLATE

SEZIONE VI - STATUTI

1. Statuto della capogruppo
2. Statuto delle società controllate
3. Statuto della società di partecipazione finanziaria o di partecipazione finanziaria mista esentata e della banca italiana designata per le funzioni di direzione e coordinamento

SEZIONE VII – SOCIETÀ DI PARTECIPAZIONE FINANZIARIA O DI PARTECIPAZIONE FINANZIARIA MISTA NON CAPOGRUPPO

1. Società di partecipazione finanziaria o di partecipazione finanziaria mista diverse dalla capogruppo
2. Società di partecipazione finanziaria o di partecipazione finanziaria mista appartenenti a gruppi soggetti a vigilanza su base consolidata di competenza di autorità di vigilanza di altri Stati dell'Unione europea

Allegato A – SCHEMA PER LA VERIFICA DELLA CONDIZIONE DEL CONTROLLO IN VIA ESCLUSIVA O PRINCIPALE DI SOCIETÀ BANCARIE O FINANZIARIE

TITOLO I - Capitolo 3

BANCHE E SOCIETÀ FINANZIARIE COMUNITARIE IN ITALIA

SEZIONE I - DISPOSIZIONI DI CARATTERE GENERALE

1. Fonti normative
2. Definizioni
3. Destinatari della disciplina
4. Procedimenti amministrativi

SEZIONE II - SUCCURSALI IN ITALIA DI BANCHE COMUNITARIE

1. Primo insediamento
2. Modifiche alle informazioni comunicate
3. Attività esercitabili

4. Disposizioni applicabili
5. I controlli
6. Uffici di rappresentanza
7. Procedure per le segnalazioni

SEZIONE III - PRESTAZIONE DI SERVIZI SENZA STABILIMENTO IN ITALIA

SEZIONE IV - PROVVEDIMENTI STRAORDINARI E INGIUNTIVI

SEZIONE V - SOCIETÀ FINANZIARIE COMUNITARIE AMMESSE AL MUTUO RICONOSCIMENTO

Allegato A - DISPOSIZIONI APPLICABILI

TITOLO I – Capitolo 4

ALBO DELLE BANCHE E DEI GRUPPI BANCARI

SEZIONE I - DISPOSIZIONI DI CARATTERE GENERALE

1. Premessa
2. Fonti normative
3. Destinatari della disciplina
4. Procedimenti amministrativi

SEZIONE II - ALBO DELLE BANCHE

1. Contenuto dell'albo
2. Iscrizione all'albo
3. Variazioni all'albo
4. Cancellazione dall'albo

SEZIONE III - ALBO DEI GRUPPI BANCARI

1. Contenuto dell'albo
2. Iscrizione all'albo
3. Variazioni all'albo
4. Cancellazione dall'albo
5. Iscrizione all'albo delle società indicate all'art. 69.2 TUB

SEZIONE IV - FORME DI PUBBLICITÀ DELL'ISCRIZIONE

1. Pubblicità dell'iscrizione
2. Pubblicazione degli albi e modalità di consultazione

Allegato A - ALBO DELLE BANCHE - SCHEMA DELLE INFORMAZIONI OGGETTO DI COMUNICAZIONE

TITOLO I - Capitolo 5

STABILIMENTO ALL' ESTERO DI BANCHE E SOCIETÀ FINANZIARIE ITALIANE

SEZIONE I - DISPOSIZIONI DI CARATTERE GENERALE

1. Fonti normative
2. Definizioni
3. Destinatari della disciplina
4. Procedimenti amministrativi
5. Linee di orientamento

SEZIONE II - STABILIMENTO DI BANCHE IN STATI COMUNITARI

1. Primo insediamento
2. Modifiche delle informazioni comunicate
3. Attività esercitabili
4. Interventi dell'Autorità di vigilanza
5. Procedure per le segnalazioni

SEZIONE III - STABILIMENTO IN STATI COMUNITARI DI SUCCURSALI DI SOCIETÀ FINANZIARIE ITALIANE AMMESSE AL MUTUO RICONOSCIMENTO

1. Condizioni per lo stabilimento della succursale
2. Procedura per lo stabilimento e interventi

SEZIONE IV – SUCCURSALI DI BANCHE IN STATI TERZI

SEZIONE V - UFFICI DI RAPPRESENTANZA

TITOLO I - Capitolo 6

PRESTAZIONE DI SERVIZI ALL'ESTERO SENZA STABILIMENTO DELLE BANCHE E DELLE SOCIETÀ FINANZIARIE ITALIANE

SEZIONE I - DISPOSIZIONI DI CARATTERE GENERALE

1. Fonti normative
2. Definizioni
3. Destinatari della disciplina
4. Procedimenti amministrativi

SEZIONE II - PROCEDURE PER LA PRESTAZIONE DI SERVIZI SENZA STABILIMENTO

1. Banche italiane in Stati comunitari
2. Società finanziarie italiane ammesse al mutuo riconoscimento in Stati comunitari
3. Banche italiane in Stati terzi
4. Interventi dell'Autorità di vigilanza

TITOLO I - Capitolo 7

BANCHE EXTRACOMUNITARIE IN ITALIA

SEZIONE I - DISPOSIZIONI DI CARATTERE GENERALE

1. Premessa

2. Fonti normative
3. Definizioni
4. Destinatari della disciplina
5. Procedimenti amministrativi

SEZIONE II – PRIMO INSEDIAMENTO DI SUCCURSALI E UFFICI DI RAPPRESENTANZA

1. Condizioni per l'autorizzazione allo stabilimento della prima succursale
2. Programma di attività
3. Requisiti e criteri di idoneità dei responsabili della succursale
4. Domanda di autorizzazione
5. Istruttoria della Banca d'Italia e rilascio dell'autorizzazione
6. Iscrizione all'albo e avvio dell'operatività
7. Primo insediamento di uffici di rappresentanza

SEZIONE III – SUCCURSALI E UFFICI DI RAPPRESENTANZA DI BANCHE EXTRACOMUNITARIE GIÀ INSEDIATE IN ITALIA

1. Succursali
2. Uffici di rappresentanza

SEZIONE IV – PRESTAZIONE DI SERVIZI SENZA STABILIMENTO

1. Domanda di autorizzazione
2. Istruttoria della Banca d'Italia e rilascio dell'autorizzazione

SEZIONE V – DECADENZA DELLE AUTORIZZAZIONI, REVOCA E CHIUSURA DI SUCCURSALI E UFFICI DI RAPPRESENTANZA

SEZIONE VI – SEGNALAZIONI

1. Segnalazioni G.I.A.V.A
2. Altri obblighi informativi

SEZIONE VII – AUTORIZZAZIONE ALL'ESERCIZIO DI SERVIZI E ATTIVITÀ DI INVESTIMENTO

1. Esercizio di servizi e attività di investimento tramite stabilimento di succursale
2. Esercizio di servizi e attività di investimento senza stabilimento
3. Domande di autorizzazione successive
4. Decadenza e revoca dell'autorizzazione

SEZIONE VIII – VIGILANZA

1. Disposizioni applicabili alle succursali
2. Disposizioni applicabili alla prestazione di servizi senza stabilimento
3. Provvedimenti straordinari e ingiuntivi

Allegato A – DISPOSIZIONI APPLICABILI

Allegato B – ARTICOLAZIONE TERRITORIALE DELLE BANCHE

TITOLO II – MISURE PRUDENZIALI

TITOLO II - Capitolo 1

RISERVE DI CAPITALE

SEZIONE I - DISPOSIZIONI DI CARATTERE GENERALE

1. Premessa
2. Fonti normative
3. Definizioni
4. Destinatari della disciplina
5. Procedimenti amministrativi

SEZIONE I-BIS – DISPOSIZIONI COMUNI

SEZIONE II - RISERVA DI CONSERVAZIONE DEL CAPITALE

1. Determinazione della riserva di conservazione del capitale

SEZIONE III - RISERVA DI CAPITALE ANTICICLICA

1. Riserva di capitale anticiclica specifica della banca
2. Criteri per la determinazione del coefficiente anticiclico interno
3. Riconoscimento dei coefficienti anticiclici superiori al 2,5% applicabili negli Stati comunitari o in Stati extracomunitari
4. Determinazione del coefficiente anticiclico applicabile in Stati extracomunitari
5. Calcolo del coefficiente anticiclico specifico della banca

SEZIONE IV - RISERVA DI CAPITALE PER LE G-SII E PER LE O-SII

1. Individuazione e classificazione delle G-SII
2. Individuazione delle O-SII e requisito applicabile
3. Disposizioni comuni

SEZIONE V – RISERVA DI CAPITALE A FRONTE DEL RISCHIO SISTEMICO

1. Calcolo del coefficiente della riserva di capitale a fronte del rischio sistemico
2. Procedura di notifica
3. Riconoscimento reciproco del coefficiente della riserva di capitale a fronte del rischio sistemico

SEZIONE VI – MISURE DI CONSERVAZIONE DEL CAPITALE

1. Limiti alle distribuzioni
2. Piano di conservazione del capitale

TITOLO III – PROCESSO DI CONTROLLO PRUDENZIALE

TITOLO III - Capitolo 1

PROCESSO DI CONTROLLO PRUDENZIALE

SEZIONE I - DISPOSIZIONI DI CARATTERE GENERALE

1. Premessa
2. Fonti normative
3. Definizioni
4. Destinatari della disciplina
5. Procedimenti amministrativi

SEZIONE II – DISPOSIZIONI COMUNI AI PROCESSI DI VALUTAZIONE AZIENDALE DELL’ADEGUATEZZA PATRIMONIALE (ICAAP) E DELL’ADEGUATEZZA DEL SISTEMA DI GOVERNO E GESTIONE DEL RISCHIO DI LIQUIDITÀ (ILAAP)

1. Premessa
2. La proporzionalità nell’ICAAP e nell’ILAAP
3. Governo societario dell’ICAAP e dell’ILAAP
4. L’informativa sull’ICAAP e sull’ILAAP

SEZIONE III – LA VALUTAZIONE AZIENDALE DELL’ADEGUATEZZA PATRIMONIALE (ICAAP)

1. Disposizioni di carattere generale
2. Le fasi dell’ICAAP
3. Riferimenti temporali dell’ICAAP

SEZIONE IV – LA VALUTAZIONE AZIENDALE SULL’ADEGUATEZZA DEL SISTEMA DI GOVERNO E GESTIONE DEL RISCHIO DI LIQUIDITÀ (ILAAP)

SEZIONE V - PROCESSO DI REVISIONE E VALUTAZIONE PRUDENZIALE (SREP)

1. Disposizioni di carattere generale
2. La proporzionalità nello SREP
3. I sistemi di analisi aziendale
4. Il confronto con le banche
5. Gli interventi correttivi
6. Le misure di intervento precoce
7. Cooperazione di vigilanza

Allegato A - RISCHI DA SOTTOPORRE A VALUTAZIONE NELL’ICAAP

Allegato B - RISCHIO DI CONCENTRAZIONE PER SINGOLE CONTROPARTI O GRUPPI DI CLIENTI CONNESSI

Allegato C - RISCHIO DI TASSO D’INTERESSE SUL PORTAFOGLIO BANCARIO IN TERMINI DI VARIAZIONI DEL VALORE ECONOMICO

Allegato C-bis – RISCHIO DI TASSO DI INTERESSE SUL PORTAFOGLIO BANCARIO IN TERMINI DI VARIAZIONI DEL MARGINE DI INTERESSE

Allegato D - SCHEMA DI RIFERIMENTO PER IL RESOCONTO ICAAP/ILAAP

TITOLO III - Capitolo 2

INFORMATIVA AL PUBBLICO STATO PER STATO - (*COUNTRY-BY-COUNTRY REPORTING*)

SEZIONE I - DISPOSIZIONI DI CARATTERE GENERALE

1. Premessa
2. Fonti normative
3. Destinatari della disciplina

SEZIONE II - REQUISITI DELL'INFORMATIVA

1. Contenuto e modalità di pubblicazione delle informazioni
2. Organizzazione e controlli

Allegato A - INFORMATIVA DA PUBBLICARE

TITOLO IV – GOVERNO SOCIETARIO, CONTROLLI INTERNI, GESTIONE DEI RISCHI

TITOLO IV – Capitolo 1

GOVERNO SOCIETARIO

SEZIONE I - DISPOSIZIONI DI CARATTERE GENERALE

1. Premessa
2. Fonti normative
3. Definizioni
4. Destinatari della disciplina

SEZIONE II - SISTEMI DI AMMINISTRAZIONE E CONTROLLO E PROGETTO DI GOVERNO SOCIETARIO

1. Principi generali
2. Linee applicative

SEZIONE III - COMPITI E POTERI DEGLI ORGANI SOCIALI

1. Disposizioni comuni
2. Organi con funzione di supervisione strategica e di gestione
3. Organo con funzione di controllo

SEZIONE IV - COMPOSIZIONE E NOMINA DEGLI ORGANI SOCIALI

1. Principi generali
2. Linee applicative

SEZIONE V - FUNZIONAMENTO DEGLI ORGANI, FLUSSI INFORMATIVI E RUOLO DEL PRESIDENTE

1. Funzionamento degli organi e flussi informativi
2. Ruolo del presidente

SEZIONE VI - AUTOVALUTAZIONE DEGLI ORGANI

1. Principi generali
2. Linee applicative
3. Criteri per il processo di autovalutazione

SEZIONE VII - OBBLIGHI DI INFORMATIVA AL PUBBLICO

1. Obblighi di informativa

SEZIONE VIII - DISPOSIZIONI TRANSITORIE E FINALI

1. Disciplina transitoria

TITOLO IV – Capitolo 2

POLITICHE E PRASSI DI REMUNERAZIONE E INCENTIVAZIONE

SEZIONE I - DISPOSIZIONI DI CARATTERE GENERALE

1. Premessa
2. Fonti normative
3. Definizioni
4. Destinatari della disciplina
5. Principi e criteri generali
6. Identificazione del “personale più rilevante”
7. Criterio di proporzionalità
8. Applicazione ai gruppi bancari
9. Procedimenti amministrativi

SEZIONE II - RUOLO E RESPONSABILITÀ DELL'ASSEMBLEA E DEGLI ORGANI AZIENDALI

1. Ruolo dell'assemblea
2. Ruolo dell'organo con funzione di supervisione strategica e del comitato per le remunerazioni
3. Funzioni aziendali di controllo

SEZIONE III - LA STRUTTURA DEI SISTEMI DI REMUNERAZIONE E INCENTIVAZIONE

1. Rapporto tra componente variabile e componente fissa
2. Remunerazione variabile
3. Compensi dei consiglieri non esecutivi, dei componenti dell'organo con funzione di controllo e dei componenti delle funzioni aziendali di controllo

SEZIONE IV - LA POLITICA DI REMUNERAZIONE PER PARTICOLARI CATEGORIE

1. Agenti in attività finanziaria, agenti di assicurazione e consulenti finanziari abilitati all'offerta fuori sede

SEZIONE V - DISPOSIZIONI DI CARATTERE PARTICOLARE

1. Banche che beneficiano di aiuti di Stato
2. Banche che non rispettano i requisiti di cui agli articoli 141 o 141-ter della CRD o che si trovano nelle situazioni di cui all'articolo 16-bis della BRRD

SEZIONE VI - OBBLIGHI DI INFORMATIVA E DI TRASMISSIONE DEI DATI

1. Obblighi di informativa al pubblico
2. Obblighi di trasmissione di dati alla Banca d'Italia
3. Obblighi di informativa all'assemblea

SEZIONE VII - DISPOSIZIONI TRANSITORIE E FINALI

1. Disposizioni transitorie

Allegato A – INFORMAZIONI DA TRASMETTERE PER L'ESCLUSIONE DEL PERSONALE DAL NOVERO DEI *RISK-TAKER*

Allegato B – INFORMAZIONI DA TRASMETTERE SULLA DECISIONE DI AUMENTO DEL LIMITE AL RAPPORTO VARIABILE/FISSO SUPERIORE A 1:1

TITOLO IV – Capitolo 3

IL SISTEMA DEI CONTROLLI INTERNI

SEZIONE I - DISPOSIZIONI PRELIMINARI E PRINCIPI GENERALI

1. Premessa
2. Fonti normative
3. Definizioni
4. Destinatari della disciplina
5. Procedimenti amministrativi
6. Principi generali

SEZIONE II – IL RUOLO DEGLI ORGANI AZIENDALI

1. Premessa
2. Organo con funzione di supervisione strategica
3. Organo con funzione di gestione
4. Organo con funzione di controllo
5. Il coordinamento delle funzioni di controllo

SEZIONE III – FUNZIONI AZIENDALI DI CONTROLLO

1. Istituzione delle funzioni aziendali di controllo
2. Programmazione e rendicontazione dell'attività di controllo
3. Requisiti specifici delle funzioni aziendali di controllo

SEZIONE IV – ESTERNALIZZAZIONE DI FUNZIONI AZIENDALI (OUTSOURCING)

1. Principi generali e requisiti particolari

2. Comunicazioni alla Banca centrale europea o alla Banca d'Italia
3. Esternalizzazione del trattamento del contante

SEZIONE V – IL RAF E IL SISTEMA DEI CONTROLLI INTERNI NEI GRUPPI BANCARI

1. Il RAF nei gruppi bancari
2. Controlli interni di gruppo
3. Comunicazioni alla Banca centrale europea o alla Banca d'Italia

SEZIONE VI – IMPRESE DI RIFERIMENTO

SEZIONE VII – SUCCURSALI DI BANCHE COMUNITARIE E DI BANCHE EXTRACOMUNITARIE AVENTI SEDE NEGLI STATI INDICATI NELL'ALLEGATO A DELLE DISPOSIZIONI INTRODUTTIVE

SEZIONE VIII – SISTEMI INTERNI DI SEGNALAZIONE DELLE VIOLAZIONI

SEZIONE IX – INFORMATIVA ALLA BANCA CENTRALE EUROPEA O ALLA BANCA D'ITALIA

Allegato A – DISPOSIZIONI SPECIALI RELATIVE A PARTICOLARI CATEGORIE DI RISCHIO

Allegato B – CONTROLLI SULLE SUCCURSALI ESTERE

Allegato C – IL RISK APPETITE FRAMEWORK

TITOLO IV – Capitolo 4

IL SISTEMA INFORMATIVO

SEZIONE I – DISPOSIZIONI DI CARATTERE GENERALE

1. Premessa
2. Fonti normative
3. Definizioni
4. Destinatari della disciplina
5. Procedimenti amministrativi

SEZIONE II – GOVERNO, ORGANIZZAZIONE E CONTROLLI DEL SISTEMA INFORMATIVO

1. Premessa
2. Compiti degli organi aziendali per i profili ICT
3. Organizzazione della funzione ICT
4. La funzione di controllo dei rischi ICT e di sicurezza
5. Internal audit

SEZIONE III – LA GESTIONE DEL RISCHIO ICT E DI SICUREZZA

SEZIONE IV – LA GESTIONE DELLA SICUREZZA DELL'INFORMAZIONE E DELLE OPERAZIONI ICT

SEZIONE IV *BIS* – LA GESTIONE DEI PROGETTI E DEI CAMBIAMENTI ICT

SEZIONE V – IL SISTEMA DI GESTIONE DEI DATI

SEZIONE VI – L'ESTERNALIZZAZIONE DEL SISTEMA INFORMATIVO E IL RICORSO A SOGGETTI TERZI PER LA PRESTAZIONE DI SERVIZI ICT

1. Premessa
2. Accordi con i fornitori e altri requisiti
3. Il ricorso a soggetti terzi

SEZIONE VII – DISPOSIZIONI SPECIFICHE IN MATERIA DI PRESTAZIONE DI SERVIZI DI PAGAMENTO

1. Sicurezza dei servizi di pagamento
2. Gestione del rapporto con gli utenti dei servizi di pagamento
3. Esenzione dall'obbligo di predisporre il meccanismo di emergenza di cui all'art. 33(4) del Regolamento delegato (UE) 2018/389 della Commissione europea

Allegato A – DOCUMENTI AZIENDALI PER LA GESTIONE E IL CONTROLLO DEL SISTEMA INFORMATIVO

TITOLO IV – Capitolo 5

LA CONTINUITÀ OPERATIVA

1. Destinatari
2. Fonti normative
3. Banche soggette ai requisiti applicabili a tutti gli operatori (Allegato A, Sezione II)
4. Banche soggette ai requisiti particolari per i processi a rilevanza sistemica (Allegato A, Sezione III)

Allegato A – REQUISITI PER LA CONTINUITÀ OPERATIVA

TITOLO IV – Capitolo 6

GOVERNO E GESTIONE DEL RISCHIO DI LIQUIDITÀ

SEZIONE I - DISPOSIZIONI DI CARATTERE GENERALE

1. Premessa
2. Fonti normative
3. Destinatari della disciplina
4. Procedimenti amministrativi

SEZIONE II – IL RUOLO DEGLI ORGANI AZIENDALI

1. Premessa
2. Compiti degli organi aziendali

3. Soglia di tolleranza al rischio di liquidità

SEZIONE III – PROCESSO DI GESTIONE DEL RISCHIO DI LIQUIDITÀ

1. Premessa
2. Identificazione e misurazione del rischio
3. Prove di stress
4. Strumenti di attenuazione del rischio di liquidità
5. Rischio di liquidità derivante dall'operatività infra-giornaliera
6. *Contingency Funding and Recovery Plan*
7. Ulteriori aspetti connessi con la gestione del rischio di liquidità nei gruppi bancari

SEZIONE IV – SISTEMA DI PREZZI DI TRASFERIMENTO INTERNO DEI FONDI

SEZIONE V – SISTEMA DEI CONTROLLI INTERNI

1. Premessa
2. Sistemi di rilevazione e di verifica delle informazioni
3. I controlli di secondo livello: la funzione di controllo dei rischi (*risk management*) sulla liquidità
4. Revisione interna

SEZIONE VI – INFORMATIVA PUBBLICA

SEZIONE VII – SUCCURSALI DI BANCHE EXTRACOMUNITARIE

SEZIONE VIII – INTERVENTI DI VIGILANZA

PARTE SECONDA - APPLICAZIONE IN ITALIA DEL CRR

Capitolo 1 - FONDI PROPRI

SEZIONE I - FONTI NORMATIVE

SEZIONE II - PROCEDIMENTI AMMINISTRATIVI

SEZIONE III - ESERCIZIO DELLE DISCREZIONALITÀ NAZIONALI

SEZIONE IV - ALTRE DISPOSIZIONI

1. Computabilità degli utili di periodo o di fine esercizio nel capitale primario di classe 1
2. Individuazione delle banche che si qualificano come cooperative ai sensi dell'art. 27, par. 1 CRR

SEZIONE V - COMUNICAZIONI ALLA BANCA CENTRALE EUROPEA E ALLA BANCA D'ITALIA

1. Indici di mercato generali

2. Detenzione di indici di strumenti di capitale
3. Cessione in blocco di immobili ad uso prevalentemente funzionale

Capitolo 2 - REQUISITI PATRIMONIALI

SEZIONE I - FONTI NORMATIVE

SEZIONE II - ESERCIZIO DELLE DISCREZIONALITÀ NAZIONALI

SEZIONE III - ALTRE DISPOSIZIONI

1. Perimetro e metodi di consolidamento
2. Norme organizzative

Capitolo 3 - RISCHIO DI CREDITO – METODO STANDARDIZZATO

SEZIONE I - FONTI NORMATIVE

SEZIONE II - PROCEDIMENTI AMMINISTRATIVI

SEZIONE III - ESERCIZIO DELLE DISCREZIONALITÀ NAZIONALI

1. Esposizioni infra-gruppo
2. Obbligazioni garantite
3. Esposizioni garantite da immobili. Innalzamento del fattore di ponderazione o applicazione di criteri di ammissibilità più restrittivi
4. *Default* di un debitore. Soglia di rilevanza delle obbligazioni creditizie in arretrato

SEZIONE IV - ALTRE DISPOSIZIONI

1. Sistemi di tutela istituzionale
2. Definizione di default

Capitolo 4 - RISCHIO DI CREDITO – METODO IRB

SEZIONE I - FONTI NORMATIVE

SEZIONE II - PROCEDIMENTI AMMINISTRATIVI

SEZIONE III - ESERCIZIO DELLE DISCREZIONALITÀ NAZIONALI

1. Esposizioni garantite da immobili. Innalzamento della LGD
2. Esposizioni in strumenti di capitale
3. Default di un debitore. Soglia di rilevanza delle obbligazioni creditizie in arretrato

SEZIONE IV - LINEE DI ORIENTAMENTO

1. Organizzazione e sistema dei controlli
2. Il processo del *rating* nell'ambito del gruppo bancario
3. Condizioni per valutare i requisiti dell'esperienza precedente nell'uso dell'IRB
4. Sistemi informativi
5. Estensione progressiva dei metodi IRB

6. Quantificazione dei parametri di rischio
7. Criteri di classificazione dei finanziamenti specializzati
8. Istanza di autorizzazione all'utilizzo dell'IRB

SEZIONE V – ALTRE DISPOSIZIONI

Allegato A - SISTEMI INFORMATIVI

Allegato B - CRITERI PER LA CLASSIFICAZIONE DEI FINANZIAMENTI SPECIALIZZATI

Allegato C - DOCUMENTAZIONE PER I METODI IRB

Allegato D - SCHEDE MODELLO

Capitolo 5 - TECNICHE DI ATTENUAZIONE DEL RISCHIO DI CREDITO (CRM)

SEZIONE I - FONTI NORMATIVE

SEZIONE II - PROCEDIMENTI AMMINISTRATIVI

SEZIONE III - ESERCIZIO DELLE DISCREZIONALITÀ NAZIONALI

Capitolo 6 - OPERAZIONI DI CARTOLARIZZAZIONE

SEZIONE I - FONTI NORMATIVE

1. Premessa

SEZIONE II - PROCEDIMENTI AMMINISTRATIVI

SEZIONE III - ESERCIZIO DELLE DISCREZIONALITÀ NAZIONALI

SEZIONE IV - LINEE DI ORIENTAMENTO

SEZIONE V - ALTRE DISPOSIZIONI

1. Requisiti generali
2. Requisiti specifici
3. Supporto implicito

Allegato A - MODULO INFORMATIVO SUL SIGNIFICATIVO TRASFERIMENTO DEL RISCHIO

Capitolo 7 - RISCHIO DI CONTROPARTE E RISCHIO DI AGGIUSTAMENTO DELLA VALUTAZIONE DEL CREDITO

SEZIONE I - FONTI NORMATIVE

SEZIONE II - PROCEDIMENTI AMMINISTRATIVI

SEZIONE III - ESERCIZIO DELLE DISCREZIONALITÀ NAZIONALI

Capitolo 8 - RISCHIO OPERATIVO

SEZIONE I - FONTI NORMATIVE

SEZIONE II - PROCEDIMENTI AMMINISTRATIVI

SEZIONE III - ESERCIZIO DELLE DISCREZIONALITÀ NAZIONALI

Capitolo 9 - RISCHIO DI MERCATO E RISCHIO DI REGOLAMENTO

SEZIONE I - FONTI NORMATIVE

SEZIONE II - PROCEDIMENTI AMMINISTRATIVI

SEZIONE III - ESERCIZIO DELLE DISCREZIONALITÀ NAZIONALI

SEZIONE IV – ALTRE DISPOSIZIONI

Capitolo 10 - GRANDI ESPOSIZIONI

SEZIONE I - FONTI NORMATIVE

SEZIONE II - PROCEDIMENTI AMMINISTRATIVI

SEZIONE III - ESERCIZIO DELLE DISCREZIONALITÀ NAZIONALI

SEZIONE IV - LINEE DI ORIENTAMENTO

1. Gruppo di clienti connessi
2. Esposizioni connesse alla prestazione di servizi di trasferimento fondi e di compensazione, regolamento e custodia di strumenti finanziari.

SEZIONE V - REGOLE ORGANIZZATIVE E PROVVEDIMENTI

1. Regole organizzative in materia di grandi esposizioni
2. Esposizioni verso soggetti del sistema bancario ombra
3. Provvedimenti della Banca centrale europea o della Banca d'Italia

Capitolo 11 - LIQUIDITÀ

SEZIONE I - FONTI NORMATIVE

SEZIONE II - PROCEDIMENTI AMMINISTRATIVI

SEZIONE III - ESERCIZIO DELLE DISCREZIONALITÀ NAZIONALI

1. Deroga all'applicazione delle regole di liquidità su base individuale
2. Requisito di copertura della liquidità
3. Requisito di finanziamento stabile
4. Segnalazioni per il monitoraggio del rischio di liquidità
5. Disposizioni transitorie

Allegato A – ADEMPIMENTI PER LE BANCHE SOGGETTE ALLA SUPERVISIONE DIRETTA DELLA BANCA D' ITALIA

Capitolo 12 - INDICE DI LEVA FINANZIARIA

SEZIONE I - FONTI NORMATIVE

SEZIONE II – PROCEDIMENTI AMMINISTRATIVI

SEZIONE III – ESERCIZIO DELLE DISCREZIONALITÀ NAZIONALI

Capitolo 13 - INFORMATIVA AL PUBBLICO

SEZIONE I - FONTI NORMATIVE

SEZIONE II - ALTRE DISPOSIZIONI

1. Obblighi di informativa ai sensi della Parte Otto del CRR: criteri generali
2. Informativa sulle attività impegnate e non impegnate
3. Informativa relativa al coefficiente di copertura della liquidità
4. Informativa relativa alle disposizioni transitorie per l'attenuazione dell'impatto dell'IFRS 9 sui fondi propri
5. Informativa sulle esposizioni deteriorate e oggetto di misure di correzione

Capitolo 14 - DISPOSIZIONI TRANSITORIE IN MATERIA DI FONDI PROPRI

SEZIONE I - DISPOSIZIONI DI CARATTERE GENERALE

1. Premessa
2. Fonti normative
3. Procedimenti amministrativi

SEZIONE II - DISPOSIZIONI TRANSITORIE

1. Requisiti di fondi propri (art. 465 CRR)
2. Perdite non realizzate misurate al valore equo (art. 467 CRR)
3. Profitti non realizzati misurati al valore equo (art. 468 CRR)
4. Profitti e perdite su derivati passivi valutati al valore equo derivanti da variazioni del proprio merito di credito (art. 468, par. 4 CRR)
5. Deduzioni dagli elementi del capitale primario di classe 1 ed esenzioni (articoli da 469 a 473 CRR)
6. Deduzioni dagli elementi aggiuntivi di classe 1 (artt. 474 e 475 CRR)
7. Deduzioni dagli elementi di classe 2 (artt. 476 e 477 CRR)
8. Interessi di minoranza; strumenti aggiuntivi di classe 1 e strumenti di classe 2 emessi da filiazioni (artt. 479 e 480 CRR)
9. Filtri e deduzioni aggiuntivi (art. 481 CRR)
10. Limiti al *grandfathering* degli elementi del capitale primario di classe 1, degli elementi aggiuntivi di classe 1 e degli elementi di classe 2 (articoli da 484 a 488)

Allegato A - FILTRI NAZIONALI

PARTE TERZA - ALTRE DISPOSIZIONI DI VIGILANZA PRUDENZIALE

Capitolo 1 - PARTECIPAZIONI DETENIBILI DALLE BANCHE E DAI GRUPPI BANCARI

SEZIONE I - DISPOSIZIONI DI CARATTERE GENERALE

1. Premessa
2. Fonti normative

3. Definizioni
4. Destinatari della disciplina
5. Procedimenti amministrativi

SEZIONE II - LIMITE GENERALE AGLI INVESTIMENTI IN PARTECIPAZIONI E IN IMMOBILI

1. Limite generale
2. Modalità di calcolo

SEZIONE III - LIMITI DELLE PARTECIPAZIONI DETENIBILI IN IMPRESE NON FINANZIARIE

1. Casi di superamento dei limiti

SEZIONE IV - PARTECIPAZIONI ACQUISITE NELL'AMBITO DELL'ATTIVITÀ DI COLLOCAMENTO E GARANZIA, IN IMPRESE IN TEMPORANEA DIFFICOLTÀ FINANZIARIA E PER RECUPERO CREDITI

1. Attività di collocamento e garanzia
2. Partecipazioni in imprese in temporanea difficoltà finanziaria
3. Partecipazioni acquisite per recupero crediti

SEZIONE V - PARTECIPAZIONI IN BANCHE, IN IMPRESE FINANZIARIE, IN IMPRESE ASSICURATIVE E IN IMPRESE STRUMENTALI

1. Autorizzazioni
2. Criteri di autorizzazione
3. Procedimento e comunicazioni

SEZIONE VI - INVESTIMENTI INDIRETTI IN EQUITY

1. Premessa
2. Definizioni e criteri di classificazione degli investimenti
3. Politiche aziendali
4. Trattamento prudenziale

SEZIONE VII - REGOLE ORGANIZZATIVE E DI GOVERNO SOCIETARIO

SEZIONE VIII - BANCHE DI CREDITO COOPERATIVO E BANCHE DI GARANZIA COLLETTIVA

SEZIONE IX - COMUNICAZIONI

Allegato A - PARTECIPAZIONI IN IMPRESE NON FINANZIARIE – PARTECIPAZIONI IN SOGGETTI DI NATURA FINANZIARIA E IN IMPRESE STRUMENTALI

Capitolo 2 - COMUNICAZIONI ALLA BANCA D' ITALIA

SEZIONE I - DISPOSIZIONI DI CARATTERE GENERALE

1. Premessa
2. Fonti normative
3. Destinatari della disciplina

SEZIONE II - COMUNICAZIONI

1. Comunicazioni dell'organo con funzione di controllo
2. Comunicazioni dei soggetti incaricati della revisione legale dei conti
3. Comunicazioni relative ai soggetti incaricati della revisione legale dei conti

Capitolo 3 - OBBLIGAZIONI BANCARIE GARANTITE

SEZIONE I - DISPOSIZIONI DI CARATTERE GENERALE

1. Premessa
2. Fonti normative
3. Definizioni
4. Destinatari della disciplina
5. Procedimenti amministrativi

SEZIONE II - DISCIPLINA DELLE OBBLIGAZIONI BANCARIE GARANTITE

1. Requisiti delle banche emittenti e/o cedenti
2. Limiti alla cessione
3. Modalità di integrazione degli attivi ceduti
4. Trattamento prudenziale
5. Responsabilità e controlli

Capitolo 4 - BANCHE IN FORMA COOPERATIVA

SEZIONE I - DISPOSIZIONI DI CARATTERE GENERALE

1. Premessa
2. Fonti normative
3. Definizioni
4. Destinatari della disciplina

SEZIONE II – VALORE DELL'ATTIVO DELLE BANCHE POPOLARI

1. Criteri e modalità di determinazione del valore dell'attivo

SEZIONE III – RIMBORSO DEGLI STRUMENTI DI CAPITALE

1. Limiti al rimborso di strumenti di capitale

Allegato A – PROSPETTO IDENTIFICATIVO DELL'ATTIVO INDIVIDUALE E CONSOLIDATO

Capitolo 5- BANCHE DI CREDITO COOPERATIVO

SEZIONE I - DISPOSIZIONI DI CARATTERE GENERALE

1. Premessa
2. Fonti normative
3. Definizioni
4. Destinatari della disciplina
5. Procedimenti amministrativi

SEZIONE II – STRUTTURA

1. Denominazione
2. Forma giuridica e azioni
3. Soci
4. Competenza territoriale
5. Modifiche statutarie e trasformazioni

SEZIONE III – OPERATIVITÀ

1. Operatività prevalente a favore dei soci
2. Operatività con non soci e fuori della zona di competenza territoriale
3. Attività esercitabili
4. Partecipazioni

SEZIONE IV – DESTINAZIONE DEGLI UTILI E RISTORNI

SEZIONE V – DISPOSIZIONI TRANSITORIE

Capitolo 6 – GRUPPO BANCARIO COOPERATIVO

SEZIONE I - DISPOSIZIONI DI CARATTERE GENERALE

1. Premessa
2. Fonti normative
3. Definizioni
4. Destinatari della disciplina
5. Procedimenti amministrativi

SEZIONE II – COMPOSIZIONE DEL GRUPPO BANCARIO COOPERATIVO E REQUISITI DELLA CAPOGRUPPO

1. Composizione del gruppo bancario cooperativo
2. Capogruppo
3. Società del gruppo
4. Sottogruppi territoriali
5. Gruppo provinciale

SEZIONE III – CONTRATTO DI COESIONE E GARANZIA IN SOLIDO

1. Contenuto minimo del contratto di coesione
2. Caratteristiche della garanzia
3. Criteri e condizioni di adesione al gruppo bancario cooperativo

SEZIONE IV – STATUTI

1. Statuto della capogruppo
2. Statuto delle banche affiliate
3. Gruppi provinciali

SEZIONE V – COSTITUZIONE DEL GRUPPO BANCARIO COOPERATIVO

1. Accertamento dei requisiti per la costituzione del gruppo
2. Adempimenti successivi
3. Prima applicazione

Capitolo 7 - VIGILANZA INFORMATIVA SU BASE INDIVIDUALE E CONSOLIDATA

SEZIONE I - DISPOSIZIONI DI CARATTERE GENERALE

1. Premessa
2. Fonti normative
3. Destinatari della disciplina

SEZIONE II – SEGNALAZIONI

1. Matrice dei conti
2. Segnalazioni prudenziali
3. Segnalazioni statistiche su base consolidata
4. Centrale dei Rischi
5. Perdite sulle posizioni in *default*
6. Organi sociali
7. Sistemi di remunerazione
8. Archivio elettronico delle partecipazioni
9. Rilevazione analitica dei tassi di interesse

SEZIONE III –BILANCIO DELL’IMPRESA E BILANCIO CONSOLIDATO

Capitolo 8 - VIGILANZA ISPETTIVA

SEZIONE I – DISPOSIZIONI DI CARATTERE GENERALE

1. Premessa
2. Fonti normative
3. Destinatari della disciplina

SEZIONE II – DISCIPLINA DEGLI ACCERTAMENTI ISPETTIVI

1. Svolgimento degli accertamenti
2. Comunicazione degli esiti ispettivi

*Capitolo 9 – CONCESSIONE DI FINANZIAMENTI DA PARTE DI SOCIETÀ VEICOLO PER LA
CARTOLARIZZAZIONE EX LEGGE 130/1999*

SEZIONE I - DISPOSIZIONI DI CARATTERE GENERALE

1. Premessa
2. Fonti normative
3. Definizioni
4. Destinatari della disciplina

SEZIONE II - OBBLIGHI DEGLI INTERMEDIARI

1. Mantenimento di un significativo interesse economico
2. Criteri di selezione dei prenditori
3. Informativa agli investitori
4. Controlli del *servicer*

Capitolo 10 – INVESTIMENTI IN IMMOBILI

SEZIONE I - DISPOSIZIONI DI CARATTERE GENERALE

1. Premessa
2. Fonti normative
3. Definizioni
4. Destinatari della disciplina
5. Procedimenti amministrativi

SEZIONE II – DISCIPLINA PRUDENZIALE

1. Immobili acquisibili
2. Regole organizzative e di governo societario
3. Limite agli investimenti immobiliari e casi di superamento
4. Provvedimenti

SEZIONE III – SOCIETÀ IMMOBILIARI SPECIALIZZATE

1. Orientamenti applicabili in materia di società immobiliari

Capitolo 11 – ATTIVITÀ DI RISCHIO E CONFLITTI DI INTERESSI NEI CONFRONTI DI SOGGETTI COLLEGATI

SEZIONE I - DISPOSIZIONI DI CARATTERE GENERALE

1. Premessa
2. Fonti normative
3. Definizioni
4. Destinatari della disciplina
5. Procedimenti amministrativi

SEZIONE II – LIMITI ALLE ATTIVITÀ DI RISCHIO

1. Limiti prudenziali
2. Modalità di calcolo
3. Casi di superamento
4. Banche di credito cooperativo e banche di garanzia collettiva

SEZIONE III – PROCEDURE DELIBERATIVE

1. Premessa e criteri generali
2. Iter di definizione delle procedure

3. Le procedure per il compimento di operazioni con soggetti collegati

SEZIONE IV – CONTROLLI

1. Controlli interni e responsabilità degli organi aziendali

SEZIONE IV – CONTROLLI

SEZIONE V – COMUNICAZIONI E INTERVENTI

1. Segnalazioni di vigilanza
2. Censimento dei soggetti collegati
3. Provvedimenti della Banca d'Italia

ALLEGATO A – LIMITI PRUDENZIALI ALLE ATTIVITÀ DI RISCHIO VERSO SOGGETTI COLLEGATI

ALLEGATO B – METODOLOGIE DI CALCOLO PER L'IDENTIFICAZIONE DELLE "OPERAZIONI DI MAGGIORE RILEVANZA"

Capitolo 12 – MISURE BASATE SULLE CARATTERISTICHE DEI CLIENTI O DEI FINANZIAMENTI

SEZIONE I - DISPOSIZIONI DI CARATTERE GENERALE

1. Premessa
2. Fonti normative
3. Definizioni
4. Destinatari della disciplina

SEZIONE II – MISURE MACROPRUDENZIALI BASATE SULLE CARATTERISTICHE DEI CLIENTI E DEI FINANZIAMENTI

1. Caratteristiche delle misure
2. Criteri per l'attivazione delle misure
3. Notifica al CERS e richiesta di riconoscimento delle misure borrower-based da parte di altri Stati comunitari
4. Riconoscimento delle misure borrower-based adottate da altri Stati comunitari

PARTE QUARTA - DISPOSIZIONI PER INTERMEDIARI PARTICOLARI

Capitolo 1 - BANCOPOSTA

SEZIONE I - DISPOSIZIONI DI CARATTERE GENERALE

1. Premessa
2. Fonti normative
3. Definizioni
4. Destinatari della disciplina
5. Procedimenti amministrativi

SEZIONE II - DISPOSIZIONI DI VIGILANZA PER IL BANCOPOSTA

1. Attività di bancoposta
2. La separazione contabile
3. La separazione patrimoniale
4. La separazione organizzativa, il governo societario e le remunerazioni
5. Sistema dei controlli interni e affidamento di funzioni a Poste
6. Succursali e attività fuori sede
7. Prestazione dei servizi senza stabilimento all'estero
8. Modifiche del Patrimonio Bancoposta

SEZIONE III - ALTRE DISPOSIZIONI APPLICABILI

1. Premessa
2. Disposizioni applicabili

Parte I – Recepimento in Italia della CRD IV

Titolo IV - Governo societario, controlli interni, gestione dei rischi

Capitolo 3 – Il sistema dei controlli interni

TITOLO IV

Capitolo 3

IL SISTEMA DEI CONTROLLI INTERNI

TITOLO IV – Capitolo 3

IL SISTEMA DEI CONTROLLI INTERNI

SEZIONE I

DISPOSIZIONI PRELIMINARI E PRINCIPI GENERALI

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, ecc.). Inoltre, alle banche che utilizzano, a fini prudenziali, sistemi interni di misurazione dei rischi diversi da quelli di base o standardizzati (1), 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 di governo e controllo delle banche, quali le disposizioni di natura organizzativa in materia di: governo societario; *information and communication technology*; assetti proprietari; requisiti degli esponenti aziendali; trasparenza e correttezza delle relazioni tra banche e clienti; attività e servizi di investimento (2); prevenzione dell'utilizzo degli intermediari e degli altri soggetti che svolgono attività finanziaria a fini di riciclaggio e di finanziamento del terrorismo; 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 e formalizzata.

(1) Con riferimento al rischio operativo, il metodo standardizzato include anche il metodo di base.

(2) Per le banche che prestano servizi di investimento, si applicano inoltre le disposizioni in materia di controlli interni emanate in attuazione del Testo Unico della Finanza (TUF).

Parte I – Recepimento in Italia della CRD IV

Titolo IV - Governo societario, controlli interni, gestione dei rischi

Capitolo 3 – Il sistema dei controlli interni

Sezione I – Disposizioni preliminari e principi generali

Le banche applicano le disposizioni secondo il principio di proporzionalità, cioè tenuto conto del profilo di rischio della banca, della dimensione e complessità operative, della natura dell'attività svolta, della tipologia dei servizi prestati (3).

La Banca centrale europea o la Banca d'Italia, nell'ambito del processo di revisione e valutazione prudenziale, verificano la completezza, la adeguatezza, la funzionalità (in termini di efficienza ed efficacia), la affidabilità del sistema dei controlli interni delle banche.

2. Fonti normative

La materia è regolata dalle seguenti disposizioni del TUB:

- art. 51, il quale prevede che le banche inviino alla Banca d'Italia, con le modalità e i tempi da essa stabiliti, le segnalazioni periodiche nonché ogni dato e documento richiesti;
- art. 52-*bis*, comma 5, che attribuisce alla Banca d'Italia il potere di emanare disposizioni attuative in materia di sistemi interni di segnalazione delle violazioni;
- art. 53, comma 1, lett. d), che attribuisce alla Banca d'Italia il potere di emanare disposizioni di carattere generale in materia di organizzazione amministrativa e contabile e controlli interni delle banche;
- art. 67, comma 1, lett. d), il quale prevede che, al fine di esercitare la vigilanza consolidata, la Banca d'Italia impartisca alla capogruppo, con provvedimenti di carattere generale, disposizioni concernenti il gruppo complessivamente considerato o i suoi componenti aventi ad oggetto l'organizzazione amministrativa e contabile e i controlli interni;
- art. 120-*undecies*, che attribuisce alla Banca d'Italia il potere di emanare disposizioni attuative in materia di valutazione del merito creditizio del consumatore che deve essere svolta dalle banche prima della conclusione dei contratti di credito (4);
- art. 120-*duodecies*, che attribuisce alla Banca d'Italia il potere di emanare disposizioni attuative in materia di valutazione dei beni immobili residenziali ai fini della concessione di credito garantito da ipoteca (5);

(3) Nella declinazione del principio di proporzionalità le banche tengono conto dei seguenti criteri: a. le dimensioni, in termini di totale bilancio della banca e delle sue filiazioni, nell'ambito del perimetro di consolidamento prudenziale; b. la presenza geografica della banca e il volume delle sue attività in ogni paese; c. la forma giuridica della banca, incluso se essa fa parte di un gruppo e, in tal caso, la valutazione della proporzionalità relativa al gruppo; d. se la banca è quotata o meno in borsa; e. se la banca è autorizzata a usare modelli interni per la misurazione dei requisiti; f. la tipologia di attività e di servizi autorizzati prestati dalla banca; g. il modello di business e la strategia di base; la natura e la complessità delle attività nonché la struttura organizzativa della banca; h. la strategia in materia di rischio, la propensione al rischio e l'effettivo profilo di rischio della banca, tenendo in considerazione anche il risultato delle valutazioni del capitale e della liquidità nello SREP; i. gli assetti proprietari e la struttura di finanziamento della banca; j. la tipologia di clienti (ad esempio, clientela al dettaglio, società, istituzioni, piccole imprese, enti pubblici) e la complessità dei prodotti o dei contratti; k. le attività esternalizzate e i canali di distribuzione; l. i sistemi informatici disponibili, inclusi i sistemi di continuità e le attività di esternalizzazione in quest'area.

(4) Le disposizioni attuative dell'art.120-*undecies*, TUB sono contenute nel paragrafo 2, allegato A, delle presenti disposizioni.

(5) Le disposizioni attuative dell'art.120-*duodecies*, TUB sono contenute nel paragrafo 2, allegato A, delle presenti disposizioni.

Parte I – Recepimento in Italia della CRD IV

Titolo IV - Governo societario, controlli interni, gestione dei rischi

Capitolo 3 – Il sistema dei controlli interni

Sezione I – Disposizioni preliminari e principi generali

- art. 124-*bis*, che attribuisce alla Banca d'Italia il potere di emanare disposizioni attuative in materia di valutazione del merito creditizio del consumatore che deve essere svolta dalle banche prima della conclusione dei contratti di credito (6);

e inoltre:

- dal decreto del Ministro dell'Economia e delle finanze, Presidente del CICR del 3 febbraio 2011 in materia, tra l'altro, di verifica del merito creditizio del consumatore nell'ambito del credito ai consumatori;
- dalla 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.

Vengono inoltre in rilievo:

- la CRD;
- il CRR;
- la direttiva 2014/17/UE;
- i seguenti documenti pubblicati da istituzioni comunitarie e organismi internazionali: Committee of European Banking Supervisors (CEBS), “*Guidelines on the management of operational risks in market-related activities*”, 12 ottobre 2010; Basel Committee on Banking Supervision (BCBS), “*Fair value measurement and modelling: An assessment of challenges and lessons learned from market stress*”, 12 giugno 2008; BCBS, “*The internal audit function in banks*”, 28 giugno 2012; BCBS, “*Core Principles for Effective Banking Supervision*”, 14 settembre 2012; BCBS, “*Corporate governance principles for banks*”, 8 luglio 2015; Financial Stability Board (FSB), “*Enhancing Market and Institutional Resilience*”, 7 aprile 2008; FSB, “*Thematic Review on Risk Governance*”, 12 febbraio 2013; European Systemic Risk Board (ESRB), “*Raccomandazione in materia di prestiti in valuta estera (ESRB/2011/1)*”, 21 settembre 2011; ESRB, “*Raccomandazione relativa al finanziamento degli enti creditizi (ESRB/2012/2)*”, 20 dicembre 2012; EBA, “*Orientamenti in materia di pratiche di gestione del rischio di credito e di rilevazione contabile delle perdite attese su crediti degli enti creditizi (EBA/GL/2017/06)*”, 20 settembre 2017; EBA, “*Orientamenti sulla governance interna*” adottati ai sensi dell'articolo 74, par. 1, della direttiva CRD; EBA, “*Orientamenti sulla gestione del rischio di tasso di interesse derivante da attività diverse dalla negoziazione (non-trading activities)*” (EBA/GL/2018/02), 18 luglio 2018; EBA, “*Orientamenti relativi alle prove di stress degli enti*” (EBA/GL/2018/04), 19 luglio 2018; EBA, “*Orientamenti in materia di esternalizzazione*” (EBA/GL/2019/02), 25 febbraio 2019; EBA, “*Orientamenti in materia di concessione e monitoraggio dei prestiti*” (EBA/GL/2020/06), 29 maggio 2020.

3. Definizioni

Ai fini delle presenti disposizioni si intendono per:

- “*organo con funzione di supervisione strategica*”: l'organo con funzione di supervisione strategica come definito nel Capitolo 1;

(6) Le disposizioni attuative dell'art.124-*bis*, TUB sono contenute nel paragrafo 2, allegato A, delle presenti disposizioni.

Parte I – Recepimento in Italia della CRD IV

Titolo IV - Governo societario, controlli interni, gestione dei rischi

Capitolo 3 – Il sistema dei controlli interni

Sezione I – Disposizioni preliminari e principi generali

- “*organo con funzione di gestione*”: l’organo con funzione di gestione come definito nel Capitolo 1;
- “*organo con funzione di controllo o organo di controllo*”: l’organo con funzione di controllo o l’organo di controllo come definito nel Capitolo 1;
- “*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;
- “*funzione aziendale*”: l’insieme dei compiti e delle responsabilità assegnate per l’espletamento di una determinata fase dell’attività aziendale. Sulla base della rilevanza della fase svolta, la funzione è incardinata presso una specifica unità organizzativa;
- “*funzione antiriciclaggio*”: la funzione definita dalle disposizioni della Banca d’Italia in materia di organizzazione, procedure e controlli interni volti a prevenire l’utilizzo degli intermediari a fini di riciclaggio e di finanziamento del terrorismo del 26 marzo 2019;
- “*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*) (7);
- “*funzioni di controllo*”: l’insieme delle funzioni che per disposizione legislativa, regolamentare, statutaria o di autoregolamentazione hanno compiti di controllo;
- “*funzione essenziale o importante*”: una funzione per la quale risulta verificata almeno una delle seguenti condizioni:
 - i. 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 nel continuo alle condizioni e agli obblighi derivanti dalla sua autorizzazione o agli obblighi previsti dalla disciplina di vigilanza;
 - ii. riguarda funzioni relative ad attività sottoposte a riserva di legge, nella misura in cui la prestazione di tali attività richiede l’autorizzazione da parte di un’autorità di vigilanza;
 - iii. riguarda compiti operativi delle funzioni aziendali di controllo, a meno che la valutazione dell’essenzialità e dell’importanza della funzione svolta dalla banca non stabilisca che la mancata o inadeguata esecuzione di questi compiti operativi non avrebbe impatti negativi sull’efficacia delle funzioni aziendali di controllo.
- “*cultura del rischio / dei rischi*”: l’insieme delle regole, degli atteggiamenti e dei comportamenti della banca che incidono sul grado di consapevolezza, sull’assunzione e gestione dei rischi, nonché sulle attività di controllo, che determinano le decisioni in materia

(7) Tra le funzioni aziendali di controllo rientrano anche la funzione antiriciclaggio, la funzione di convalida come disciplinata dalle relative disposizioni e la funzione di controllo dei rischi ICT e di sicurezza come disciplinata dal Capitolo 4, Sez. II, par. 4.

Parte I – Recepimento in Italia della CRD IV

Titolo IV - Governo societario, controlli interni, gestione dei rischi

Capitolo 3 – Il sistema dei controlli interni

Sezione I – Disposizioni preliminari e principi generali

di rischi. La cultura del rischio influenza le decisioni degli organi aziendali e del personale nello svolgimento quotidiano delle proprie attività e influisce sui rischi assunti dalla banca;

- “*personale*”: il personale come definito nella disciplina della Banca d’Italia in materia di politiche e prassi di remunerazione e incentivazione (Parte I, Tit. IV, Cap. 2, Sez. I, par. 3);
- “*processo di gestione dei rischi*”: l’insieme delle regole, delle procedure, delle risorse (umane, tecnologiche e organizzative) e delle attività di controllo volte a identificare, misurare o valutare, monitorare, prevenire o attenuare nonché comunicare ai livelli gerarchici appropriati tutti i rischi assunti o assumibili (8) nei diversi segmenti, a livello di portafoglio di impresa e di gruppo, relativi ad attività in bilancio e fuori bilancio, cogliendone, in una logica integrata e sulla base di valutazioni di tipo *top-down* e *bottom-up*, anche le interrelazioni reciproche e con l’evoluzione del contesto esterno;
- “*risk appetite framework*” – “RAF” (sistema degli obiettivi di rischio): il quadro di riferimento che definisce – in coerenza con il massimo rischio assumibile, il *business model* e il piano strategico – la propensione al rischio, le soglie di tolleranza, i limiti di rischio, le politiche di governo dei rischi, i processi di riferimento necessari per definirli e attuarli (cfr. Allegato C). Si forniscono, di seguito, le definizioni dei concetti rilevanti ai fini del RAF:
 - *risk capacity (massimo rischio assumibile)*: il livello massimo di rischio che una banca è tecnicamente in grado di assumere senza violare i requisiti regolamentari o gli altri vincoli imposti dagli azionisti o dall’autorità di vigilanza;
 - *risk appetite (obiettivo di rischio o propensione al rischio)*: il livello di rischio (complessivo e per tipologia) che la banca intende assumere, nel limite del massimo rischio assumibile, per il perseguimento dei suoi obiettivi strategici;
 - *risk tolerance (soglia di tolleranza)*: la devianza massima dal *risk appetite* consentita; la soglia di tolleranza è fissata in modo da assicurare in ogni caso alla banca margini sufficienti per operare, anche in condizioni di stress, entro il massimo rischio assumibile. Nel caso in cui sia consentita l’assunzione di rischio oltre l’obiettivo di rischio fissato, fermo restando il rispetto della soglia di tolleranza, sono individuate le azioni gestionali necessarie per ricondurre il rischio assunto entro l’obiettivo prestabilito;
 - *risk profile (rischio effettivo)*: il rischio effettivamente assunto, misurato in un determinato istante temporale;
 - *risk limits (limiti di rischio)*: l’articolazione degli obiettivi di rischio in limiti operativi, definiti, in linea con il principio di proporzionalità, per tipologie di rischio, unità e o linee di *business*, linee di prodotto, tipologie di clienti;
- “*esternalizzazione*”: l’accordo in qualsiasi forma tra una banca e un fornitore di servizi in base al quale il fornitore realizza un processo, un servizio o un’attività che sarebbe altrimenti svolto dalla stessa banca;

(8) Devono essere considerati, a titolo esemplificativo e non esaustivo, il rischio strategico, il rischio di credito, il rischio di controparte, il rischio di concentrazione, il rischio di mercato, il rischio di tasso di interesse, il rischio operativo, il rischio di liquidità, il rischio connesso alla quota di attività vincolate (*asset encumbrance*), il rischio di reputazione, il rischio di modello, i rischi derivanti da prestiti in valuta estera, il rischio paese, il rischio di trasferimento nonché i rischi derivanti dall’ambiente macroeconomico in cui la banca opera anche con riferimento all’andamento del ciclo economico e i rischi di sostenibilità (ambientali, sociali o di *governance*, ESG). 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.

Parte I – Recepimento in Italia della CRD IV

Titolo IV - Governo societario, controlli interni, gestione dei rischi

Capitolo 3 – Il sistema dei controlli interni

Sezione I – Disposizioni preliminari e principi generali

- “*subesternalizzazione*”: la situazione in cui il fornitore di servizi nell’ambito di un accordo di esternalizzazione trasferisce ulteriormente una funzione esternalizzata a un altro fornitore di servizi;
- “*fornitore di servizi*”: un soggetto terzo che realizza, in tutto o in parte, un processo, un servizio o un’attività esternalizzata nell’ambito di un accordo di esternalizzazione;
- “*servizi cloud*”: servizi in *cloud computing*, ossia un modello che consente l’accesso in rete diffuso, conveniente e su richiesta a un gruppo condiviso di risorse informatiche configurabili (ad esempio reti, server, memorie, applicazioni e servizi), che possono essere forniti e messi a disposizione rapidamente con un minimo di attività gestionale o di interazione con il fornitore del servizio. Si forniscono, di seguito, le definizioni delle diverse tipologie rilevanti di *cloud computing*:
 - *Cloud pubblico (public cloud)*: infrastruttura *cloud* in cui i servizi sono erogati a un vasto numero di clienti con funzionalità offerte in maniera aperta e condivisa;
 - *Cloud privato (private cloud)*: infrastruttura *cloud* disponibile per l’utilizzo esclusivo da parte della banca;
 - *Cloud di comunità (community cloud)*: infrastruttura *cloud* disponibile per l’utilizzo esclusivo da parte di una specifica comunità di banche, compresa una pluralità di banche e altre società appartenenti a un unico gruppo;
 - *Cloud ibrido (hybrid cloud)*: infrastruttura *cloud* costituita da due o più infrastrutture *cloud* distinte.

4. Destinatari della disciplina

Le presenti disposizioni si applicano:

- alle banche autorizzate in Italia, ad eccezione delle succursali di banche extracomunitarie aventi sede negli Stati indicati nell’Allegato A delle Disposizioni introduttive (9);
- 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 aventi sede negli Stati indicati nell’Allegato A delle Disposizioni introduttive, secondo quanto previsto dalla Sezione VII.

5. Procedimenti amministrativi

Si indicano di seguito i procedimenti amministrativi relativi al presente Capitolo:

- *autorizzazione alla deroga, in tutto o in parte, all’applicazione su base individuale degli obblighi relativi al sistema dei controlli interni per le banche che sono state autorizzate alla*

(9) Per le banche che prestano servizi di investimento, si applicano inoltre le disposizioni in materia di controlli interni emanate in attuazione del Testo Unico della Finanza (TUF).

Parte I – Recepimento in Italia della CRD IV

Titolo IV - Governo societario, controlli interni, gestione dei rischi

Capitolo 3 – Il sistema dei controlli interni

Sezione I – Disposizioni preliminari e principi generali

deroga all'applicazione su base individuale dei requisiti prudenziali di cui all'art. 7 del CRR (ai sensi dell'art. 53-bis, co. 1, lettera d, TUB) (termine: 120 giorni).

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 i limiti indicati nel quadro di riferimento per la determinazione della propensione al rischio della banca (*Risk Appetite Framework* - "RAF") (cfr. Allegato C);
- 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 (10);
- 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 aziendali e delle loro interrelazioni; orienta i mutamenti delle linee strategiche e delle politiche aziendali e consente 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 aziendali 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 identificare, misurare, comunicare, gestire i rischi.

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

- assicurare la completezza, l'adeguatezza, la funzionalità (in termini di efficienza ed efficacia), l'affidabilità del processo di gestione dei rischi e la sua coerenza con il RAF;
- prevedere attività di controllo diffuse a ogni segmento operativo e livello gerarchico (11);
- 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;

(10) Cfr. Capitolo 4 (Il sistema informativo).

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

Parte I – Recepimento in Italia della CRD IV

Titolo IV - Governo societario, controlli interni, gestione dei rischi

Capitolo 3 – Il sistema dei controlli interni

Sezione I – Disposizioni preliminari e principi generali

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 a esso attribuite;
- il processo di gestione dei rischi è efficacemente integrato. Sono considerati parametri di integrazione, riportati a titolo esemplificativo e non esaustivo: la diffusione di un linguaggio comune nella gestione dei rischi a tutti i livelli della banca; l'adozione di metodi e strumenti di rilevazione e valutazione tra di loro coerenti (ad es., un'unica tassonomia dei processi e un'unica mappa dei rischi); la definizione di modelli di reportistica dei rischi, al fine di favorirne la comprensione e la corretta valutazione, anche in una logica integrata; l'individuazione di momenti formalizzati di coordinamento ai fini della pianificazione delle rispettive attività; la previsione di flussi informativi su base continuativa tra le diverse funzioni in relazione ai risultati delle attività di controllo di propria pertinenza; la condivisione nella individuazione delle azioni di rimedio;
- 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 risultanze di valutazioni basate su metodi quantitativi sono integrate da valutazioni qualitative per mitigare il rischio di modello;
- le procedure operative e di controllo devono: minimizzare i rischi legati a frodi o infedeltà dei dipendenti; prevenire o, laddove non sia possibile, attenuare i potenziali conflitti d'interesse; prevenire il coinvolgimento, anche inconsapevole, in fatti di riciclaggio, usura o di finanziamento al terrorismo;
- il sistema informativo rispetta la disciplina del Capitolo 4 (Il sistema informativo);
- i livelli di continuità operativa garantiti sono adeguati e conformi a quanto stabilito dal Capitolo 5 (La continuità operativa);
- la normativa e la documentazione siano costantemente aggiornate.

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.

Parte I – Recepimento in Italia della CRD IV

Titolo IV - Governo societario, controlli interni, gestione dei rischi

Capitolo 3 – Il sistema dei controlli interni

Sezione II – Il ruolo degli organi aziendali

SEZIONE II

IL RUOLO DEGLI ORGANI AZIENDALI

1. Premessa

Le banche assicurano la completezza, l'adeguatezza, la funzionalità e l'affidabilità del sistema dei controlli interni. In tale ambito, formalizzano il quadro di riferimento per la determinazione della propensione al rischio (*Risk Appetite Framework* - "RAF"), le politiche di governo dei rischi, il processo di gestione dei rischi, ne assicurano l'applicazione e procedono al loro riesame periodico per garantirne 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:

— definisce e approva:

- a. 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;
- b. gli indirizzi strategici 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;
- c. gli obiettivi di rischio, la soglia di tolleranza (ove identificata) e le politiche di governo dei rischi;
- d. le linee di indirizzo del sistema dei controlli interni, verificando che esso sia coerente con gli indirizzi strategici e la propensione al rischio stabiliti nonché sia in grado di cogliere l'evoluzione dei rischi aziendali e l'interazione tra gli stessi;
- e. 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);

— approva:

- a. la costituzione delle funzioni aziendali 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 valuta la compatibilità con gli indirizzi strategici e le politiche di governo dei rischi;

DISPOSIZIONI DI VIGILANZA PER LE BANCHE

Parte I – Recepimento in Italia della CRD IV

Titolo IV - Governo societario, controlli interni, gestione dei rischi

Capitolo 3 – Il sistema dei controlli interni

Sezione II – Il ruolo degli organi aziendali

- c. le politiche e i processi di valutazione delle attività aziendali, e, in particolare, degli strumenti finanziari, verificandone la costante adeguatezza; stabilisce altresì i limiti massimi 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 (1) (2) e ne valuta periodicamente il corretto funzionamento;
- e. il processo per l'approvazione di nuovi prodotti e servizi, l'avvio di nuove attività, l'inserimento in nuovi mercati (cfr. *infra*, par. 3);
- f. la politica aziendale in materia di esternalizzazione di funzioni aziendali (cfr. Sezione IV) (3);
- g. al fine di attenuare i rischi operativi e di reputazione della banca e favorire la diffusione di una corretta cultura dei rischi e dei controlli interni (4), un codice etico cui sono tenuti a uniformarsi i componenti degli organi aziendali e i dipendenti. Il codice definisce i principi di condotta (ad es., regole deontologiche e regole da osservare nei rapporti con i clienti) a cui deve essere improntata l'attività aziendale (5);
- h. i sistemi interni di segnalazione delle violazioni, secondo quanto previsto dalla Sezione VIII;
- i. il programma delle prove di stress, così come delineato dagli "Orientamenti relativi alle prove di stress degli enti" (EBA/GL/2018/04);

— assicura che:

- a. 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 (6);
- b. il sistema dei controlli interni e l'organizzazione aziendale siano costantemente uniformati ai principi indicati nella Sezione I e che le funzioni aziendali di controllo possiedano i requisiti e rispettino le previsioni della Sezione III. Nel caso emergano carenze o anomalie, promuove con tempestività l'adozione di idonee misure correttive e ne valuta l'efficacia, anche nel tempo mediante apposite procedure di *follow up*;

(1) Ai fini dell'utilizzo dei sistemi interni di misurazione dei rischi per la determinazione dei requisiti patrimoniali si applicano le specifiche disposizioni organizzative previste nella Parte tre, Titoli II, III, IV e VI del CRR, che disciplinano le varie tipologie di rischio rilevanti a fini prudenziali.

(2) Per processo di convalida si intende l'insieme formalizzato di attività, strumenti e procedure volti a valutare l'accuratezza delle stime di tutte le componenti rilevanti di rischio e a esprimere un giudizio in merito al regolare funzionamento, alla capacità predittiva e alla performance di un sistema interno di misurazione dei rischi non utilizzato a fini regolamentari.

(3) La politica di esternalizzazione è definita in conformità con quanto previsto alla Sezione 7 degli Orientamenti dell'EBA in materia di esternalizzazione.

(4) Una corretta cultura dei rischi promuove un ambiente in cui sono possibili una comunicazione e una partecipazione aperte e costruttive, che stimoli il dibattito e un'adeguata dialettica tra i dipendenti.

(5) Al riguardo, le banche fanno riferimento a quanto previsto alla Sezione 10 degli Orientamenti dell'EBA sulla *governance* interna.

(6) A questo fine, gli intermediari si attengono a quanto previsto nella Sezione 6.3 degli Orientamenti dell'EBA sulla *governance* interna.

DISPOSIZIONI DI VIGILANZA PER LE BANCHE

Parte I – Recepimento in Italia della CRD IV

Titolo IV - Governo societario, controlli interni, gestione dei rischi

Capitolo 3 – Il sistema dei controlli interni

Sezione II – Il ruolo degli organi aziendali

- c. l'attuazione del RAF sia coerente con gli obiettivi di rischio e la soglia di tolleranza (ove identificata) approvati; valuta periodicamente l'adeguatezza e l'efficacia del RAF e la compatibilità tra il rischio effettivo e gli obiettivi di rischio;
 - d. il piano strategico, il RAF, l'ICAAP, il programma delle prove di stress, i budget e il sistema dei controlli interni siano coerenti ed integrati, avuta anche presente l'evoluzione delle condizioni interne ed esterne in cui opera la banca;
 - e. la quantità e l'allocatione del capitale e della liquidità detenuti siano coerenti con la propensione al rischio, 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 attenuarli e ne assicura il controllo effettivo;
 - con cadenza almeno annuale, approva il programma di attività, compreso il piano di *audit* predisposto dalla funzione di revisione interna (cfr. Sezione III, par. 2), ed esamina le relazioni annuali predisposte dalle funzioni aziendali di controllo. Approva altresì il piano di *audit* pluriennale.

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 il RAF 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:

- 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.

Parte I – Recepimento in Italia della CRD IV

Titolo IV - Governo societario, controlli interni, gestione dei rischi

Capitolo 3 – Il sistema dei controlli interni

Sezione II – Il ruolo degli organi aziendali

3. Organo con funzione di gestione

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

Tale organo cura l'attuazione degli indirizzi strategici, del RAF e delle politiche di governo dei rischi definiti dall'organo con funzione di supervisione strategica ed è responsabile per l'adozione di tutti gli interventi necessari ad assicurare l'aderenza dell'organizzazione e del sistema dei controlli interni ai principi e requisiti di cui alle Sezioni I e III, monitorandone nel continuo il rispetto.

In particolare, l'organo con funzione di gestione:

- definisce e cura l'attuazione del processo di gestione dei rischi. In tale ambito:
 - a. stabilisce limiti operativi all'assunzione delle varie tipologie di rischio, coerenti con la propensione al rischio, 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. agevola lo sviluppo e la diffusione a tutti i livelli di una cultura del rischio integrata in relazione alle diverse tipologie di rischi ed estesa a tutta la banca (7). In particolare, sono 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. è responsabile dell'attuazione e della performance del programma delle prove di stress e assicura che siano assegnate e distribuite responsabilità chiare e risorse sufficienti e che tutti gli elementi del programma siano appropriatamente documentati e regolarmente aggiornati nelle procedure interne (8).

(7) A questo fine, le banche fanno riferimento a quanto previsto alla Sezione 9, paragrafo 98, degli Orientamenti dell'EBA sulla *governance* interna (EBA/GL/2017/11).

(8) Per i contenuti minimi del programma delle prove di stress e della relativa documentazione si rimanda agli Orientamenti dell'EBA relativi alle prove di stress degli enti (EBA/GL/2018/04).

DISPOSIZIONI DI VIGILANZA PER LE BANCHE

Parte I – Recepimento in Italia della CRD IV

Titolo IV - Governo societario, controlli interni, gestione dei rischi

Capitolo 3 – Il sistema dei controlli interni

Sezione II – Il ruolo degli organi aziendali

- definisce e cura l’attuazione del 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:
 - a. identifica in modo chiaro le condizioni per la sua applicazione (anche attraverso la definizione di nuovi prodotti / servizi / cambiamenti significativi) (9), in modo da assicurare il corretto coinvolgimento delle funzioni interessate;
 - b. assicura il rispetto della normativa applicabile e che prima dell’approvazione siano pienamente valutati – anche con il coinvolgimento della funzione di controllo dei rischi e della funzione di conformità – i rischi derivanti dalla nuova operatività, che detti rischi siano coerenti con la propensione al rischio e che la banca sia in grado di gestirli;
 - c. definisce le fasce di clientela a cui si intendono distribuire nuovi prodotti o servizi in relazione alla complessità degli stessi e a eventuali vincoli normativi esistenti;
 - d. consente di stimare gli impatti della nuova operatività in termini di costi, ricavi, risorse (umane, organizzative e tecnologiche) nonché di valutare gli impatti sulle procedure amministrative e contabili della banca;
 - e. individua le strutture e/o il personale responsabili e le eventuali modifiche da apportare all’organizzazione e al sistema dei controlli interni;
- definisce e cura l’attuazione della politica aziendale in materia di esternalizzazione di funzioni aziendali (cfr. Sezione IV);
- definisce e cura l’attuazione dei processi e delle metodologie di valutazione delle attività aziendali, e, in particolare, degli strumenti finanziari; ne cura il loro costante aggiornamento;
- 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 e la verifica del rispetto del RAF;
- nell’ambito del RAF, se è stata definita la soglia di tolleranza, autorizza il superamento della propensione al rischio entro il limite rappresentato dalla soglia di tolleranza e provvede a darne pronta informativa all’organo con funzione di supervisione strategica, individuando le azioni gestionali necessarie per ricondurre il rischio assunto entro l’obiettivo prestabilito;
- pone in essere le iniziative e gli interventi necessari per garantire nel continuo la completezza, l’adeguatezza, la funzionalità e l’affidabilità del sistema dei controlli interni e porta i risultati delle verifiche effettuate a conoscenza dell’organo con funzione di supervisione strategica;
- predispone e 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;
- assicura:
 - a. la coerenza del processo di gestione dei rischi con la propensione al rischio e le politiche di governo dei rischi, avuta anche presente l’evoluzione delle condizioni interne ed esterne in cui opera la banca;

(9) Sono oggetto di valutazione preventiva anche le modifiche derivanti da operazioni di fusione, acquisizione e altre operazioni societarie, nonché gli impatti sui processi e sui sistemi della banca che possono derivare dal trattare nuovi prodotti o avviare nuovi servizi.

Parte I – Recepimento in Italia della CRD IV

Titolo IV - Governo societario, controlli interni, gestione dei rischi

Capitolo 3 – Il sistema dei controlli interni

Sezione II – Il ruolo degli organi aziendali

- b. 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 al RAF 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:

- 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 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, adeguatezza, funzionalità e affidabilità del sistema dei controlli interni e del RAF.

Nell'espletamento di tale compito, l'organo con funzione di controllo vigila sul rispetto delle previsioni di cui i) alla presente Sezione, ii) alle Sezioni I e III e iii) al processo 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.

L'organo con funzione di controllo svolge, di norma, le funzioni dell'organismo di vigilanza – eventualmente istituito ai sensi del d.lgs. 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 del

Parte I – Recepimento in Italia della CRD IV

Titolo IV - Governo societario, controlli interni, gestione dei rischi

Capitolo 3 – Il sistema dei controlli interni

Sezione II – Il ruolo degli organi aziendali

medesimo decreto legislativo (10). Le banche possono affidare tali funzioni a un organismo appositamente istituito dandone adeguata motivazione.

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 (11).

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, vigila – nell'ambito della più generale attività di verifica del processo di gestione dei rischi – sulla completezza, adeguatezza, funzionalità, affidabilità, dei sistemi stessi e sulla loro rispondenza ai requisiti previsti dalla normativa.

5. Il coordinamento delle funzioni di controllo

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 (12), i soggetti incaricati della revisione legale dei conti, le funzioni di controllo.

L'ordinamento e le fonti di autoregolamentazione attribuiscono, poi, compiti di controllo a specifiche funzioni - diverse dalle funzioni aziendali 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 del d.lgs. 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.

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, diffuso a tutte le strutture interessate, nel quale sono definiti i compiti e le

(10) 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.

(11) Cfr. Capitolo 1, cui si rimanda per la descrizione dettagliata dei compiti e poteri dell'organo con funzione di controllo.

(12) Cfr. Capitolo 1, cui si rimanda per la descrizione dettagliata dei compiti e poteri dell'organo con funzione di controllo.

DISPOSIZIONI DI VIGILANZA PER LE BANCHE

Parte I – Recepimento in Italia della CRD IV

Titolo IV - Governo societario, controlli interni, gestione dei rischi

Capitolo 3 – Il sistema dei controlli interni

Sezione II – Il ruolo degli organi aziendali

responsabilità dei vari organi e funzioni 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 di controllo, le banche prestano attenzione a non alterare, anche nella sostanza, le responsabilità primarie degli organi aziendali sul sistema dei controlli interni.

Parte I – Recepimento in Italia della CRD IV

Titolo IV - Governo societario, controlli interni, gestione dei rischi

Capitolo 3 – Il sistema dei controlli interni

Sezione III – Funzioni aziendali di controllo

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*); 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:

- a) tali funzioni dispongono dell'autorità, delle risorse (umane, economiche, tecnologiche e informatiche, ecc.) e delle competenze necessarie per lo svolgimento dei loro compiti. Le funzioni sono dotate di sistemi informativi e di supporto adeguati e hanno accesso ai dati aziendali e a quelli esterni necessari per svolgere in modo appropriato i propri compiti. Le risorse economiche, eventualmente attivabili in autonomia, permettono, tra l'altro, alle funzioni aziendali di controllo di ricorrere a consulenze esterne. Il personale è adeguato per numero, competenze tecnico-professionali, aggiornamento, anche attraverso l'inserimento di programmi di formazione, anche esterni, 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 formalizza e incentiva programmi di rotazione delle risorse, tra le funzioni aziendali di controllo;
- b) i responsabili:
 - possiedono requisiti di professionalità adeguati;
 - sono collocati in posizione gerarchica e funzionale adeguata; in particolare, i responsabili delle funzioni di controllo dei rischi e di conformità alle norme sono collocati alle dirette dipendenze dell'organo con funzione di gestione o dell'organo con funzione di supervisione strategica; il responsabile della funzione di revisione interna è collocato sempre alle dirette dipendenze dell'organo con funzione di supervisione strategica;
 - non hanno responsabilità diretta di aree operative sottoposte a controllo né sono gerarchicamente subordinati ai responsabili di tali aree;
 - sono nominati e revocati (motivandone le ragioni) dall'organo con funzione di supervisione strategica, sentito l'organo con funzione di controllo (1). Il responsabile di funzioni aziendali di controllo può essere un componente dell'organo amministrativo, purché sia destinatario di specifiche deleghe in materia di controlli e non sia destinatario di altre deleghe che ne pregiudichino l'autonomia;
 - riferiscono direttamente agli organi aziendali e rispondono a tali organi per lo svolgimento dei propri compiti e responsabilità. In particolare, i responsabili della

(1) I responsabili delle funzioni aziendali di controllo sono nominati secondo procedure di selezione formalizzate.

Parte I – Recepimento in Italia della CRD IV

Titolo IV - Governo societario, controlli interni, gestione dei rischi

Capitolo 3 – Il sistema dei controlli interni

Sezione III – Funzioni aziendali di controllo

funzione di controllo dei rischi e della funzione di conformità alle norme hanno, in ogni caso, accesso diretto all'organo con funzione di supervisione strategica e all'organo con funzione di controllo e comunicano con essi senza restrizioni o intermediazioni; il responsabile della funzione di revisione interna ha accesso diretto all'organo con funzione di controllo e comunica con esso senza restrizioni o intermediazioni;

- c) il personale che partecipa alle funzioni aziendali di controllo non è 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 sono tra loro separate, sotto un profilo organizzativo. I rispettivi ruoli e responsabilità sono formalizzati;
- e) i criteri di remunerazione del personale che partecipa alle funzioni aziendali di controllo non ne compromettono l'obiettività e concorrono a creare un sistema di incentivi coerente con le finalità della funzione svolta (2).

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 a un'unica struttura lo svolgimento della funzione di conformità alle norme e della funzione di controllo dei rischi;
- affidare lo svolgimento delle funzioni aziendali di controllo all'esterno o all'interno del gruppo, secondo quanto previsto dalle disposizioni in materia di esternalizzazione contenute nella Sezione IV;
- affidare il ruolo di responsabile della funzione di controllo dei rischi e/o della funzione di conformità a un soggetto che svolge anche altri compiti, a condizione che ciò non sia fonte di possibili conflitti di interesse e siano rispettati tutti i requisiti previsti per i responsabili delle funzioni aziendali di controllo.

Tenuto conto che le 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.

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.

(2) Cfr. Capitolo 2.

Parte I – Recepimento in Italia della CRD IV

Titolo IV - Governo societario, controlli interni, gestione dei rischi

Capitolo 3 – Il sistema dei controlli interni

Sezione III – Funzioni aziendali 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 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, funzionalità e affidabilità del sistema dei controlli interni.

In ogni caso, le funzioni aziendali di controllo informano tempestivamente gli organi aziendali su ogni violazione o carenza rilevante riscontrate (ad 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, in via generale, le responsabilità e i principali compiti di ciascuna delle funzioni aziendali di controllo.

Indicazioni più specifiche concernenti le responsabilità e 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 (ad 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

Parte I – Recepimento in Italia della CRD IV

Titolo IV - Governo societario, controlli interni, gestione dei rischi

Capitolo 3 – Il sistema dei controlli interni

Sezione III – Funzioni aziendali di controllo

primo luogo dove il rischio viene generato: è pertanto necessaria un'adeguata responsabilizzazione di tutto il personale.

La funzione di conformità alle norme presiede, secondo un approccio *risk based*, alla gestione del rischio di non conformità con riguardo a tutta l'attività aziendale, verificando che le procedure interne siano adeguate a prevenire tale rischio. A tal fine, è necessario che la funzione di conformità alle norme abbia accesso a tutte le attività della banca, centrali e periferiche, e a qualsiasi informazione a tal fine rilevante, anche attraverso il colloquio diretto con il personale.

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; la verifica della loro adeguatezza e corretta applicazione;
- 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 (ad 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.

Per le norme più rilevanti ai fini del rischio di non conformità, quali 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, e per quelle norme per le quali non siano già previste forme di presidio specializzato all'interno della banca, la funzione è direttamente responsabile della gestione del rischio di non conformità.

Con riferimento ad altre normative per le quali siano già previste forme specifiche di presidio specializzato (ad es.: normativa sulla sicurezza sul lavoro, in materia di trattamento dei dati personali), la banca, in base a una valutazione dell'adeguatezza dei controlli specialistici a gestire i profili di rischio di non conformità, può graduare i compiti della *compliance*, che comunque è responsabile, in collaborazione con le funzioni specialistiche incaricate, almeno della definizione delle metodologie di valutazione del rischio di non conformità e della individuazione delle relative procedure, e procede alla verifica dell'adeguatezza delle procedure medesime a prevenire il rischio di non conformità.

La banca può adottare tale approccio anche con riferimento al presidio del rischio di non conformità alle normative di natura fiscale (3), che richiede almeno: (i) la definizione di procedure (4) volte a prevenire violazioni o elusioni di tale normativa e ad attenuare i rischi connessi a

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

(4) Tali procedure possono prevedere il ricorso a figure interne alla banca esperte in materia fiscale oppure, nei casi più complessi, l'acquisizione del parere delle autorità tributarie competenti.

Parte I – Recepimento in Italia della CRD IV

Titolo IV - Governo societario, controlli interni, gestione dei rischi

Capitolo 3 – Il sistema dei controlli interni

Sezione III – Funzioni aziendali di controllo

situazioni che potrebbero integrare fattispecie di abuso del diritto, in modo da minimizzare le conseguenze sia sanzionatorie, sia reputazionali derivanti dalla non corretta applicazione della normativa fiscale; (ii) la verifica dell'adeguatezza di tali procedure e della loro idoneità a realizzare effettivamente l'obiettivo di prevenire il rischio di non conformità.

Ferme restando le responsabilità della funzione di *compliance* per l'espletamento dei compiti previsti da normative specifiche (quali, ad es., le discipline in materia di politiche e prassi di remunerazione e incentivazione, di trasparenza delle operazioni e correttezza delle relazioni tra intermediari e clienti e di attività di rischio e conflitti di interesse nei confronti di soggetti collegati), altre aree di intervento sono:

- il coinvolgimento nella valutazione *ex ante* della conformità alla regolamentazione applicabile di tutti i progetti innovativi (inclusa l'operatività in nuovi prodotti o servizi nell'ambito del relativo processo di approvazione, secondo quanto previsto nella Sezione II, paragrafo 3) 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;
- 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.

Sotto il profilo organizzativo, tenuto conto dei 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 risorse appartenenti ad altre strutture organizzative (ad 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.

3.3 Funzione di controllo dei rischi (*risk management function*)

La funzione di controllo dei rischi ha la finalità di collaborare alla definizione e all'attuazione del RAF e delle relative politiche di governo dei rischi, attraverso un adeguato processo di gestione dei rischi (5).

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.

(5) La funzione di controllo dei rischi 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.

Parte I – Recepimento in Italia della CRD IV

Titolo IV - Governo societario, controlli interni, gestione dei rischi

Capitolo 3 – Il sistema dei controlli interni

Sezione III – Funzioni aziendali di controllo

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 RAF, delle politiche di governo dei rischi e delle varie fasi che costituiscono il processo di gestione dei rischi nonché nella fissazione dei limiti operativi all'assunzione delle varie tipologie di rischio. In tale ambito, ha, tra l'altro, il compito di proporre i parametri quantitativi e qualitativi necessari per la definizione del RAF, che utilizzano come input i risultati degli scenari di stress e delle analisi di *sensitivity*, in caso di modifiche del contesto operativo interno ed esterno della banca, l'adeguamento di tali parametri;
- verifica l'adeguatezza del RAF;
- verifica nel continuo l'adeguatezza del processo di gestione dei rischi e dei limiti operativi;
- 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;
- valuta, almeno annualmente, robustezza ed efficacia del programma delle prove di stress e la necessità di aggiornamento dello stesso. La valutazione deve includere sia aspetti qualitativi che quantitativi, secondo quanto riportato negli Orientamenti relativi alle prove di stress degli enti (EBA/GL/2018/04), e devono essere considerate le possibili interconnessioni tra prove di stress sulla solvibilità e quelle sulla liquidità;
- definisce metriche comuni di valutazione dei rischi operativi coerenti con il RAF, coordinandosi con la funzione di conformità alle norme, con la funzione ICT e con la funzione di continuità operativa;
- definisce modalità di valutazione e controllo dei rischi reputazionali, coordinandosi con la funzione di conformità alle norme e le funzioni aziendali maggiormente esposte;
- coadiuva gli organi aziendali nella valutazione del rischio strategico monitorando le variabili significative;
- assicura la coerenza dei sistemi di misurazione e controllo dei rischi con i processi e le metodologie di valutazione delle attività aziendali, coordinandosi con le strutture aziendali interessate;

Parte I – Recepimento in Italia della CRD IV

Titolo IV - Governo societario, controlli interni, gestione dei rischi

Capitolo 3 – Il sistema dei controlli interni

Sezione III – Funzioni aziendali di controllo

- sviluppa e applica indicatori in grado di evidenziare situazioni di anomalia e di inefficienza dei sistemi di misurazione e controllo dei rischi;
- analizza i rischi dei nuovi prodotti e servizi e quelli derivanti dall'ingresso in nuovi segmenti operativi e di mercato ipotizzando diversi scenari di rischio e valutando la capacità della banca di assicurare una efficace gestione del rischio. Può chiedere che modifiche da apportare a specifici prodotti o servizi siano preventivamente sottoposte al vaglio degli organi aziendali nel rispetto del processo di approvazione dei nuovi prodotti di cui alla Sezione II, paragrafi 2 e 3;
- dà pareri preventivi sulla coerenza con il RAF delle operazioni di maggiore rilievo eventualmente acquisendo, in funzione della natura dell'operazione, il parere di altre funzioni coinvolte nel processo di gestione dei rischi; in caso di parere negativo su operazioni diverse da quelle deliberate direttamente dall'organo con funzione di supervisione strategica o di gestione (*veto power*), sono adottate procedure specifiche e formalizzate per l'approvazione di tali operazioni da parte dell'organo con funzione di supervisione strategica o di gestione (cd. procedure di *escalation*) (6);
- monitora costantemente il rischio effettivo assunto dalla banca e la sua coerenza con gli obiettivi di rischio nonché il rispetto dei limiti operativi assegnati alle strutture operative in relazione all'assunzione delle varie tipologie di rischio, verificando che le decisioni sull'assunzioni dei rischi assunte ai diversi livelli aziendali siano coerenti con i pareri da essa forniti;
- in caso di violazione del RAF, inclusi i limiti operativi, ne valuta le cause e gli effetti sulla situazione aziendale, anche in termini di costi, ne informa le unità operative interessate e gli organi aziendali e propone misure correttive. Assicura che l'organo con funzione di supervisione strategica sia informato in caso di violazioni gravi; la funzione di controllo dei rischi ha un ruolo attivo nell'assicurare che le misure raccomandate siano adottate dalle funzioni interessate e portate a conoscenza degli organi aziendali;
- verifica il corretto svolgimento del monitoraggio andamentale sulle singole esposizioni creditizie (cfr. Allegato A, par. 2);
- 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, l'adeguatezza, la funzionalità e l'affidabilità della struttura organizzativa e delle altre componenti del sistema dei controlli interni, portando all'attenzione degli organi aziendali i possibili miglioramenti, con particolare riferimento al RAF, 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:

(6) Il parere del responsabile della funzione di controllo dei rischi ha invece una funzione consultiva per le operazioni deliberate direttamente dall'organo con funzione di supervisione strategica o di gestione.

DISPOSIZIONI DI VIGILANZA PER LE BANCHE

Parte I – Recepimento in Italia della CRD IV

Titolo IV - Governo societario, controlli interni, gestione dei rischi

Capitolo 3 – Il sistema dei controlli interni

Sezione III – Funzioni aziendali di controllo

- valuta la completezza, l'adeguatezza, la funzionalità, l'affidabilità delle altre componenti del sistema dei controlli interni, del processo di gestione dei rischi e degli altri processi aziendali, avendo riguardo anche alla capacità di individuare errori ed irregolarità. In tale contesto, sottopone, tra l'altro, a verifica le funzioni aziendali di controllo dei rischi e di conformità alle norme;
- valuta l'efficacia del processo di definizione del RAF, la coerenza interna dello schema complessivo e la conformità dell'operatività aziendale al RAF e, in caso di strutture finanziarie particolarmente complesse, la conformità di queste alle strategie approvate dagli organi aziendali;
- 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 è coerente con l'attività svolta e la propensione al rischio; tuttavia sono condotti anche accertamenti ispettivi casuali e non preannunciati;
 - b. il monitoraggio della conformità alle norme dell'attività 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 il RAF 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");
 - h. nelle banche che adottano sistemi interni di misurazione dei rischi, l'integrità dei processi che garantiscono l'affidabilità dei metodi e delle tecniche, delle ipotesi e delle fonti di informazioni utilizzati dalla banca nei modelli interni (ad es., la modellazione dei rischi e le misurazioni contabili); dovrebbero essere anche valutati la qualità e l'uso di strumenti qualitativi di identificazione e valutazione dei rischi e le misure di attenuazione del rischio adottate;
- effettua test periodici sul funzionamento delle procedure operative e di controllo interno;
- espleta compiti d'accertamento anche con riguardo a specifiche irregolarità;
- 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 controlla altresì i piani di continuità operativa dei fornitori di servizi 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;

Parte I – Recepimento in Italia della CRD IV

Titolo IV - Governo societario, controlli interni, gestione dei rischi

Capitolo 3 – Il sistema dei controlli interni

Sezione III – Funzioni aziendali di controllo

- qualora nell’ambito della collaborazione e dello scambio di informazioni con il soggetto incaricato della revisione legale dei conti, viene a conoscenza di criticità emerse durante l’attività di revisione legale dei conti, 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 anche:

- 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’appropriatezza delle ipotesi utilizzate nelle analisi di sensitività e di scenario e negli stress test;
- l’allineamento con le *best practice* diffuse nel settore.

Nello svolgimento dei propri compiti la funzione di revisione interna tiene conto di quanto previsto dagli standard professionali diffusamente accettati.

L’organizzazione della funzione di revisione interna è coerente con l’articolazione ed il grado di complessità della banca. Fermo restando che la funzione va posta alle dirette dipendenze dell’organo con funzione di supervisione strategica, vanno, tuttavia, preservati i raccordi con l’organo con funzione di gestione.

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 è espressamente 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 conclusi con giudizi negativi o che evidenzino carenze di rilievo sono trasmessi integralmente, tempestivamente e direttamente agli organi aziendali.

Per svolgere adeguatamente i propri compiti, la funzione di revisione interna ha 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 es., 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 (ad es., funzione legale, organizzazione, sicurezza) 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.

DISPOSIZIONI DI VIGILANZA PER LE BANCHE

Parte I – Recepimento in Italia della CRD IV

Titolo IV - Governo societario, controlli interni, gestione dei rischi

Capitolo 3 – Il sistema dei controlli interni

Sezione III – Funzioni aziendali di controllo

Specificata attenzione è posta nell'articolazione dei flussi informativi tra le funzioni aziendali di controllo; in particolare, i responsabili della funzione di controllo dei rischi e della funzione di conformità alle norme informano il responsabile della funzione di revisione interna delle criticità rilevate nelle proprie attività di controllo che possano essere di interesse per l'attività di *audit*. 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.

Parte I – Recepimento in Italia della CRD IV

Titolo IV - Governo societario, controlli interni, gestione dei rischi

Capitolo 3 – Il sistema dei controlli interni

Sezione IV – Esternalizzazione di funzioni aziendali (*outsourcing*)

SEZIONE IV

ESTERNALIZZAZIONE DI FUNZIONI AZIENDALI (OUTSOURCING)

1. Principi generali e requisiti particolari

Le banche che ricorrono all'esternalizzazione di funzioni aziendali all'interno o all'esterno del gruppo applicano i Titoli I, II, III e IV degli *Orientamenti in materia di outsourcing* dell'EBA (1).

Ai fini dell'applicazione di questi Orientamenti, si precisa che:

- (i) per “funzioni di controllo interno” si intendono le “funzioni aziendali di controllo”, per “funzione di *audit* interno” si intende la “funzione di revisione interna”;
- (ii) si considerano di norma funzioni essenziali o importanti le funzioni necessarie per lo svolgimento delle “linee di operatività principale” e delle “funzioni essenziali” ai sensi dell'art. 1, comma 1, lettere *hh*) e *bb*), del d.lgs. 180/2015.

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

- delegare le proprie responsabilità, né la responsabilità degli organi aziendali;
- 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.

L'esternalizzazione di compiti operativi delle funzioni aziendali di controllo, all'interno o all'esterno del gruppo, è ammessa nel rispetto del principio di proporzionalità. Resta ferma la responsabilità degli organi aziendali e del responsabile della funzione esternalizzata per il corretto svolgimento dei compiti esternalizzati.

2. Comunicazioni alla Banca centrale europea o alla Banca d'Italia

Dopo l'approvazione da parte degli organi competenti e prima di dare corso all'esternalizzazione di funzioni essenziali o importanti, le banche comunicano alla Banca centrale europea o alla Banca d'Italia le informazioni di cui al paragrafo 54 degli Orientamenti dell'EBA in materia di esternalizzazione. È facoltà per le banche avviare un confronto preliminare con l'autorità di vigilanza sui progetti di esternalizzazione più rilevanti e/o innovativi, prima di conferire l'incarico. Restano in ogni caso fermi tutti i poteri, anche di intervento e sanzionatori, spettanti all'autorità di vigilanza.

(1) https://eba.europa.eu/documents/10180/2761380/EBA+revised+Guidelines+on+outsourcing_IT.pdf/1c9aaefc-e10d-45a6-8a51-1fb450814a29.

Parte I – Recepimento in Italia della CRD IV

Titolo IV - Governo societario, controlli interni, gestione dei rischi

Capitolo 3 – Il sistema dei controlli interni

Sezione IV – Esternalizzazione di funzioni aziendali (*outsourcing*)

Le banche informano la Banca centrale europea o la Banca d'Italia se una funzione esternalizzata è stata successivamente qualificata come funzione operativa essenziale o importante. L'informativa attesta il rispetto delle condizioni previste per l'esternalizzazione di funzioni essenziali o importanti.

Le banche informano tempestivamente la Banca centrale europea o la Banca d'Italia di modifiche rilevanti e/o eventi gravi riguardanti i propri accordi di esternalizzazione che potrebbero avere un impatto significativo sulla continuità delle proprie attività operative.

Entro il 30 aprile di ogni anno le banche trasmettono alla Banca centrale europea o 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 essenziali o importanti esternalizzate a fornitori di servizi al di fuori del gruppo, alle carenze eventualmente riscontrate e alle conseguenti azioni correttive adottate.

3. Esternalizzazione del trattamento del contante

Fatta salva l'applicazione delle disposizioni in materia di esternalizzazione di funzioni essenziali o importanti della presente Sezione e al fine di minimizzare i rischi operativi, in particolare di natura legale e reputazionale 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 il fornitore di servizi 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;
- la possibilità per le banche di verificare la performance del servizio reso e di richiedere eventuali misure correttive;

DISPOSIZIONI DI VIGILANZA PER LE BANCHE

Parte I – Recepimento in Italia della CRD IV

Titolo IV - Governo societario, controlli interni, gestione dei rischi

Capitolo 3 – Il sistema dei controlli interni

Sezione IV – Esternalizzazione di funzioni aziendali (*outsourcing*)

- il diritto per la banca di recedere, senza penalità, nel caso in cui la controparte violi gli obblighi contrattuali e non vi ponga rimedio entro il periodo di tempo indicato nel contratto stesso.

Parte I – Recepimento in Italia della CRD IV

Titolo IV - Governo societario, controlli interni, gestione dei rischi

Capitolo 3 – Il sistema dei controlli interni

Sezione V – Il RAF e il sistema dei controlli interni nei gruppi bancari

SEZIONE V

IL RAF E IL SISTEMA DEI CONTROLLI INTERNI NEI GRUPPI BANCARI

1. Il RAF nei gruppi bancari

La capogruppo definisce e approva il RAF di gruppo secondo le indicazioni contenute nell'Allegato C, in quanto compatibili, assicurando la coerenza tra l'operatività, la complessità e le dimensioni del gruppo e il RAF stesso.

Il RAF di gruppo tiene conto delle specifiche operatività e dei connessi profili di rischio di ciascuna delle società componenti il gruppo in modo da risultare integrato e coerente. Per il conseguimento di tale obiettivo è necessario che gli organi aziendali della capogruppo svolgano i compiti loro affidati con riferimento non soltanto alla propria realtà aziendale ma anche valutando l'operatività complessiva del gruppo e i rischi cui esso è esposto.

Gli organi aziendali delle società componenti il gruppo, secondo le rispettive competenze, agiscono in coerenza con il RAF di gruppo e sono responsabili della sua attuazione per quanto concerne gli aspetti relativi alla propria realtà aziendale. A tal fine, è necessario che la capogruppo renda partecipi, nei modi ritenuti più opportuni, gli organi aziendali delle controllate delle scelte effettuate in materia di RAF.

2. Controlli interni di gruppo

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

- 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) (1);
- b. un *controllo gestionale* volto ad assicurare il mantenimento delle condizioni di equilibrio economico, finanziario, patrimoniale e di liquidità 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.

La capogruppo che esercita l'attività di direzione e coordinamento in violazione dei principi di corretta gestione societaria e imprenditoriale è responsabile ai sensi degli artt. 2497 e ss. del codice civile.

(1) Con riferimento alla struttura del gruppo, il controllo strategico mira ad assicurare che il numero, il grado di interconnessione e la complessità del gruppo non interferiscano con il corretto funzionamento degli assetti di governo e controllo del gruppo nel suo complesso e delle sue componenti.

Parte I – Recepimento in Italia della CRD IV

Titolo IV - Governo societario, controlli interni, gestione dei rischi

Capitolo 3 – Il sistema dei controlli interni

Sezione V – Il RAF e il sistema dei controlli interni nei gruppi bancari

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 nelle precedenti Sezioni. A livello di gruppo - tenendo conto delle disposizioni in materia di organizzazione e controllo dei soggetti diversi dalle banche - vanno anche stabiliti e definiti:

- procedure formalizzate di coordinamento e collegamento fra le società appartenenti al gruppo e la capogruppo per tutte le aree di attività;
- compiti e responsabilità degli organi e delle funzioni di controllo all'interno del gruppo, le procedure di coordinamento, i rapporti organizzativi, i flussi informativi e i relativi raccordi; a tali fini, l'organo con funzione di supervisione strategica della capogruppo approva un apposito documento di coordinamento dei controlli nell'ambito del gruppo. 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 (2);
- 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 vigila anche sul 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 presidono 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

(2) I flussi informativi includono in particolare informazioni periodiche sull'andamento dei principali fattori di rischio, report periodici sul rispetto da parte delle componenti del gruppo degli indirizzi strategici e della conformità al quadro vigente.

Parte I – Recepimento in Italia della CRD IV

Titolo IV - Governo societario, controlli interni, gestione dei rischi

Capitolo 3 – Il sistema dei controlli interni

Sezione V – Il RAF e il sistema dei controlli interni nei gruppi bancari

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. La capogruppo decide, infine, in merito all'adozione dei sistemi interni di misurazione dei rischi per la determinazione dei requisiti patrimoniali e ne determina le caratteristiche essenziali, assumendosi la responsabilità della realizzazione del progetto nonché della supervisione sul corretto funzionamento di tali sistemi e sul loro costante adeguamento sotto il profilo metodologico, organizzativo e procedurale.

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.

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.

3. Comunicazioni alla Banca centrale europea o alla Banca d'Italia

La capogruppo, sulla base delle relazioni delle funzioni aziendali di controllo (cfr. Sezione III, par. 2 e par. 2), invia annualmente alla Banca centrale europea o alla Banca d'Italia una relazione riguardante gli accertamenti effettuati sulle società controllate e i risultati emersi, i punti di debolezza rilevati con riferimento sia al gruppo bancario nel suo complesso sia alle singole entità e la descrizione degli interventi da adottare per la rimozione delle carenze rilevate.

Parte I – Recepimento in Italia della CRD IV

Titolo IV - Governo societario, controlli interni, gestione dei rischi

Capitolo 3 – Il sistema dei controlli interni

Sezione VI – Imprese di riferimento

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 (1); 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.

(1) Cfr. Disposizioni introduttive, Ambito di applicazione, Sezione III, par. 1 della presente Circolare.

DISPOSIZIONI DI VIGILANZA PER LE BANCHE

Parte I – Recepimento in Italia della CRD IV

Titolo IV - Governo societario, controlli interni, gestione dei rischi

Capitolo 3 – Il sistema dei controlli interni

Sezione VII – Succursali di banche comunitarie e di banche extracomunitarie aventi sede negli stati indicati nell'Allegato A delle Disposizioni introduttive

SEZIONE VII

SUCCURSALI DI BANCHE COMUNITARIE E DI BANCHE EXTRACOMUNITARIE AVENTI SEDE NEGLI STATI INDICATI NELL'ALLEGATO A DELLE DISPOSIZIONI INTRODUTTIVE

Nel caso delle succursali di banche comunitarie e delle succursali di banche extracomunitarie aventi sede negli Stati indicati nell'Allegato A delle Disposizioni introduttive, 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 (1).

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.

Nel caso delle succursali di banche extracomunitarie aventi sede negli Stati indicati nell'Allegato A delle Disposizioni introduttive, il legale rappresentante attesta altresì che la completezza, l'adeguatezza, la funzionalità, l'affidabilità del sistema dei controlli interni è stata verificata attraverso un processo di revisione interna.

(1) L'attestato contiene almeno la descrizione sintetica: i) dell'attività svolta dalla succursale; ii) delle soluzioni organizzative adottate.

Parte I – Recepimento in Italia della CRD IV

Titolo IV - Governo societario, controlli interni, gestione dei rischi

Capitolo 3 – Il sistema dei controlli interni

Sezione VIII – Sistemi interni di segnalazione delle violazioni

SEZIONE VIII

SISTEMI INTERNI DI SEGNALAZIONE DELLE VIOLAZIONI

In linea con il principio di proporzionalità, le banche definiscono i sistemi interni volti a permettere la segnalazione da parte del personale (1) di atti o fatti che possano costituire una violazione delle norme disciplinanti l'attività bancaria (2).

I sistemi interni di segnalazione garantiscono in ogni caso la riservatezza e la protezione dei dati personali del soggetto che effettua la segnalazione e del soggetto eventualmente segnalato (3). Per effettuare la segnalazione non è necessario che il segnalante disponga di prove della violazione; tuttavia, deve disporre di informazioni sufficientemente circostanziate che ne facciano ritenere ragionevole l'invio.

I suddetti sistemi sono strutturati in modo da garantire che le segnalazioni vengano ricevute, esaminate e valutate attraverso canali specifici, autonomi e indipendenti che differiscono dalle ordinarie linee di *reporting*. A tal fine, i sistemi interni di segnalazione prevedono canali alternativi a disposizione del segnalante in modo da assicurare che il soggetto preposto alla ricezione, all'esame e alla valutazione della segnalazione (v. *infra* lett. c) non sia gerarchicamente o funzionalmente subordinato all'eventuale soggetto segnalato, non sia esso stesso il presunto responsabile della violazione e non abbia un potenziale interesse correlato alla segnalazione tale da comprometterne l'imparzialità e l'indipendenza di giudizio.

I soggetti preposti alla ricezione, all'esame e alla valutazione delle segnalazioni non partecipano all'adozione degli eventuali provvedimenti decisionali, che sono rimessi alle funzioni o agli organi aziendali competenti.

Le banche nominano un responsabile dei sistemi interni di segnalazione il quale assicura il corretto svolgimento del procedimento e riferisce direttamente e senza indugio agli organi aziendali le informazioni oggetto di segnalazione, ove rilevanti (4). Il responsabile dei sistemi interni di segnalazione tiene un apposito registro delle segnalazioni.

I soggetti che ricevono, esaminano e valutano le segnalazioni, il responsabile dei sistemi interni di segnalazione e ogni altro soggetto coinvolto nella procedura hanno l'obbligo di garantire la confidenzialità delle informazioni ricevute, anche in merito all'identità del segnalante che, in ogni caso, deve essere opportunamente tutelato da condotte ritorsive, discriminatorie o comunque sleali conseguenti alla segnalazione. Il presunto responsabile della violazione è tutelato da ripercussioni negative derivanti dalla segnalazione nel caso in cui dal procedimento di segnalazione non emergano elementi che giustificano l'adozione di provvedimenti nei suoi confronti (5).

(1) Ai sensi dell'art. 1, comma 2, lett. h-*novies*), TUB, per "personale" si intende: "i dipendenti e coloro che comunque operano sulla base di rapporti che ne determinano l'inserimento nell'organizzazione aziendale, anche in forma diversa dal rapporto di lavoro subordinato".

(2) Ai fini delle presenti disposizioni per "attività bancaria" si intende quella disciplinata dall'art. 10, commi 1, 2 e 3, TUB.

(3) Gli obblighi di riservatezza non possono essere opposti quando le informazioni richieste sono necessarie per le indagini o i procedimenti avviati dall'autorità giudiziaria in seguito alla segnalazione.

(4) Il responsabile dei sistemi interni di segnalazione, in linea con il principio di proporzionalità, può direttamente gestire le fasi di ricezione, esame e valutazione del procedimento di segnalazione.

(5) In caso di adozione di provvedimenti nei confronti del responsabile della violazione, costui dovrà essere tutelato da eventuali effetti negativi diversi da quelli previsti dai provvedimenti adottati.

Parte I – Recepimento in Italia della CRD IV

Titolo IV - Governo societario, controlli interni, gestione dei rischi

Capitolo 3 – Il sistema dei controlli interni

Sezione VIII – Sistemi interni di segnalazione delle violazioni

Le procedure relative ai sistemi interni di segnalazione devono essere formalizzate e accessibili a tutto il personale; esse prevedono:

- a. i soggetti che, in conformità a quanto disposto dall'art. 1, comma 2, lett. h-*novies*, TUB (6), li possono attivare (7);
- b. fermo restando quanto previsto dall'art. 52-*bis*, comma 1, TUB (8), gli atti o i fatti che possono essere oggetto di segnalazione;
- c. le modalità attraverso cui segnalare le presunte violazioni e i soggetti preposti alla ricezione delle segnalazioni;
- d. il procedimento che si instaura nel momento in cui viene effettuata una segnalazione con l'indicazione, ad esempio, dei tempi e delle fasi di svolgimento del procedimento, dei soggetti coinvolti nello stesso, delle ipotesi in cui il responsabile dei sistemi interni di segnalazione è tenuto a fornire immediata comunicazione agli organi aziendali; quando richiesto dal segnalante, le informazioni oggetto di segnalazione sono portate a conoscenza degli organi aziendali assicurando l'anonimato del segnalante;
- e. le modalità attraverso cui è fornita conferma, ove possibile, al segnalante del ricevimento della segnalazione;
- f. le modalità attraverso cui il soggetto segnalante e il soggetto segnalato devono essere informati sugli sviluppi del procedimento;
- g. l'obbligo per il soggetto segnalante di dichiarare se ha un interesse privato collegato alla segnalazione;
- h. nel caso in cui il segnalante sia corresponsabile delle violazioni, un trattamento privilegiato per quest'ultimo rispetto agli altri corresponsabili, compatibilmente con la disciplina applicabile.

Al fine di incentivare l'uso dei sistemi interni di segnalazione e di favorire la diffusione di una cultura della legalità, le banche illustrano al proprio personale in maniera chiara, precisa e completa il procedimento di segnalazione interno adottato indicando i presidi posti a garanzia della riservatezza dei dati personali del segnalante e del presunto responsabile della violazione, con l'espreso avvertimento che le disposizioni europee e nazionali in materia di protezione dei dati personali che regolano l'accesso ai dati personali non trovano applicazione con riguardo all'identità del segnalante, che può essere rivelata solo con il suo consenso o quando la conoscenza sia indispensabile per la difesa del segnalato.

Nel rispetto di quanto previsto dalla disciplina sulla protezione dei dati personali, il responsabile dei sistemi interni di segnalazione redige una relazione annuale sul corretto funzionamento dei sistemi interni di segnalazione, contenente le informazioni aggregate sulle risultanze dell'attività svolta a seguito delle segnalazioni ricevute, che viene approvata dagli organi aziendali e messa a disposizione al personale della banca.

Le banche, fermo restando il rispetto delle disposizioni di cui alla presente Sezione e alla Sezione IV, possono esternalizzare l'attività di ricezione, esame e valutazione delle segnalazioni.

(6) V. *supra*, nota 1.

(7) Le procedure possono prevedere che le informazioni sull'identità del segnalante siano trattate in forma anonima.

(8) Ai sensi dell'art. 52-*bis*, comma 1, TUB “le banche e le relative capogruppo adottano procedure specifiche per la segnalazione al proprio interno da parte del personale, di atti o fatti che possono costituire una violazione delle norme disciplinanti l'attività bancaria”.

Parte I – Recepimento in Italia della CRD IV

Titolo IV - Governo societario, controlli interni, gestione dei rischi

Capitolo 3 – Il sistema dei controlli interni

Sezione IX – Informativa alla Banca centrale europea o alla Banca d'Italia

SEZIONE IX

INFORMATIVA ALLA BANCA CENTRALE EUROPEA O ALLA BANCA D'ITALIA

Le banche comunicano tempestivamente alla Banca centrale europea o 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 centrale europea o 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 essenziali o importanti esternalizzate a fornitori di servizi al di fuori del gruppo, alle carenze eventualmente riscontrate e alle conseguenti azioni correttive adottate (cfr. Sezione IV, par. 2);
- qualora ve ne siano le condizioni, la relazione di cui al punto 2.1 dell'Allegato A.

Dopo l'approvazione da parte degli organi competenti e prima di dare corso all'esternalizzazione di funzioni essenziali o importanti, le banche non appartenenti a gruppi comunicano alla Banca centrale europea o alla Banca d'Italia le informazioni di cui al paragrafo 54 degli Orientamenti dell'EBA in materia di esternalizzazione (cfr. Sezione IV, par. 2).

Nel caso di gruppi bancari, le capogruppo coordinano e trasmettono alla Banca centrale europea o alla Banca d'Italia, per tutte le banche del gruppo, la stessa documentazione richiesta nel caso delle banche non appartenenti a gruppi bancari, ad eccezione delle relazioni delle funzioni aziendali di controllo delle società controllate (Sezione III, par. 2). In luogo di queste ultime, inviano annualmente alla Banca centrale europea o alla Banca d'Italia la relazione di cui alla Sezione V, par. 3, riguardante gli accertamenti effettuati sulle società controllate e i risultati emersi, i punti di debolezza rilevati con riferimento sia al gruppo bancario nel suo complesso sia alle singole entità e la descrizione degli interventi da adottare per la rimozione delle carenze rilevate.

Dopo l'approvazione da parte degli organi competenti e prima di dare corso all'esternalizzazione di funzioni essenziali o importanti nell'ambito del gruppo bancario di appartenenza, le capogruppo comunicano alla Banca centrale europea o alla Banca d'Italia le informazioni di cui al paragrafo 54 degli Orientamenti dell'EBA in materia di esternalizzazione (cfr. Sezione IV, par. 2).

Nel caso delle succursali di banche comunitarie e delle succursali di banche extracomunitarie aventi sede negli Stati indicati nell'Allegato A delle Disposizioni introduttive, 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 centrale europea o alla Banca d'Italia in merito all'esito di tale verifica (cfr. Sezione VII).

DISPOSIZIONI DI VIGILANZA PER LE BANCHE

Parte I – Recepimento in Italia della CRD IV

Titolo IV - Governo societario, controlli interni, gestione dei rischi

Capitolo 3 – Il sistema dei controlli interni

Sezione IX – Informativa alla Banca centrale europea o alla Banca d'Italia

Nel caso delle succursali di banche extracomunitarie aventi sede negli Stati indicati nell'Allegato A delle Disposizioni introduttive, il legale rappresentante attesta altresì che la completezza, l'adeguatezza, la funzionalità, l'affidabilità del sistema dei controlli interni è stata verificata attraverso un processo di revisione interna (cfr. Sezione VII).

Le succursali di banche extracomunitarie non aventi sede negli Stati indicati nell'Allegato A delle Disposizioni introduttive, individuano un referente per ciascuna funzione aziendale di controllo della succursale. I nominativi dei referenti e le eventuali variazioni sono comunicati alla Banca centrale europea o alla Banca d'Italia.

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.

Inoltre, nell'ambito del rischio di credito e di controparte, le presenti disposizioni definiscono i presidi che le banche sono tenute ad adottare per assicurare una corretta valutazione nel continuo dei beni immobili posti a garanzia delle esposizioni (1). In particolare, sono previsti i requisiti di carattere organizzativo, le regole relative alla corretta valutazione degli immobili e i requisiti di professionalità e indipendenza dei soggetti che effettuano la valutazione degli immobili (c.d. periti).

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 esposizioni. A tal fine, le banche sono tenute al rispetto della disciplina dettata nella Parte Seconda, Capitolo 10, Sezione V.

(1) Per la definizione di "esposizione" si rimanda a quanto previsto dall'art. 5, n. 1), CRR.

DISPOSIZIONI DI VIGILANZA PER LE BANCHE

Parte I – Recepimento in Italia della CRD IV

Titolo IV - Governo societario, controlli interni, gestione dei rischi

Capitolo 3 – Il sistema dei controlli interni

Allegato A – Disposizioni speciali relative a particolari categorie di rischio

Nella fase istruttoria, le banche acquisiscono tutta la documentazione necessaria per effettuare un'adeguata valutazione del merito di credito del prestatore, sotto il profilo patrimoniale e reddituale, e 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 prestatore, anche alla luce del complesso delle relazioni intrattenute. Le procedure di sfruttamento delle informazioni devono fornire indicazioni circostanziate sul livello di affidabilità del cliente (ad es., attraverso sistemi di *credit scoring* e/o di *rating*).

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, ecc.). 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 dei passaggi a perdita.

I criteri di classificazione, valutazione e gestione delle esposizioni deteriorate (2), nonché le relative unità responsabili devono essere stabiliti dall'organo con funzione di supervisione strategica con apposita delibera che indichi anche le modalità di raccordo tra tali criteri e quelli previsti per le segnalazioni di vigilanza. La deroga all'applicazione dei criteri prefissati è consentita esclusivamente in casi predeterminati e seguendo procedure rafforzate, che prevedano il coinvolgimento dell'organo con funzione di gestione. Devono essere altresì stabilite procedure atte a individuare, in dettaglio, gli interventi da attuare in presenza di deterioramento delle posizioni di rischio.

In particolare, la determinazione del valore di recupero dei crediti deteriorati tiene conto dei seguenti fattori: i) tipologia di procedura esecutiva attivata ed esito delle fasi già esperite; ii) valore di pronto realizzo delle garanzie (calcolando per i beni immobili *haircut* in funzione dell'aggiornamento della perizia e del contesto di mercato; per le attività finanziarie scarti coerenti con la natura del prodotto e la situazione di mercato); iii) criteri per la stima del periodo di recupero e dei tassi di attualizzazione dei flussi attesi. Le suddette indicazioni sono periodicamente aggiornate sulla base dell'evoluzione del quadro di riferimento.

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

DISPOSIZIONI DI VIGILANZA PER LE BANCHE

Parte I – Recepimento in Italia della CRD IV

Titolo IV - Governo societario, controlli interni, gestione dei rischi

Capitolo 3 – Il sistema dei controlli interni

Allegato A – Disposizioni speciali relative a particolari categorie di rischio

La verifica del corretto svolgimento del monitoraggio andamentale sulle singole esposizioni, in particolare di quelle deteriorate, e la valutazione della coerenza delle classificazioni, della congruità degli accantonamenti e dell'adeguatezza del processo di recupero è svolta, a livello centrale e periferico, dalla funzione di controllo dei rischi o, per le banche di maggiore dimensione e complessità operativa, da una specifica unità, che riporta al responsabile della funzione di controllo dei rischi.

Tali unità verificano, tra l'altro, l'operato delle unità operative e di recupero crediti, assicurando la corretta classificazione delle esposizioni deteriorate e l'adeguatezza del relativo grado di irrecuperabilità (3). Nel caso di valutazioni discordanti, si applicano le valutazioni formulate dalla funzione di controllo dei rischi.

L'*internal audit* assicura periodiche verifiche sull'affidabilità ed efficacia del complessivo processo.

Gli organi aziendali, nell'ambito delle rispettive competenze, sono costantemente aggiornati dei risultati conseguiti nell'applicazione dei criteri e delle procedure individuate e valutano l'esigenza di definire interventi di miglioramento di tali criteri e procedure.

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 (4).

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 abbiano fondamento giuridico. Nel caso in cui i predetti accordi intendano riconoscere anche a fini prudenziali l'effetto di riduzione del rischio devono attenersi al rispetto dei criteri previsti dalla normativa (cfr. Parte tre, Titolo II, Capo 4, e Parte tre, Titolo II, Capo 6, Sezione 7 del CRR).

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);

(3) I controlli dovranno riguardare tra l'altro: la presenza di aggiornati valori peritali delle garanzie; la registrazione nelle procedure automatiche di tutte le informazioni necessarie per la valutazione dei crediti; la tracciabilità del processo di recupero; le stime dei tempi di recupero e i tassi di attualizzazione utilizzati.

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

Parte I – Recepimento in Italia della CRD IV

Titolo IV - Governo societario, controlli interni, gestione dei rischi

Capitolo 3 – Il sistema dei controlli interni

Allegato A – Disposizioni speciali relative a particolari categorie di rischio

- il costante monitoraggio degli impegni assunti con riferimento sia al volume sia al grado di rischio 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 si astengono dal sottoscrivere i contratti relativi alle garanzie rilasciate prima della definizione di 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 valutazioni del merito di credito rilasciate dalle ECAI sono utilizzate ai fini dell'applicazione di coefficienti di ponderazione diversificati per la determinazione dei requisiti patrimoniali a fronte del rischio di credito nel metodo standardizzato conformemente a quanto previsto dal CRR (Cfr. Parte tre, Titolo II, Capo 2).

Tenuto conto dell'obbligo di non fare eccessivo affidamento sui rating del credito (5), l'utilizzo dei rating esterni non esaurisce il processo di valutazione del merito di credito che le banche devono svolgere nei confronti della clientela; 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 dei prenditori, titoli, posizioni verso le cartolarizzazioni nonché del rischio di credito a livello di portafoglio (6).

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

Le banche, oltre ad analizzare la qualità dei singoli prenditori nell'ambito del processo di gestione del rischio, sono tenute a 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 con funzione di supervisione strategica e dell'organo con funzione di controllo. Ove dall'esame emergano frequenti e significativi disallineamenti fra valutazioni interne ed esterne, copia della citata relazione è trasmessa alla Banca centrale europea o alla Banca d'Italia.

(5) Cfr. Regolamento (CE) n. 1060/2009 del 16 settembre 2009 del Parlamento europeo e del Consiglio relativo alle agenzie di rating del credito, come modificato dal Regolamento (UE) n. 462/2013 del 21 maggio 2013 (in particolare, art. 5-bis).

(6) Le banche, in linea con il principio di proporzionalità, possono non sviluppare apposite metodologie per la valutazione interna del rischio di credito derivante dalle esposizioni verso amministrazioni centrali e banche centrali.

Parte I – Recepimento in Italia della CRD IV

Titolo IV - Governo societario, controlli interni, gestione dei rischi

Capitolo 3 – Il sistema dei controlli interni

Allegato A – Disposizioni speciali relative a particolari categorie di rischio

2.2. Valutazione degli immobili posti a garanzia delle esposizioni.

L'organo con funzione di supervisione strategica, su proposta dell'organo con funzione di gestione, approva le politiche e i processi di valutazione degli immobili posti a garanzia delle esposizioni verificandone l'adeguatezza, la funzionalità e la coerenza con il RAF e con il processo di gestione dei rischi con frequenza almeno annuale.

Tali politiche e processi definiscono almeno:

- gli standard affidabili per la valutazione degli immobili. A tal fine le banche adottano standard per la valutazione degli immobili elaborati e riconosciuti a livello internazionale (7) o standard elaborati a livello nazionale purché i principi, i criteri e le metodologie di valutazione in essi contenuti siano coerenti con i suddetti standard internazionali;
- fermo restando quanto previsto dai paragrafi 2.2.1. e 2.2.2., i requisiti di professionalità e di indipendenza dal processo di commercializzazione del credito o da aspetti nevralgici del processo di erogazione del credito (8) della banca o del gruppo bancario dei periti; l'eventuale possibilità di ricorrere a periti esterni per la valutazione degli immobili e i criteri per la loro selezione;
- gli indicatori per monitorare nel continuo le variazioni delle condizioni del mercato immobiliare che possono incidere in maniera significativa sul valore degli immobili. A tal fine le banche tengono anche conto della banca dati dell'Osservatorio del mercato immobiliare dell'Agenzia delle entrate.

2.2.1. Requisiti di professionalità e indipendenza dei periti

I periti che effettuano la valutazione degli immobili possono essere dipendenti della banca o periti esterni, persone fisiche o soggetti costituiti in forma societaria o associativa.

I periti persone fisiche (9) devono avere una comprovata esperienza nella valutazione degli immobili di almeno 3 anni precedenti all'attribuzione dell'incarico, attestata mediante apposita documentazione trasmessa alla banca. Inoltre, i periti persone fisiche e gli esponenti dei soggetti costituiti in forma societaria o associativa non devono essere coinvolti – neanche indirettamente – in alcuna attività relativa al processo di commercializzazione del credito o ad aspetti nevralgici del processo di erogazione del credito della banca o del gruppo bancario.

Tenendo conto della documentazione prodotta, la banca verifica che il perito persona fisica sia in possesso delle competenze professionali idonee allo svolgimento dell'attività di valutazione. Nell'ambito di tale verifica la banca valuta le competenze anche in relazione alla complessità dell'incarico in concreto affidato (che può dipendere dalla numerosità e dalle caratteristiche dei beni oggetto di valutazione quali, ad esempio, gli aspetti strutturali e tipologici, la collocazione geografica, il contesto urbanistico e la redditività dell'immobile).

(7) Ad esempio, si fa riferimento agli standard redatti dall'*International Valuation Standards Committee*, dall'*European Group of Valuers' Association* o dal *Royal Institution of Chartered Surveyors*.

(8) Cfr. sezione IV, paragrafo 1, del presente capitolo.

(9) Per periti persone fisiche si intendendo: i dipendenti della banca, i periti esterni persone fisiche e i soggetti deputati in concreto alla valutazione degli immobili nel caso in cui la banca affidi l'incarico a soggetti costituiti in forma societaria o associativa.

Parte I – Recepimento in Italia della CRD IV

Titolo IV - Governo societario, controlli interni, gestione dei rischi

Capitolo 3 – Il sistema dei controlli interni

Allegato A – Disposizioni speciali relative a particolari categorie di rischio

Al fine di verificare le competenze professionali dei soggetti incaricati di effettuare la valutazione degli immobili, la banca tiene conto di uno o più dei seguenti elementi:

- nell'ipotesi in cui i periti siano persone fisiche, dell'iscrizione in un albo professionale la cui appartenenza comporta l'idoneità a effettuare valutazioni tecniche o economiche dei beni immobili; dello svolgimento di attività professionali o di insegnamento universitario di ruolo nel campo dell'ingegneria, dell'architettura o in materie strettamente attinenti alla valutazione degli immobili; del possesso di certificazioni comprovanti le competenze necessarie per svolgere la valutazione degli immobili mediante l'applicazione degli standard internazionali o nazionali;
- nell'ipotesi in cui i periti siano soggetti costituiti in forma societaria o associativa, anche dell'adeguatezza della struttura organizzativa di tali soggetti; dell'iscrizione in un albo professionale la cui appartenenza comporta l'idoneità a effettuare valutazioni tecniche o economiche dei beni immobili.

Le banche, inoltre, verificano che i periti persone fisiche e gli esponenti dei soggetti costituiti in forma societaria o associativa incaricati di valutare gli immobili non versino in concreto in una situazione di conflitto di interessi rispetto al processo di commercializzazione del credito o ad aspetti nevralgici del processo di erogazione del credito della banca o del gruppo bancario. A tal fine, tengono anche conto dei rapporti di matrimonio o di unione civile, di parentela, di affinità e di convivenza di fatto e delle relazioni di natura professionale e patrimoniale intercorrenti tra tali soggetti e:

- i soggetti coinvolti nel processo di erogazione del credito a garanzia del quale viene posto l'immobile oggetto di valutazione;
- i soggetti destinatari del finanziamento garantito dall'immobile oggetto di valutazione.

2.2.2. Affidamento dell'attività di valutazione degli immobili posti a garanzia delle esposizioni a periti esterni

Le banche che incaricano soggetti terzi per la valutazione degli immobili mantengono la capacità di controllo e la responsabilità dell'attività di valutazione degli immobili.

Le banche definiscono il processo di selezione e controllo dei periti esterni e adottano soluzioni organizzative per governare i relativi rischi. A tal fine, le banche:

- definiscono il processo decisionale per il conferimento degli incarichi (livelli decisionali; funzioni coinvolte; valutazione dei rischi, inclusi quelli connessi con potenziali conflitti di interesse; impatto sulle funzioni aziendali; criteri per la scelta del perito esterno);
- definiscono il contenuto minimo del contratto e gli obblighi del perito;
- controllano, nel continuo, il corretto svolgimento dell'attività di valutazione degli immobili e assicurano l'utilizzo da parte dei periti esterni degli standard di valutazione adottati dalla banca;
- identificano le misure attivabili in caso di non corretto svolgimento delle attività affidate al perito esterno incaricato della valutazione degli immobili.

Ai fini del rispetto delle disposizioni di cui sopra gli accordi di affidamento dell'incarico di valutazione degli immobili a periti esterni, da stipularsi per iscritto, definiscono chiaramente:

DISPOSIZIONI DI VIGILANZA PER LE BANCHE

Parte I – Recepimento in Italia della CRD IV

Titolo IV - Governo societario, controlli interni, gestione dei rischi

Capitolo 3 – Il sistema dei controlli interni

Allegato A – Disposizioni speciali relative a particolari categorie di rischio

- a) i diritti e gli obblighi delle parti, i livelli di servizio attesi, espressi in termini oggettivi e misurabili, nonché le informazioni necessarie per la verifica del loro rispetto; le modalità e la frequenza della reportistica dovuta alla banca. L'accordo prevede espressamente l'obbligo dei periti di dare riscontro tempestivamente a qualsiasi richiesta di informazione relativa alla valutazione degli immobili da parte della banca, che resta in ogni caso responsabile del corretto espletamento dell'attività;
- b) le opportune cautele per prevenire gli eventuali conflitti di interesse; 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;
- c) le clausole risolutive espresse che consentano alla banca di porre termine all'accordo in presenza di eventi che possano incidere negativamente sul profilo di rischio della stessa e comprometterne la sana e prudente gestione;
- d) gli obblighi di informativa su qualsiasi evento che potrebbe incidere sulla capacità del perito esterno di svolgere le funzioni a esso affidate in maniera efficace e in conformità con la normativa vigente.

Il contratto inoltre attesta che il perito esterno che svolge la valutazione degli immobili:

- a) possieda i requisiti di professionalità e di indipendenza dal processo di commercializzazione del credito o da aspetti nevralgici del processo di erogazione del credito della banca o del gruppo bancario indicati nel paragrafo 2.2.1;
- b) garantisca la sicurezza delle informazioni relative all'attività dell'intermediario, sotto l'aspetto della disponibilità, integrità e riservatezza; in particolare assicuri il rispetto delle norme sulla protezione dei dati personali.

Il perito esterno, che per lo svolgimento dell'attività di valutazione degli immobili si avvale di propri collaboratori o di proprio personale (10), rimane responsabile verso la banca per l'esatto adempimento del proprio incarico.

Il perito esterno non può a sua volta incaricare soggetti terzi dello svolgimento dell'incarico ricevuto.

2.2.3. Attività di valutazione degli immobili posti a garanzia delle esposizioni

L'immobile deve essere stimato a un valore non superiore al valore di mercato (11).

La valutazione dell'immobile è documentata attraverso un'apposita relazione corredata da tutti i documenti utilizzati per effettuarla.

Nel caso in cui la valutazione dell'immobile sia svolta da un perito esterno la banca acquisisce la relazione di valutazione.

La relazione di valutazione è conservata in maniera ordinata dalla banca su supporto cartaceo o altro supporto durevole per tutta la durata del rapporto con il cliente e per i dieci anni successivi all'estinzione del rapporto.

(10) Ai sensi dell'art. 1, comma 2, lett. h-*novies*), TUB, per "personale" si intende: "i dipendenti e coloro che comunque operano sulla base di rapporti che ne determinano l'inserimento nell'organizzazione aziendale, anche in forma diversa dal rapporto di lavoro subordinato".

(11) Per la definizione di "valore di mercato" si rimanda a quanto previsto dall'art. 4, n. 76), CRR.

Parte I – Recepimento in Italia della CRD IV

Titolo IV - Governo societario, controlli interni, gestione dei rischi

Capitolo 3 – Il sistema dei controlli interni

Allegato A – Disposizioni speciali relative a particolari categorie di rischio

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 contenuti nella Parte tre, Titolo II, Capo 4 del CRR.

4. Concentrazione dei rischi

Regole organizzative specifiche in materia di grandi esposizioni sono contenute nella Parte Seconda, Capitolo 10, 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. Parte Prima, Titolo III, Sezione III, Allegato B).

5. Rischi derivanti da operazioni di cartolarizzazione

Regole organizzative specifiche in materia di operazioni di cartolarizzazione sono contenute nella Parte cinque, Titolo II del CRR e nella Parte Seconda, Capitolo 6.

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 nella Parte tre, Titolo IV del CRR.

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.

Parte I – Recepimento in Italia della CRD IV

Titolo IV - Governo societario, controlli interni, gestione dei rischi

Capitolo 3 – Il sistema dei controlli interni

Allegato A – Disposizioni speciali relative a particolari categorie di rischio

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. Parte Prima, Titolo III, Capitolo 1, Sezione III, Allegato C e Allegato C-bis).

In proposito le banche applicano la sezione 4.3 degli orientamenti EBA in materia di *governance* del rischio di tasso di interesse derivante da attività diverse dalla negoziazione (EBA/GL/2018/02) (12).

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 approvate e attuate 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 riportate nella Parte tre, Titolo III del CRR. Esse 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*”).

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 organizzativi da predisporre a fronte di questa categoria di rischio (cfr. Capitolo 6).

(12) Ai fini dell’applicazione di questi Orientamenti, per “organo di gestione” si intende l’“organo con funzione di supervisione strategica” e per “alta dirigenza” si intende l’“organo con funzione di gestione” (come definiti nella Parte Prima, Titolo IV, Capitolo 3, Sezione 1).

Parte I – Recepimento in Italia della CRD IV

Titolo IV - Governo societario, controlli interni, gestione dei rischi

Capitolo 3 – Il sistema dei controlli interni

Allegato A – Disposizioni speciali relative a particolari categorie di rischio

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 nella Parte terza, Capitolo 3, Sezione II, Paragrafo 5.

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 nella Parte Terza, Capitolo 1, 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 le disposizioni in materia di controlli interni e responsabilità degli organi aziendali contenute nella Parte III, Capitolo 11.

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 VIII, Capitolo 1, Sezioni II e IV del Regolamento sulla gestione collettiva del risparmio del 19 gennaio 2015.

Parte I – Recepimento in Italia della CRD IV

Titolo IV - Governo societario, controlli interni, gestione dei rischi

Capitolo 3 – Il sistema dei controlli interni

Allegato A – Disposizioni speciali relative a particolari categorie di rischio

15. Rischio paese e rischio di trasferimento (*Country and transfer risks*)

Le banche sono tenute a presidiare efficacemente, in linea con il principio di proporzionalità, il rischio paese (13) e il rischio di trasferimento (14).

In particolare, le banche, tengono conto di tali rischi nell’ambito del RAF, del processo per determinare il capitale complessivo adeguato in termini attuali e prospettici (ICAAP) (15) e del processo di gestione dei rischi.

Le banche formalizzano criteri per la determinazione di accantonamenti adeguati a fronte delle singole esposizioni soggette ai rischi menzionati.

16. Gestione del rischio connesso alla quota di attività vincolate (*encumbered assets*) (16)

Nell’ambito del RAF e del processo di gestione dei rischi, le banche tengono anche conto del rischio connesso alla quota di attività vincolate. In particolare, nel delineare le politiche di governo del rischio di *asset encumbrance*, le banche valutano i seguenti fattori: i) il modello di *business* della banca; ii) gli Stati in cui la stessa opera; iii) le specificità dei mercati della provvista; iv) la situazione macroeconomica.

Le banche includono nei propri piani di emergenza (di cui al Capitolo 6, Sezione III) strategie volte a gestire il potenziale aumento della quota di attività vincolate derivante da situazioni di tensione rilevanti, ossia da shock plausibili benché improbabili, avendo riguardo anche al declassamento del *rating* del credito della banca, alla svalutazione delle attività costituite in pegno e all’aumento dei requisiti di margine.

Le banche assicurano che gli organi aziendali ricevano informazioni tempestive almeno in merito a: i) livello, evoluzione e natura delle attività vincolate e fonti costitutive del vincolo, quali operazioni di finanziamento garantite o altre transazioni; ii) ammontare evoluzione e qualità creditizia delle attività non vincolate ma vincolabili, con un’indicazione del volume di attività potenzialmente vincolabili; iii) ammontare, evoluzione e natura delle attività vincolate risultante dal materializzarsi di scenari di stress (quota potenziale di attività vincolate).

17. Gestione del rischio di credito e rilevazione contabile delle perdite attese su crediti (*expected credit losses*)

Nella gestione del rischio di credito e nella rilevazione contabile delle perdite attese su crediti le banche applicano le sezioni 2, 3 e le sottosezioni 4.1, 4.2.1, 4.2.2, 4.2.3, 4.2.4, 4.2.5, 4.2.6,

(13) Il rischio paese è il rischio di perdite causate da eventi che si verificano in un paese diverso dall’Italia. Il concetto di rischio paese è più ampio di quello di rischio sovrano in quanto è riferito a tutte le esposizioni indipendentemente dalla natura delle controparti, siano esse persone fisiche, imprese, banche o amministrazioni pubbliche.

(14) Il rischio di trasferimento è il rischio che una banca, esposta nei confronti di un soggetto che si finanzia in una valuta diversa da quella in cui percepisce le sue principali fonti di reddito, realizzi delle perdite dovute alle difficoltà del debitore di convertire la propria valuta nella valuta in cui è denominata l’esposizione.

(15) Cfr. Parte Prima, Titolo III, Sezione II - La valutazione aziendale dell’adeguatezza patrimoniale (ICAAP).

(16) Per la definizione di “*encumbered asset*” si rimanda alla “Raccomandazione relativa al finanziamento degli enti creditizi (ESRB/2012/2)”, 20 dicembre 2012, Sezione 2.

DISPOSIZIONI DI VIGILANZA PER LE BANCHE

Parte I – Recepimento in Italia della CRD IV

Titolo IV - Governo societario, controlli interni, gestione dei rischi

Capitolo 3 – Il sistema dei controlli interni

Allegato A – Disposizioni speciali relative a particolari categorie di rischio

4.2.7 e 4.3 degli *Orientamenti in materia di pratiche di gestione del rischio di credito e di rilevazione contabile delle perdite attese su crediti degli enti creditizi* dell'EBA (17).

Ai fini dell'applicazione di questi Orientamenti, per “organo di gestione” si intende l’“organo con funzione di supervisione strategica” e per “alta dirigenza” si intende l’“organo con funzione di gestione” (come definiti nella Parte Prima, Titolo IV, Capitolo 3, Sezione 1).

(17) https://www.eba.europa.eu/documents/10180/1965596/Guidelines+on+Accounting+for+ECL+%28EBA-GL-2017-06%29_IT.pdf/6083495c-2d89-40af-ab37-7d8dd891c202.

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, tenuto conto sia della rischiosità della succursale rispetto alla complessiva propensione al rischio della banca, sia della complessità operativa/organizzativa della succursale stessa, un'unità incaricata dei controlli di secondo livello e un'unità avente funzioni di revisione interna. Gli addetti a tali unità, di norma gerarchicamente dipendenti dalle funzioni 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 a 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 proporre 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.

DISPOSIZIONI DI VIGILANZA PER LE BANCHE

Parte I – Recepimento in Italia della CRD IV

Titolo IV - Governo societario, controlli interni, gestione dei rischi

Capitolo 3 – Il sistema dei controlli interni

Allegato B – Controlli sulle succursali estere

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 è graduata in relazione all'operatività svolta e ai mercati di insediamento. I risultati delle verifiche sono portati tempestivamente a conoscenza degli organi aziendali.

IL RISK APPETITE FRAMEWORK

1. Premessa

Le banche definiscono un quadro di riferimento per la determinazione della propensione al rischio (*Risk Appetite Framework* - “RAF”), che fissi *ex ante* gli obiettivi di rischio/rendimento che l’intermediario intende raggiungere e i conseguenti limiti operativi.

La formalizzazione, attraverso la definizione del RAF, di obiettivi di rischio coerenti con il massimo rischio assumibile, il *business model* e gli indirizzi strategici è un elemento essenziale per la determinazione di una politica di governo dei rischi e di un processo di gestione dei rischi improntati ai principi della sana e prudente gestione aziendale.

Le banche, inoltre, coordinano il quadro di riferimento per la determinazione della propensione al rischio con il processo ICAAP (cfr. Parte Prima, Titolo III, Capitolo 1) e ne assicurano la corretta attuazione attraverso una organizzazione e un sistema dei controlli interni adeguati (1).

2. Indicazioni sul contenuto del RAF

Nel presente paragrafo sono fornite indicazioni minimali per la definizione del *Risk Appetite Framework*, fermo restando che l’effettiva articolazione del RAF va calibrata in base alle caratteristiche dimensionali e di complessità operativa di ciascuna banca.

Le banche assicurano una stretta coerenza e un puntuale raccordo tra: il modello di *business*, il piano strategico le prove di stress, il RAF (e i parametri utilizzati per definirlo), il processo ICAAP, i budget, l’organizzazione aziendale e il sistema dei controlli interni.

Il RAF, tenuto conto del piano strategico e dei rischi rilevanti ivi individuati, e definito il massimo rischio assumibile, indica le tipologie di rischio che la banca intende assumere; per ciascuna tipologia di rischio, fissa gli obiettivi di rischio, le eventuali soglie di tolleranza e i limiti operativi in condizioni sia di normale operatività, sia di stress. Sono, altresì, indicate le circostanze, inclusi gli esiti degli scenari di stress, al ricorrere delle quali l’assunzione di determinate categorie di rischio va evitata o contenuta rispetto agli obiettivi e ai limiti fissati.

Gli obiettivi di rischio, le soglie di tolleranza e i limiti di rischio sono, di norma, declinati in termini di:

- a. misure espressive del capitale a rischio o capitale economico (VaR, *expected shortfall*, ecc);
- b. adeguatezza patrimoniale;
- c. liquidità.

(1) Nell’ambito della definizione del RAF, il perimetro delle attività e dei rischi presi in considerazione coincide almeno con quello utilizzato ai fini del calcolo dei requisiti prudenziali su base consolidata.

DISPOSIZIONI DI VIGILANZA PER LE BANCHE

Parte I – Recepimento in Italia della CRD IV

Titolo IV - Governo societario, controlli interni, gestione dei rischi

Capitolo 3 – Il sistema dei controlli interni

Allegato C – Il *risk appetite framework*

Con riferimento ai rischi quantificabili, la declinazione degli elementi costituenti del RAF avviene attraverso l'utilizzo di opportuni parametri quantitativi e qualitativi, calibrati in funzione del principio di proporzionalità; a tal fine, le banche possono fare riferimento alle metodologie di misurazione dei rischi utilizzate ai fini della valutazione aziendale dell'adeguatezza patrimoniale (ICAAP) (cfr. Parte Prima, Titolo III, Capitolo 1, Sezione II).

Con riferimento ai rischi difficilmente quantificabili (quali, ad es. il rischio strategico, il rischio reputazionale o il rischio di *compliance*), il RAF fornisce specifiche indicazioni di carattere qualitativo che siano in grado di orientare la definizione e l'aggiornamento dei processi e dei presidi del sistema dei controlli interni.

Nel RAF sono definite le procedure e gli interventi gestionali da attivare nel caso in cui sia necessario ricondurre il livello di rischio entro l'obiettivo o i limiti prestabiliti. In particolare, sono definiti gli interventi gestionali da adottare al raggiungimento della soglia di tolleranza (ove definita). Sono precisate anche le tempistiche e le modalità da seguire per l'aggiornamento del RAF.

Il RAF, infine, precisa i compiti degli organi e di tutte le funzioni aziendali coinvolte nella definizione del processo.

Parte Prima – Recepimento in Italia della CRD IV

Titolo IV – Governo societario, controlli interni e gestione dei rischi

Capitolo 4 – Il sistema informativo

TITOLO IV

Capitolo 4

IL SISTEMA INFORMATIVO

Parte Prima – Recepimento in Italia della CRD IV

Titolo IV – Governo societario, controlli interni e gestione dei rischi

Capitolo 4 – Il sistema informativo

Sezione I – Disposizioni di carattere generale

TITOLO IV - Capitolo 4

IL SISTEMA INFORMATIVO

SEZIONE I

DISPOSIZIONI DI CARATTERE GENERALE

1. Premessa

Il sistema informativo – inclusivo delle risorse tecnologiche (hardware, software, dati, documenti elettronici, reti telematiche), dei processi e delle procedure, nonché delle risorse umane dedicate alla loro gestione – rappresenta uno strumento di primaria importanza per il conseguimento degli obiettivi strategici e operativi degli intermediari, in considerazione della criticità dei processi aziendali che dipendono da esso. Infatti:

- dal punto di vista strategico, un sistema informativo sicuro ed efficiente, basato su un’architettura flessibile, resiliente e integrata a livello di gruppo consente di sfruttare le opportunità offerte dalla tecnologia per ampliare e migliorare i prodotti e i servizi per la clientela, innovare i modelli di business, accrescere la qualità dei processi di lavoro, favorire la dematerializzazione dei valori, ridurre i costi anche attraverso la virtualizzazione dei servizi bancari;
- nell’ottica della sana e prudente gestione, il sistema informativo consente al management di disporre di informazioni dettagliate, pertinenti e aggiornate per l’assunzione di decisioni consapevoli e tempestive e per la corretta attuazione del processo di gestione dei rischi (cfr. Capitolo 3);
- 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, fanno affidamento sulla funzionalità dei processi e dei controlli automatizzati;
- in tema di *compliance*, al sistema informativo 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 e da regolamenti interni ed esterni.

Le previsioni contenute nel presente Capitolo rappresentano requisiti di carattere generale per lo sviluppo e la gestione del sistema informativo da parte degli intermediari; le concrete misure da adottare tengono conto degli specifici obiettivi strategici e, secondo il principio di proporzionalità, della dimensione, dell’assetto organizzativo, delle complessità operative della banca e del livello di automazione dei suoi processi e servizi, nonché della natura dell’attività svolta con riferimento, in particolare, alla tipologia, all’ambito, alla complessità e alla rischiosità dei prodotti e dei servizi prestati o che si intende prestare.

Parte Prima – Recepimento in Italia della CRD IV

Titolo IV – Governo societario, controlli interni e gestione dei rischi

Capitolo 4 – Il sistema informativo

Sezione I – Disposizioni di carattere generale

A tal proposito, le banche valutano l'opportunità di avvalersi degli standard e *best practice* definiti a livello internazionale in materia di governo, gestione, sicurezza e controllo del sistema informativo.

I requisiti di carattere generale sono integrati da requisiti organizzativi specifici da adottare in funzione dell'attività esercitata o di specifiche tipologie di rischio cui la banca è esposta. Particolare rilievo assumono i rischi assunti in relazione alla prestazione di servizi di pagamento (cfr. Sezione VII).

2. Fonti normative

La materia è regolata:

— dalle seguenti disposizioni del TUB:

- art. 51, il quale prevede che le banche inviino alla Banca d'Italia, con le modalità e i tempi da essa stabiliti, le segnalazioni periodiche nonché ogni dato e documento richiesti;
- art. 53, comma 1, lett. d), che attribuisce alla Banca d'Italia il potere di emanare disposizioni di carattere generale in materia di organizzazione amministrativa e contabile e controlli interni delle banche;
- art. 67, comma 1, lett. d), il quale prevede che, al fine di esercitare la vigilanza consolidata, la Banca d'Italia impartisca alla capogruppo, con provvedimenti di carattere generale, disposizioni concernenti il gruppo complessivamente considerato o i suoi componenti aventi ad oggetto l'organizzazione amministrativa e contabile e i controlli interni;
- art. 146, comma 2 lett. b), che attribuisce alla Banca d'Italia il potere di emanare disposizioni aventi ad oggetto gli assetti organizzativi e di controllo relativi alle attività svolte nel sistema dei pagamenti;

e inoltre:

- dal decreto legislativo 27 gennaio 2010, n. 11, Attuazione della direttiva 2007/64/CE, relativa ai servizi di pagamento nel mercato interno, recante modifica delle direttive 97/7/CE, 2002/65/CE, 2005/60/CE, 2006/48/CE, e che abroga la direttiva 97/5/CE, e successive modifiche e integrazioni (d.lgs. n. 11/2010);
- del decreto legislativo 5 dicembre 2017, n. 218, Recepimento della direttiva (UE) 2015/2366 relativa ai servizi di pagamento nel mercato interno (PSD2), che modifica le direttive 2002/65/CE, 2009/110/CE e 2013/36/UE e il regolamento (UE) n. 1093/2010, e abroga la direttiva 2007/64/CE, nonché adeguamento delle disposizioni interne al regolamento (UE) n. 751/2015 relativo alle commissioni interbancarie sulle operazioni di pagamento basate su carta;
- dal regolamento della Commissione europea recante le norme tecniche di regolamentazione per l'autenticazione forte del cliente e gli standard aperti di comunicazione comuni e sicuri (Regolamento delegato (UE) 2018/389 del 27 novembre 2017).

Vengono altresì in rilievo:

Parte Prima – Recepimento in Italia della CRD IV

Titolo IV – Governo societario, controlli interni e gestione dei rischi

Capitolo 4 – Il sistema informativo

Sezione I – Disposizioni di carattere generale

- la direttiva CRD;
- la direttiva (UE) 2015/2366 del Parlamento europeo e del Consiglio del 25 novembre 2015 relativa ai servizi di pagamento nel mercato interno, che modifica le direttive 2002/65/CE, 2009/110/CE e 2013/36/UE e il regolamento (UE) n.1093/2010, e abroga la direttiva 2007/64/CE (PSD2);
- gli Orientamenti aggiornati in materia di segnalazione dei gravi incidenti ai sensi della PSD2 (EBA/GL/2021/03), emanati dall'EBA il 10 giugno 2021 (1);
- gli Orientamenti sulle condizioni per beneficiare dell'esenzione dal meccanismo di emergenza a norma dell'articolo 33, paragrafo 6, del regolamento (UE) 2018/389 (norme tecniche di regolamentazione per l'autenticazione forte del cliente e gli *standard* aperti di comunicazione comuni e sicuri, RTS on SCA and SCS) (EBA/GL/2018/07), emanati dall'EBA il 4 dicembre 2018;
- gli Orientamenti in materia di esternalizzazione (EBA/GL/2019/02) emanati dall'EBA il 25 febbraio 2019;
- gli Orientamenti sulla gestione dei rischi relativi alle tecnologie dell'informazione (*Information and Communication Technology*, ICT) e di sicurezza (EBA/GL/2019/04) emanati dall'EBA il 28 novembre 2019.

Si è anche tenuto conto di:

- i *Principles for effective risk data aggregation and risk reporting*, pubblicato dal Comitato di Basilea per la vigilanza bancaria (*Basel Committee for Banking Supervision*, BCBS) nel gennaio 2013 (2);
- i *Principles for operational resilience*, pubblicati dal BCBS il 31 marzo 2021 (3);
- l'*Opinion on the implementation of the RTS on SCA and CSC* (EBA-Op-2018-04), emanata dall'EBA in data 13 giugno 2018;
- l'*Opinion on the use of eIDAS certificates under the RTS on SCA and CSC* (EBA-Op-2018-7), emanata dall'EBA in data 10 dicembre 2018;
- l'*Opinion on the elements of strong customer authentication under PSD2* (EBA-Op-2019-06), emanata dall'EBA il 21 giugno 2019;
- l'*Opinion on obstacles to the provision of third-party provider services under the Payment Services Directive* (EBA/OP/2020/10), emanata dall'EBA il 4 giugno 2020.

3. Definizioni

Ai fini della presente disciplina si definisce:

-
- (1) Le EBA/GL/2021/03 sono attuate con la Comunicazione della Banca d'Italia del 29 ottobre 2021.
<https://www.bancaditalia.it/compiti/vigilanza/normativa/archivio-norme/comunicazioni/com-20211029/index.html>.
- (2) <http://www.bis.org/publ/bcbs239.pdf>.
- (3) <https://www.bis.org/bcbs/publ/d516.pdf>.

DISPOSIZIONI DI VIGILANZA PER LE BANCHE

Parte Prima – Recepimento in Italia della CRD IV

Titolo IV – Governo societario, controlli interni e gestione dei rischi

Capitolo 4 – Il sistema informativo

Sezione I – Disposizioni di carattere generale

- “*no single point of failure*”: il principio architettonico secondo il quale l’eventuale guasto di un singolo componente di un sistema non compromette il regolare funzionamento dell’intero sistema;
- “*operazioni critiche*”: le operazioni relative a funzioni essenziali o importanti effettuate in ambiente di produzione che, se errate o non effettuate, possono pregiudicare il regolare funzionamento di componenti critiche del sistema informativo (con riferimento a dati, a programmi o alla configurazione del sistema) nonché quelle che possono alterare, direttamente o indirettamente, i valori aziendali;
- “*procedura di contingency*”: una procedura che, in caso di indisponibilità o grave malfunzionamento del sistema, prevede il ricorso in condizioni di emergenza a strumenti a bassa integrazione nei processi aziendali (ad es., ricorrendo ad attività manuali) al fine di completare un insieme limitato di operazioni di particolare criticità;
- “*procedura di fall-back*”: una procedura attivata in occasione di gravi problemi in caso di aggiornamento tecnologico o migrazione a nuove piattaforme, volta a fornire modalità alternative per lo svolgimento delle funzioni applicative non funzionanti;
- “*progetti ICT*”: qualsiasi progetto, o parte di esso, in cui i sistemi e i servizi ICT sono modificati, sostituiti, dismessi o implementati. I progetti ICT possono far parte di più ampi programmi ICT o di trasformazione aziendale;
- “*rischio ICT e di sicurezza*”: il rischio di incorrere in perdite dovuto alla violazione della riservatezza, carente integrità dei sistemi e dei dati, inadeguatezza o indisponibilità dei sistemi e dei dati o incapacità di sostituire la tecnologia dell’informazione (IT) entro ragionevoli limiti di tempo e costi in caso di modifica dei requisiti del contesto esterno o dell’attività (*agility*), nonché i rischi di sicurezza derivanti da processi interni inadeguati o errati o da eventi esterni, inclusi gli attacchi informatici o un livello di sicurezza fisica inadeguata. Nella rappresentazione integrata dei rischi aziendali a fini prudenziali (ICAAP), tale tipologia di rischio è considerata, secondo gli specifici aspetti, tra i rischi operativi, reputazionali e strategici;
- “*rischio ICT e di sicurezza residuo*”: il rischio ICT e di sicurezza a cui l’intermediario è esposto una volta applicate le misure di attenuazione individuate nel processo di analisi dei rischi;
- “*risk appetite (obiettivo di rischio o propensione al rischio)*”: il *risk appetite* come definito, nell’ambito del *risk appetite framework* (RAF), nel Capitolo 3, Sezione I, paragrafo 2;
- “*risorsa informatica (o ICT)*”: qualsiasi *software* o *hardware* presente nel contesto aziendale;
- “*risorsa informativa*”: una raccolta di informazioni, tangibile o intangibile, che merita protezione;
- “*segregazione dei compiti (segregation of duties)*”: il principio che stabilisce che l’esecuzione di operazioni di particolare criticità sia svolta attraverso la cooperazione di più utenti o amministratori di sistema con responsabilità formalmente ripartite;
- “*servizi ICT*”: i servizi forniti dai sistemi ICT a uno o più utenti interni o esterni. Tali servizi comprendono, ad esempio: servizi di inserimento, archiviazione, elaborazione e

Parte Prima – Recepimento in Italia della CRD IV

Titolo IV – Governo societario, controlli interni e gestione dei rischi

Capitolo 4 – Il sistema informativo

Sezione I – Disposizioni di carattere generale

comunicazione di dati, servizi di monitoraggio, di supporto alle attività e alle decisioni aziendali;

- “*sistemi ICT*”: ICT adottato come parte di un meccanismo o di una rete di interconnessione a supporto delle operazioni della banca;
- “*soggetto terzo*”: un soggetto o organizzazione che ha stretto rapporti commerciali o stipulato contratti con una banca per la fornitura di un prodotto o un servizio;
- “*utente responsabile*”: la figura aziendale identificata per ciascun sistema ICT e che ne assume formalmente la responsabilità, in rappresentanza degli utenti e nei rapporti con le funzioni preposte allo sviluppo e alla gestione tecnica;
- “*verificabilità*”: la garanzia di poter ricostruire, all’occorrenza e anche a distanza di tempo, eventi connessi all’utilizzo del sistema informativo e al trattamento di dati.

Con riferimento alla prestazione dei servizi di pagamento, restano ferme le definizioni previste dal d.lgs. n. 11/2010 e dalle disposizioni attuative di PSD2 direttamente applicabili.

Nei casi in cui le presenti disposizioni rinviano direttamente agli Orientamenti dell’EBA in materia di gestione dei rischi ICT e di sicurezza, ai fini della loro applicazione si precisa che:

- per “alta dirigenza” si intende l’“organo con funzione di gestione” come definito nel Capitolo 1;
- per “funzione di *audit*” si intende la “funzione di revisione interna” (4).

4. Destinatari della disciplina

Le presenti disposizioni si applicano:

- alle banche italiane e alle succursali di banche extracomunitarie, ad eccezione di quelle aventi sede negli Stati indicati nell’Allegato A delle Disposizioni introduttive (5); queste ultime applicano le presenti disposizioni esclusivamente con riferimento alla prestazione di servizi di pagamento;
- alle capogruppo di gruppi bancari;
- alle imprese di riferimento, secondo quanto previsto dalla Sezione VI del Capitolo 3.

5. Procedimenti amministrativi

Si indicano di seguito i procedimenti amministrativi relativi al presente Capitolo:

(4) Cfr. Capitolo 3, Sezione III, in particolare par. 3.4.

(5) Per le banche che prestano servizi di investimento, cfr. inoltre le disposizioni del regolamento della Banca d’Italia di attuazione degli articoli 4-*undecies* e 6, comma 1, lettere b) e *c-bis*), del Testo Unico della Finanza (TUF), in particolare articolo 5, comma 2.

DISPOSIZIONI DI VIGILANZA PER LE BANCHE

Parte Prima – Recepimento in Italia della CRD IV

Titolo IV – Governo societario, controlli interni e gestione dei rischi

Capitolo 4 – Il sistema informativo

Sezione I – Disposizioni di carattere generale

- *esenzione dall'obbligo di predisporre l'interfaccia di fall-back prevista dall'art. 33, par. 4 del Regolamento delegato 2018/389 della Commissione Europea del 27 novembre 2017, ai sensi dell'art. 33, par. 6 del Regolamento delegato 2018/389 (termine: 45 giorni);*
- *revoca dell'esenzione dall'obbligo di predisporre l'interfaccia di fall-back prevista dall'art. 33, par. 4 del Regolamento delegato 2018/389 della Commissione Europea del 27 novembre 2017, ai sensi dell'art. 33, par. 7 del Regolamento delegato 2018/389 (termine: 45 giorni).*

SEZIONE II

GOVERNO, ORGANIZZAZIONE E CONTROLLI DEL SISTEMA INFORMATIVO

1. Premessa

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 del sistema informativo e dei rischi ICT e di sicurezza, nel rispetto del principio della separazione delle funzioni di controllo da quelle di supervisione e gestione.

2. Compiti degli organi aziendali per i profili ICT

2.1 Compiti dell'organo con funzione di supervisione strategica

L'organo con funzione di supervisione strategica assume la generale responsabilità di indirizzo e controllo del sistema informativo, nell'ottica di un ottimale impiego delle risorse tecnologiche a sostegno delle strategie aziendali (*ICT governance*).

In tale ambito esso:

- definisce e approva la strategia ICT, in considerazione dell'evoluzione del settore di riferimento e in coerenza con gli indirizzi strategici della banca e con l'articolazione attuale e prospettica dei settori di operatività, dei processi e dell'organizzazione aziendale; in tale contesto approva il modello di riferimento per l'architettura del sistema informativo. La strategia ICT definisce: a) il modo in cui il sistema ICT aziendale dovrebbe evolvere per supportare e contribuire efficacemente alla strategia aziendale, inclusa l'evoluzione della struttura organizzativa, le modifiche dei sistemi ICT e le dipendenze chiave da soggetti terzi; b) l'evoluzione pianificata dell'architettura ICT, incluse le dipendenze da soggetti terzi; c) chiari obiettivi in materia di sicurezza dell'informazione, soprattutto con riferimento ai sistemi e ai servizi ICT, al personale e ai processi;
- approva l'assetto organizzativo e di governo della banca con riferimento al sistema informativo, alla gestione del rischio ICT e di sicurezza e alla continuità operativa, garantendo la chiara distinzione dei compiti e delle responsabilità degli organi e delle funzioni aziendali (1);
- approva:
 - a. i piani d'azione predisposti dall'organo con funzione di gestione per l'attuazione della strategia ICT;
 - b. la *policy* di sicurezza dell'informazione (2);

(1) Inclusi, se previsti, i comitati endo-consiliari.

(2) Nel caso di *full outsourcing* del sistema informativo l'organo di supervisione strategica, qualora non abbia le necessarie competenze al proprio interno, potrà avvalersi di risorse esterne indipendenti dal fornitore di servizi. Inoltre, nella definizione dei documenti richiesti (cfr. Allegato A), si può fare riferimento ad analogha documentazione prodotta dal fornitore.

Parte Prima – Recepimento in Italia della CRD IV

Titolo IV – Governo societario, controlli interni e gestione dei rischi

Capitolo 4 – Il sistema informativo

Sezione II – Governo, organizzazione e controlli del sistema informativo

- c. le linee di indirizzo in materia di selezione del personale con funzioni tecniche e di acquisizione di sistemi, software e servizi ICT, incluso il ricorso a soggetti terzi e all'esternalizzazione (cfr. Sezione VI);
- promuove lo sviluppo, la condivisione e l'aggiornamento di conoscenze in materia di ICT all'interno dell'azienda;
- è informato:
 - a. con cadenza almeno annuale circa l'adeguatezza dei servizi erogati e il supporto di tali servizi all'evoluzione dell'operatività aziendale, in rapporto ai costi sostenuti;
 - b. periodicamente circa l'applicazione e l'adeguatezza dei piani d'azione per l'attuazione della strategia ICT;
 - c. tempestivamente in caso di gravi problemi per l'attività aziendale derivanti da incidenti e malfunzionamenti del sistema informativo; ed è aggiornato su impatto, misure correttive e controlli aggiuntivi a seguito di tali eventi;
 - d. circa l'avvio e l'avanzamento dei progetti ICT, considerati singolarmente o in forma aggregata e in funzione delle loro dimensioni e importanza e dei rischi ad essi associati, su base periodica e, se del caso, all'occorrenza;
- assicura che il sistema di governo e controllo dei rischi ICT e di sicurezza sia costantemente adeguato, anche in termini di dimensionamento qualitativo e quantitativo del personale e di risorse finanziarie disponibili, alle esigenze operative della funzione ICT e dei processi di gestione dei rischi ICT e di sicurezza e per l'attuazione della strategia ICT.

Con riguardo all'esercizio della responsabilità di supervisione della gestione del rischio ICT e di sicurezza (cfr. Sezione III), lo stesso organo:

- approva il quadro di riferimento organizzativo e metodologico per la gestione del rischio ICT e di sicurezza, promuovendo l'opportuna valorizzazione dell'informazione sul rischio tecnologico all'interno della funzione ICT e l'integrazione con i sistemi di misurazione e gestione dei rischi (in particolare quelli operativi, reputazionali e strategici). Il quadro di riferimento è rivisto almeno annualmente, anche alla luce dell'esperienza acquisita durante la sua attuazione e il suo monitoraggio, in un'ottica di continuo miglioramento;
- approva la propensione al rischio ICT e di sicurezza, avuto riguardo ai servizi interni e a quelli offerti alla clientela, in conformità con gli obiettivi di rischio e il quadro di riferimento per la determinazione della propensione al rischio definiti a livello aziendale (cfr. Capitolo 3, Allegato C);
- è informato in maniera chiara e tempestiva, e in ogni caso con cadenza almeno annuale, sulla situazione di rischio ICT e di sicurezza rispetto alla propensione al rischio, inclusi i risultati della valutazione dei rischi.

Nell'Allegato A, sono riportati i documenti che l'organo con funzione di supervisione strategica approva nell'ambito del suo ruolo e responsabilità nella materia.

Parte Prima – Recepimento in Italia della CRD IV

Titolo IV – Governo societario, controlli interni e gestione dei rischi

Capitolo 4 – Il sistema informativo

Sezione II – Governo, organizzazione e controlli del sistema informativo

2.2. *Compiti dell'organo con funzione di gestione*

L'organo con funzione di gestione ha il compito di assicurare la completezza, l'adeguatezza, la funzionalità (in termini di efficacia ed efficienza) e l'affidabilità del sistema informativo. In particolare, tale organo:

- definisce i piani di azione contenenti le misure da adottare per conseguire gli obiettivi della strategia ICT, ne monitora e misura l'efficacia, ne cura il riesame periodico per assicurarne l'adeguatezza e la coerenza con la strategia aziendale nel tempo, informando a tale riguardo l'organo con funzione di supervisione strategica. Inoltre, si assicura che il contenuto dei piani d'azione approvati dall'organo con funzione di supervisione strategica sia comunicato a tutto il personale interessato, inclusi i soggetti terzi ove opportuno;
- definisce la struttura organizzativa della funzione ICT (ove presente) (3) assicurandone nel tempo la rispondenza alle strategie e ai modelli architetturali definiti dall'organo con funzione di supervisione strategica;
- definisce i ruoli e le responsabilità per la funzione ICT e per la gestione del rischio ICT e di sicurezza, nonché per le relative attività di continuità operativa (4);
- definisce l'assetto organizzativo, metodologico e procedurale per il processo di gestione del rischio ICT e di sicurezza, perseguendo un opportuno livello di raccordo con la funzione di *risk management* per i processi di stima del rischio operativo;
- assicura che tutto il personale, incluso il personale che riveste ruoli chiave, riceva una formazione adeguata in materia di rischi ICT e di sicurezza, nonché di sicurezza dell'informazione, almeno una volta all'anno o con maggiore frequenza se necessario; al riguardo, definisce e approva un piano di formazione e di sensibilizzazione sulla sicurezza dell'informazione;
- approva le procedure e i processi di gestione delle operazioni ICT che riguardano le risorse e i servizi non esternalizzati, garantendo l'efficacia ed efficienza dell'impianto nonché la complessiva completezza e coerenza, con particolare riguardo a una 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 (ove del caso, in raccordo con le procedure del fornitore di servizi) 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 o utilizzando sistemi integrati di

(3) Nel caso di gruppo bancario che abbia accentrato la funzione ICT in una società controllata del gruppo, il compito di definizione della funzione ICT può essere demandato all'organo con funzione di gestione di tale società, previa individuazione di opportuni canali informativi verso gli organi aziendali della capogruppo.

(4) Per quanto riguarda gli aspetti relativi al ruolo e ai compiti degli organi aziendali con riferimento alla continuità operativa per il sistema informativo, si veda il Capitolo 5, Allegato A, Sezione II, par. 3 (in particolare, 3.1).

Parte Prima – Recepimento in Italia della CRD IV

Titolo IV – Governo societario, controlli interni e gestione dei rischi

Capitolo 4 – Il sistema informativo

Sezione II – Governo, organizzazione e controlli del sistema informativo

misurazione delle prestazioni (5), assumendo gli opportuni interventi e iniziative di miglioramento;

- approva almeno annualmente la valutazione del rischio delle componenti critiche nonché la relazione sull'adeguatezza e costi dei servizi ICT, informando a tale riguardo l'organo con funzione di supervisione strategica; in tale ambito, riscontra la complessiva situazione del rischio ICT e di sicurezza in rapporto alla propensione al rischio definita, disponendo allo scopo di idonei flussi informativi concernenti, come minimo, il livello di rischio residuo per le diverse risorse informatiche, lo stato di implementazione dei presidi di attenuazione del rischio (cfr. Sezione III), l'evoluzione delle minacce connesse con l'utilizzo di ICT nonché gli incidenti registratisi nel periodo di riferimento;
- monitora il regolare svolgimento dei processi di gestione e di controllo dei servizi ICT e, a fronte di anomalie rilevate, pone in atto opportune azioni correttive;
- assume decisioni tempestive in merito a gravi incidenti operativi o di sicurezza (cfr. Sezione IV), di cui è prontamente informato, e fornisce informazioni all'organo con funzione di supervisione strategica in caso di gravi problemi per l'attività aziendale derivanti da incidenti e malfunzionamenti, con particolare riferimento all'impatto, alla risposta e ai controlli supplementari da definire.

In relazione alla responsabilità e ai compiti assegnati, l'organo con funzione di gestione è dotato di competenze tecnico – manageriali, tenuto conto della dimensione, complessità e articolazione organizzativa dell'intermediario nonché delle strategie di *sourcing*.

Nell'Allegato A sono riportati le procedure, gli standard e i piani soggetti all'approvazione dell'organo con funzione di gestione.

3. Organizzazione della funzione ICT

La funzione ICT è responsabile dello svolgimento dei processi operativi del sistema informativo. L'articolazione organizzativa della funzione ICT dipende da fattori quali la complessità della struttura societaria, la dimensione, i settori di attività, le strategie di *business* e gestionali. Essa si ispira a criteri di funzionalità, efficienza e sicurezza, definendo chiaramente compiti e responsabilità e contemplando in particolare:

- linee di riporto dirette a livello dell'organo con funzione di gestione (6) a garanzia dell'unitarietà della visione gestionale e del rischio ICT e di sicurezza nonché dell'uniformità di applicazione delle norme riguardanti il sistema informativo; eventuali unità di sviluppo

(5) I sistemi integrati di misurazione e *reporting* delle prestazioni sono procedure automatizzate, di norma basate su metodologie (ad es., *balanced scorecards*) volte 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. In caso di *outsourcing* è opportuno definire nel contratto un insieme di *report* minimi, utili anche a verificare il rispetto delle SLA (*Service level agreement*).

(6) Nel caso di gruppo bancario che abbia accentrato la funzione ICT in una società controllata, è possibile individuare all'interno di questa l'organo responsabile di tale funzione per l'intero gruppo, purché siano stabiliti canali informativi diretti tra esso e l'organo con funzione di gestione della capogruppo; in tale opzione, l'organo con funzione di gestione della capogruppo assume la responsabilità di seguire la pianificazione delle iniziative ICT, garantendone la rispondenza alle esigenze e alle strategie del gruppo.

Parte Prima – Recepimento in Italia della CRD IV

Titolo IV – Governo societario, controlli interni e gestione dei rischi

Capitolo 4 – Il sistema informativo

Sezione II – Governo, organizzazione e controlli del sistema informativo

decentrato sotto il controllo delle linee di *business* sono comunque inquadrati nel più generale disegno architeturale e agiscono nell’ambito di regole definite a livello aziendale;

- le responsabilità e gli assetti connessi con la pianificazione e il controllo del portafoglio dei progetti ICT, con il governo dell’evoluzione dell’architettura e dell’innovazione tecnologica nonché con le attività di gestione del sistema informativo (7);
- la realizzazione degli opportuni meccanismi di raccordo con le linee di *business*, con particolare riguardo alle attività di individuazione e pianificazione delle iniziative ICT (regolare rilevazione delle esigenze di servizi ICT e promozione delle opportunità tecnologiche offerte dall’evoluzione del sistema informativo).

4. La funzione di controllo dei rischi ICT e di sicurezza

Fermo restando quanto previsto dal Capitolo 3, Sezione III, par. 1, nell’ambito del sistema dei controlli interni le banche si dotano di una funzione di controllo di secondo livello responsabile della gestione e della supervisione dei rischi ICT e di sicurezza.

La funzione di controllo è responsabile del monitoraggio e del controllo dei rischi ICT e di sicurezza (8), nonché della verifica dell’aderenza delle operazioni ICT al sistema di gestione dei rischi ICT e di sicurezza (cfr. Sezione III). A tal fine, la funzione di controllo:

- concorre alla definizione della policy di sicurezza dell’informazione ed è informata su qualsiasi attività o evento che influenzi in modo rilevante il profilo di rischio della banca (9), incidenti operativi o di sicurezza significativi, nonché qualsiasi modifica sostanziale ai sistemi e ai processi ICT;
- è coinvolta attivamente nei progetti di modifica sostanziale del sistema informativo e, in particolare, nei processi di controllo dei rischi relativi a tali progetti.

Le banche possono attribuire i compiti della funzione di controllo dei rischi ICT e di sicurezza a una funzione di secondo livello appositamente istituita; alla funzione si applicano le disposizioni previste dal Capitolo 3, Sezione III, par. 1. Tra la funzione di controllo ICT e le altre funzioni aziendali di controllo sono assicurati opportuni livelli di raccordo e adeguate forme di coordinamento, conformemente a quanto previsto nel Capitolo 3, Sezione III, par. 3.5.

In alternativa, le banche possono assegnare tali compiti alle funzioni aziendali di controllo dei rischi e di *compliance*, in relazione ai ruoli, alle responsabilità e alle competenze proprie di ciascuna delle due funzioni, a condizione che siano assicurati il corretto svolgimento dei compiti, l’efficacia dei controlli e le necessarie competenze tecniche.

(7) Nel caso di *full outsourcing* della funzione ICT, al referente per l’attività esternalizzata è assegnata la responsabilità di seguire la pianificazione dei progetti informatici; la stessa figura garantisce, in collaborazione con il fornitore di servizi, la realizzazione degli opportuni meccanismi di raccordo con le linee di *business*.

(8) In particolare, la funzione di controllo assicura che i rischi ICT e di sicurezza siano individuati, misurati, valutati, gestiti, monitorati nonché riportati e mantenuti entro i limiti della propensione al rischio della banca.

(9) Con riferimento alla politica di sicurezza dell’informazione, cfr. Sezione IV.

Parte Prima – Recepimento in Italia della CRD IV

Titolo IV – Governo societario, controlli interni e gestione dei rischi

Capitolo 4 – Il sistema informativo

Sezione II – Governo, organizzazione e controlli del sistema informativo

5. Internal audit

L'*internal audit*, nell'ambito dei compiti e responsabilità previsti dal Capitolo 3, Sezione III, par. 3.4, dispone – al suo interno o mediante il ricorso a risorse esterne (10) – delle competenze specialistiche necessarie per assolvere ai propri compiti di *assurance* attinenti al sistema informativo aziendale (*ICT audit*), nonché alle attività e all'assetto organizzativo della banca afferente ai profili ICT, in coerenza con il principio di proporzionalità.

Il piano di *audit*, redatto secondo un approccio *risk-based*, è sottoposto all'approvazione dell'organo con funzione di supervisione strategica (11) e include le verifiche di *audit* riferite al sistema ICT e a ogni sua modifica significativa. La pianificazione degli interventi ispettivi assicura nel tempo un'adeguata copertura delle varie applicazioni, infrastrutture e processi di gestione, incluse le eventuali componenti esternalizzate (12).

A prescindere dalla forma adottata per gli accertamenti (ad es., *audit* mirati ovvero verifiche sulle applicazioni e componenti del sistema informativo nell'ambito di ispezioni su strutture organizzative o processi produttivi), la frequenza e il contenuto dei controlli tengono conto del complessivo profilo di rischio del processo o sistema oggetto di verifica, con particolare riguardo ai rischi di sicurezza.

L'*internal audit* è in grado di fornire valutazioni sui principali rischi tecnologici identificabili e sulla complessiva gestione del rischio ICT e di sicurezza dell'intermediario.

(10) Anche in caso di ricorso all'esterno, le risorse impegnate nell'*audit* mantengono l'indipendenza rispetto alle unità assoggettate al controllo.

(11) Cfr. Capitolo 3, Sezione II, par. 2 e Sezione III, par. 2 e 4.3.

(12) Tenuto conto del principio di proporzionalità, per le verifiche su componenti o servizi ICT esternalizzati, la funzione di *audit* dell'intermediario potrà scegliere, sotto la sua responsabilità, di fare affidamento sull'*internal audit* del fornitore di servizi, previa valutazione della sua professionalità e indipendenza.

SEZIONE III

LA GESTIONE DEL RISCHIO ICT E DI SICUREZZA

Il processo di gestione dei rischi ICT e di sicurezza è pienamente integrato e allineato con il processo di gestione dei rischi della banca (cfr. Capitolo 3, Sezione I, par. 6). Le banche assicurano che tutti i rischi ICT e di sicurezza assunti o assumibili siano individuati, analizzati, misurati, monitorati, gestiti, comunicati e mantenuti entro i limiti della propensione al rischio ICT e di sicurezza della banca. Esse assicurano inoltre la conformità dei sistemi e dei progetti ICT, nonché di tutte le attività svolte nell'ambito del sistema informativo, alle disposizioni di legge, regolamentari o statutarie e ai regolamenti e codici interni applicabili alla banca.

Nella gestione dei rischi ICT e di sicurezza le banche applicano le Sezioni 1.3.1 (paragrafi 13 e 14), 1.3.2, 1.3.3 e 1.3.4 degli Orientamenti dell'EBA sulla gestione dei rischi ICT e di sicurezza (1).

Ai fini dell'applicazione di questi Orientamenti si forniscono le seguenti specificazioni:

- il processo di analisi dei rischi ICT e di sicurezza è svolto con il concorso dell'utente responsabile (2), del personale della funzione ICT, della funzione di controllo responsabile della gestione e della supervisione dei rischi ICT e di sicurezza (cfr. Sez. II, par. 4) e, ove opportuno, della funzione di revisione interna, secondo metodologie e responsabilità formalmente definite dall'organo con funzione di gestione;
- l'analisi determina il rischio ICT e di sicurezza residuo da sottoporre ad accettazione formale dell'utente responsabile (3). Qualora il rischio residuo ecceda la propensione al rischio ICT e di sicurezza, approvata dall'organo con funzione di supervisione strategica (cfr. Sezione II, par. 2.1), l'analisi propone l'adozione di misure alternative o ulteriori di trattamento del rischio (4), definite con il coinvolgimento della funzione di controllo dei rischi ICT e sottoposte all'approvazione dell'organo con funzione di gestione;
- per le procedure in esercizio (5) per le quali siano stati individuati successivamente eventuali presidi in aggiunta a quelli già in essere, è adottato un piano di implementazione specifico. I tempi di attuazione del piano e i presidi compensativi di tipo organizzativo o procedurale nelle more dell'attuazione, sono documentati e sottoposti all'accettazione formale dell'utente responsabile. In ogni caso, l'aggiornamento delle misure di sicurezza che riguardano componenti critiche è effettuato senza indebiti ritardi.

(1) Si fa riferimento alla numerazione delle Sezioni nella versione italiana degli Orientamenti.

(2) Per le componenti e applicazioni critiche l'utente responsabile è individuato a un adeguato livello gerarchico. In caso di esternalizzazione del sistema, il referente per l'attività esternalizzata partecipa, in qualità di utente responsabile, all'analisi del rischio svolta dal fornitore di servizi, anche tramite "comitati utente"; nel caso di *full outsourcing* presso una società strumentale del gruppo di appartenenza, l'utente responsabile è collocato all'esterno della funzione ICT (ad es., presso la capogruppo, secondo un modello accentrato, o presso i singoli intermediari, nell'approccio decentrato).

(3) Nel documento approvato dall'utente responsabile, il rischio residuo è chiaramente espresso, perlomeno in termini qualitativi e con una descrizione non tecnica degli eventi dannosi che potrebbero comunque verificarsi in determinate circostanze.

(4) Ad esempio, si potrebbe ritenere di non abilitare funzioni o operazioni troppo rischiose (*risk avoidance*), ovvero di acquisire una polizza assicurativa (*risk transfer*).

(5) In sede di valutazione dei rischi su componenti del sistema informativo e applicazioni già in essere, la banca tiene conto dei dati disponibili in merito agli incidenti di sicurezza informatica verificatisi in passato.

DISPOSIZIONI DI VIGILANZA PER LE BANCHE

Parte Prima – Recepimento in Italia della CRD IV

Titolo IV – Governo societario, controlli interni e gestione dei rischi

Capitolo 4 – Il sistema informativo

Sezione IV – La gestione della sicurezza dell'informazione e delle operazioni ICT

SEZIONE IV

LA GESTIONE DELLA SICUREZZA DELL'INFORMAZIONE E DELLE OPERAZIONI ICT

Con riferimento alla gestione della sicurezza dell'informazione (*information security*) e alla gestione delle operazioni ICT (*ICT operations*), le banche applicano le Sezioni 1.4 e 1.5 degli Orientamenti dell'EBA sulla gestione dei rischi ICT e di sicurezza.

Fermo restando quanto previsto dalla Sezione 3.5.1 degli Orientamenti dell'EBA sulla gestione dei rischi ICT e di sicurezza (1), i gravi incidenti operativi o di sicurezza sono notificati tempestivamente alla Banca d'Italia, con l'invio di un rapporto sintetico recante una descrizione dell'incidente e dei disservizi provocati agli utenti interni e alla clientela, nonché degli altri dati e informazioni previsti dalle istruzioni emanate dalla Banca d'Italia (2).

(1) Si fa riferimento alla numerazione delle Sezioni nella versione italiana degli Orientamenti (pag. 17).

(2) Le istruzioni, che specificano anche le modalità e tempi della segnalazione, sono disponibili sul sito della Banca d'Italia all'indirizzo: <https://www.bancaditalia.it/compiti/vigilanza/incidenti-operativi/index.html>.

Parte Prima – Recepimento in Italia della CRD IV

Titolo IV – Governo societario, controlli interni e gestione dei rischi

Capitolo 4 – Il sistema informativo

Sezione IV bis – La gestione dei progetti e dei cambiamenti ICT

SEZIONE IV BIS

LA GESTIONE DEI PROGETTI E DEI CAMBIAMENTI ICT

Le banche si dotano di processi per la gestione dei progetti ICT nel corso del loro intero ciclo di vita, l'acquisizione e lo sviluppo e la manutenzione di servizi e sistemi ICT, nonché per la gestione dei cambiamenti di tali servizi e sistemi, secondo quanto previsto dalla Sezione 1.6 degli Orientamenti dell'EBA sulla gestione dei rischi ICT e di sicurezza.

Il processo per la gestione dei cambiamenti ICT si svolge sotto la responsabilità di una figura o struttura aziendale con elevato grado di indipendenza rispetto alla funzione di sviluppo e prevede, in modo proporzionato alla complessità e al profilo di rischio tecnologico dell'intermediario, l'autorizzazione formale di ogni cambiamento in ambiente di produzione (1); tale procedura comprende l'accettazione, nei casi critici individuati nell'analisi dei rischi, del nuovo rischio residuo.

Le iniziative di ampio impatto sul sistema ICT (ad esempio, modifiche rilevanti sulle componenti critiche, adeguamenti in conseguenza di fusioni o scissioni, migrazione ad altre piattaforme informatiche), che si inseriscono di norma in piani strategici all'attenzione dell'organo con funzione di supervisione strategica, sono preventivamente comunicate alla Banca centrale europea o alla Banca d'Italia.

(1) Il livello autorizzativo è adeguato all'entità dei rischi emersi nell'analisi.

DISPOSIZIONI DI VIGILANZA PER LE BANCHE

Parte Prima – Recepimento in Italia della CRD IV

Titolo IV – Governo societario, controlli interni e gestione dei rischi

Capitolo 4 – Il sistema informativo

Sezione V – Il sistema di gestione dei dati

registrando data, ora, autore e motivo dell'intervento, ambiente operativo interessato e i dati precedenti la modifica;

- i processi di acquisizione di dati da *information provider* esterni sono documentati e presidiati;
- i dati sono conservati con una granularità adeguata a consentire le diverse analisi e aggregazioni richieste dalle procedure di sfruttamento;
- i rapporti prodotti espongono le principali assunzioni e gli eventuali criteri di stima adottati (ad es., nell'ambito del monitoraggio dei rischi aziendali);
- il sistema di *reporting* consente di produrre informazioni tempestive e di qualità elevata per l'autorità di vigilanza e per il mercato.

SEZIONE VI

**L'ESTERNALIZZAZIONE DEL SISTEMA INFORMATIVO
E IL RICORSO A SOGGETTI TERZI PER LA PRESTAZIONE DI SERVIZI ICT**

1. Premessa

L'esternalizzazione delle risorse e servizi ICT può assumere diverse forme a seconda del modello architetturale e delle strategie di outsourcing adottate dall'intermediario: *outsourcing* verticale (relativo a determinati processi operativi), *outsourcing* orizzontale di servizi trasversali come la gestione degli apparati hardware (*facility management*), lo sviluppo e la gestione del parco applicativo (*application management*), i collegamenti di rete, l'*help desk* tecnico e gli interventi di riparazione e manutenzione delle risorse ICT, fino al *full outsourcing* del complessivo sistema informativo aziendale. Viene inoltre in rilievo il *cloud computing* (servizi *cloud*), un modello che consente l'accesso in rete diffuso, conveniente, flessibile e su richiesta, a un gruppo condiviso di risorse informatiche (ad esempio reti, server, memorie, applicazioni e servizi), che vengono rese disponibili rapidamente, con un minimo di attività gestionale o di interazione con il fornitore del servizio.

Le banche che ricorrono all'esternalizzazione del sistema informativo, sia in caso di *full outsourcing* sia di esternalizzazione di componenti critiche del sistema informativo, si attengono a quanto previsto in materia di *outsourcing* di funzioni aziendali nel Capitolo 3, Sezione IV. Le norme di cui al par. 2 declinano con specifico riferimento alle risorse e ai servizi ICT gli obblighi informativi previsti in via generale dagli Orientamenti dell'EBA in materia di esternalizzazione.

Nell'utilizzo di un modello di *cloud computing* (1) le banche definiscono i requisiti di sicurezza dei dati e dei sistemi nell'ambito dell'accordo di esternalizzazione e ne monitorano costantemente il rispetto; le banche inoltre adottano un approccio basato sul rischio con riferimento al luogo (paese e regione/località) dove sono conservati e trattati i dati e alla sicurezza delle informazioni.

2. Accordi con i fornitori e altri requisiti

Fermo restando quanto previsto al Capitolo 3, Sezione IV, con riferimento all'esternalizzazione del sistema informativo si precisa inoltre che:

- a. nell'accordo scritto tra la banca e i fornitori di sistemi e servizi ICT sono chiaramente definiti e formalizzati i seguenti aspetti:
 - i. le misure di attenuazione dei rischi del fornitore dei servizi, che devono essere conformi con il quadro di riferimento per la gestione del rischio della banca, con particolare riguardo a quello ICT e di sicurezza;
 - ii. misure idonee a garantire l'*accountability* e la ricostruibilità delle operazioni effettuate, almeno con riferimento alle operazioni critiche e agli accessi a dati personali o sensibili;

(1) Cfr. definizione di *cloud computing* al Capitolo 3, Sezione I, par. 3.

Parte Prima – Recepimento in Italia della CRD IV

Titolo IV – Governo societario, controlli interni e gestione dei rischi

Capitolo 4 – Il sistema informativo

Sezione VI – L'esternalizzazione del sistema informativo e il ricorso a soggetti terzi per la prestazione di servizi ICT

- iii. l'obbligo per il fornitore di servizi, una volta concluso il rapporto contrattuale e trascorso un periodo di tempo concordato, di eliminare – facendo uso di opportuni strumenti e soluzioni tecniche, debitamente documentati – qualsiasi copia o stralcio di dati personali o sensibili presente su propri sistemi o supporti in ragione dei servizi in precedenza esternalizzati dalla banca, in modo da escludere qualunque accesso successivo da parte del proprio personale o di terzi;
 - iv. la ripartizione dei compiti e delle responsabilità attinenti all'attuazione della politica di *Information Security* della banca;
 - v. il raccordo con i ruoli e le procedure dell'intermediario attinenti alla gestione del rischio ICT e di sicurezza (cfr. Sezione III) e per il sistema di gestione dei dati (cfr. Sezione V);
 - vi. le misure e gli obiettivi in materia di sicurezza dell'informazione, compresi i requisiti minimi di sicurezza informatica, che devono essere adeguati e proporzionati; le specifiche relative al ciclo di vita dei dati della banca ed eventuali requisiti relativi alla cifratura dei dati, alla sicurezza di rete e ai processi di monitoraggio della sicurezza, e l'ubicazione dei centri dati;
 - vii. le procedure di gestione degli incidenti operativi e di sicurezza, tra cui la notifica e l'attivazione dei livelli successivi di intervento;
- b. l'informativa alla Banca centrale europea o alla Banca d'Italia (cfr. Capitolo 3, Sezione IV, par. 2), sottoscritta dal legale rappresentante della banca, attesta la conformità dell'operazione alle disposizioni di vigilanza applicabili e include le informazioni di seguito indicate:
- i. i risultati della valutazione dei rischi dell'accordo di esternalizzazione condotta dalla banca secondo quanto previsto dalla Sezione 12.2 degli Orientamenti dell'EBA in materia di esternalizzazione;
 - ii. una descrizione delle strategie d'uscita (*exit strategies*), delle strategie di esternalizzazione della banca, del modello di riferimento per il sistema informativo come modificato dall'esternalizzazione e dei processi di funzionamento dei servizi esternalizzati, con particolare riguardo alle modalità con cui sono garantiti i requisiti di cui al presente Capitolo.

Nella relazione relativa ai controlli svolti sulle funzioni esternalizzate a fornitori di servizi al di fuori del gruppo (cfr. Capitolo 3, Sezione IV, par. 2) la banca dà conto, tra l'altro, delle iniziative di esternalizzazione del sistema informativo che sono state oggetto di informativa preventiva, nonché dei principali servizi ICT per i quali si fa ricorso a soggetti terzi e che non assumono la qualifica di esternalizzazione.

3. Il ricorso a soggetti terzi

Le banche che ricorrono a soggetti terzi per la prestazione di servizi ICT al di fuori di un rapporto di esternalizzazione applicano la Sezione 1.2.3 degli Orientamenti dell'EBA sulla gestione dei rischi ICT e di sicurezza.

Parte Prima – Recepimento in Italia della CRD IV

Titolo IV – Governo societario, controlli interni e gestione dei rischi

Capitolo 4 – Il sistema informativo

Sezione VII – Disposizioni specifiche in materia di prestazione di servizi di pagamento

SEZIONE VII

**DISPOSIZIONI SPECIFICHE
IN MATERIA DI PRESTAZIONE DI SERVIZI DI PAGAMENTO**

1. Sicurezza dei servizi di pagamento

Le banche che prestano servizi di pagamento applicano le disposizioni del presente Capitolo e del Capitolo 5 anche con riferimento ai rischi operativi e di sicurezza dei servizi di pagamento ai sensi della direttiva (UE) 2015/2366 (PSD2).

In materia di sicurezza dei servizi di pagamento, le banche:

- trasmettono alla Banca d'Italia, entro il 30 aprile di ogni anno, una relazione contenente una valutazione aggiornata e approfondita dei rischi operativi e di sicurezza relativi ai servizi di pagamento che esse prestano e dell'adeguatezza delle misure di mitigazione e dei meccanismi di controllo messi in atto per affrontarli (1);
- notificano senza indugio alla Banca d'Italia i gravi incidenti operativi o di sicurezza relativi ai servizi di pagamento prestati conformemente agli Orientamenti aggiornati dell'EBA in materia di segnalazione dei gravi incidenti ai sensi della PSD2 (2). Se l'incidente incide o potrebbe incidere sugli interessi finanziari dei propri utenti di servizi di pagamento, le banche informano altresì questi ultimi, senza indugio, dell'incidente e di tutte le misure a disposizione che possono adottare per attenuarne gli effetti negativi e trasmettono alla Banca d'Italia copia delle eventuali comunicazioni inviate (o che saranno inviate) alla clientela, non appena disponibili (3).

2. Gestione del rapporto con gli utenti dei servizi di pagamento

Nella gestione del rapporto con gli utenti dei servizi di pagamento, le banche applicano la Sezione 1.8 degli Orientamenti dell'EBA sulla gestione dei rischi ICT e di sicurezza.

(1) Le banche redigono la relazione in linea con quanto previsto nelle istruzioni dalla Banca d'Italia relative all'applicazione della direttiva PSD2 (cfr. https://www.bancaditalia.it/compiti/vigilanza/normativa/archivio-norme/circolari/c285/direttiva-psd2/Istruzioni_Procedure_BI_PSD2.pdf).

La relazione contiene anche la descrizione delle soluzioni eventualmente adottate sulla base dell'art. 17 del Regolamento delegato (UE) 2018/389 del 27 novembre 2017 in materia di processi e protocolli di pagamento sicuri per le imprese. Le relative informazioni, dovute soltanto alla prima occorrenza, sono trasmesse alla Banca d'Italia con apposito modulo disponibile al seguente indirizzo: https://www.bancaditalia.it/compiti/vigilanza/normativa/archivio-norme/circolari/c285/direttiva-psd2/Esenzione_dall_autenticazione_forte_del_cliente_per_i_pagamenti_corporate.pdf.

(2) Cfr. Comunicazione della Banca d'Italia del 29 ottobre 2021 relativa all'attuazione per i prestatori di servizi di pagamento degli Orientamenti aggiornati dell'EBA in materia di segnalazione dei gravi incidenti ai sensi della PSD2 (EBA/GL/2021/03).

<https://www.bancaditalia.it/compiti/vigilanza/normativa/archivio-norme/comunicazioni/com-20211029/index.html>.

Le segnalazioni dei gravi incidenti sono effettuate secondo le modalità indicate nelle istruzioni, emanate dalla Banca d'Italia, disponibili all'indirizzo: <https://www.bancaditalia.it/compiti/vigilanza/incidenti-operativi/index.html>.

(3) Cfr. Articolo 96, paragrafo 1, comma 2, della direttiva (UE) 2015/2366 del Parlamento europeo e del Consiglio del 25 novembre 2015 relativa ai servizi di pagamento nel mercato interno (PSD2).

Parte Prima – Recepimento in Italia della CRD IV

Titolo IV – Governo societario, controlli interni e gestione dei rischi

Capitolo 4 – Il sistema informativo

Sezione VII – Disposizioni specifiche in materia di prestazione di servizi di pagamento

3. Esenzione dall’obbligo di predisporre il meccanismo di emergenza di cui all’articolo 33(4) del Regolamento delegato (UE) 2018/389 della Commissione europea

Nel rispetto di quanto previsto dal Regolamento delegato (UE) 2018/389 della Commissione, le banche che prestano servizi di pagamento di radicamento di conti di pagamento che intendono richiedere l’esenzione dalla predisposizione del meccanismo di emergenza (“interfaccia di *fall-back*”) previsto dall’art. 33, par. 4, del Regolamento delegato si attengono a quanto previsto dagli Orientamenti dell’EBA sulle condizioni per beneficiare dell’esenzione dal meccanismo di emergenza a norma dell’articolo 33, paragrafo 6, del regolamento (UE) 2018/389 (EBA/GL/2018/07) (4).

(4) Cfr. <https://www.eba.europa.eu/regulation-and-policy/payment-services-and-electronic-money/guidelines-on-the-conditions-to-be-met-to-benefit-from-an-exemption-from-contingency-measures-under-article-33-6-of-regulation-eu-2018/389-rti-on-sca-csc-> .

DISPOSIZIONI DI VIGILANZA PER LE BANCHE

Parte Prima – Recepimento in Italia della CRD IV

Titolo IV – Governo societario, controlli interni e gestione dei rischi

Capitolo 4 – Il sistema informativo

Allegato A – Documenti aziendali per la gestione e il controllo del sistema informativo

Allegato A

**DOCUMENTI AZIENDALI
PER LA GESTIONE E IL CONTROLLO DEL SISTEMA INFORMATIVO**

Documento	Approvazione	Aggiornamento	Note
DOCUMENTI DI <i>POLICY</i> E STANDARD AZIENDALI			
Documento di indirizzo strategico	Organo con funzione di supervisione strategica	In dipendenza della periodicità dei piani strategici aziendali (3 – 5 anni)	Contiene (cfr. Sezione II, par. 1): <ul style="list-style-type: none"> – modello di riferimento architettuale – strategie di <i>sourcing</i> – propensione al rischio ICT e di sicurezza – linee di indirizzo in materia di selezione del personale con funzioni tecniche e di acquisizione di sistemi, <i>software</i> e servizi ICT
Metodologia di gestione del rischio ICT e di sicurezza	Organo con funzione di supervisione strategica	In base alla necessità (almeno annuale)	
<i>Policy</i> di sicurezza dell'informazione	Organo con funzione di supervisione strategica	In base alla necessità	
Organigramma della funzione ICT	Organo con funzione di supervisione strategica	In base alla necessità	
Standard di <i>data governance</i>	Organo con funzione di gestione	Periodicità definita	

**ALTRI DOCUMENTI ESSENZIALI
PER LA GESTIONE E LO SVILUPPO DEI SISTEMI ICT**

Piani d'azione per l'attuazione della strategia ICT	Organo con funzione di supervisione strategica	In base alla necessità	
Procedure e processi di gestione delle operazioni ICT	Organo con funzione di gestione	In base alla necessità	Include (cfr. Sezione II, par. 2.2):

DISPOSIZIONI DI VIGILANZA PER LE BANCHE

Parte Prima – Recepimento in Italia della CRD IV

Titolo IV – Governo societario, controlli interni e gestione dei rischi

Capitolo 4 – Il sistema informativo

Allegato A – Documenti aziendali per la gestione e il controllo del sistema informativo

Documento	Approvazione	Aggiornamento	Note
Piano operativo	Organo con funzione di gestione	Annuale	<ul style="list-style-type: none"> – procedura di gestione dei cambiamenti ICT – procedura di gestione degli incidenti
Piano di formazione e sensibilizzazione sulla sicurezza dell'informazione	Organo con funzione di gestione	Almeno annuale	
VALUTAZIONI AZIENDALI			
Rapporto sintetico su adeguatezza e costi dell'ICT	Organo con funzione di gestione	Almeno annuale	
Rapporto sintetico sulla situazione del rischio ICT e di sicurezza	Organo con funzione di gestione	Almeno annuale	
Relazione sulle risultanze dell'analisi dei rischi operativi e di sicurezza relativi ai servizi di pagamento	Organo con funzione di supervisione strategica	Annuale	
Rapporti dell' <i>internal audit</i> e delle altre funzioni responsabili della valutazione della sicurezza	Organo con funzione di supervisione strategica	Almeno annuale	

Parte Prima – Recepimento in Italia della CRD IV

Titolo IV – Governo societario, controlli interni e gestione dei rischi

Capitolo 5 – La continuità operativa

TITOLO IV

Capitolo 5

LA CONTINUITÀ OPERATIVA

TITOLO IV – Capitolo 5

LA CONTINUITÀ OPERATIVA

1. Destinatari

L'Allegato A, Sezione II (Requisiti per tutti gli operatori) si applica alle banche e ai gruppi bancari.

L'Allegato A, Sezione III (Requisiti particolari per i processi a rilevanza sistemica) si applica, in aggiunta ai requisiti previsti nella Sezione II dell'Allegato A, ai soggetti, individuati nominativamente, con apposita comunicazione, fra i gruppi bancari e le banche non appartenenti a gruppi con una quota di mercato, calcolata sul totale attivo, superiore al 5 per cento del totale del sistema bancario.

Nell'ambito dei gruppi bancari, i requisiti particolari si applicano alla capogruppo, alle singole controllate bancarie italiane con totale attivo superiore a 5 miliardi di euro e alle altre controllate bancarie, finanziarie e strumentali che, indipendentemente dalla dimensione e localizzazione, svolgono in misura rilevante i processi a rilevanza sistemica o danno un supporto essenziale a questi ultimi.

Possono essere altresì assoggettati ai requisiti particolari gli operatori, incluse le succursali italiane di banche estere, che, su base individuale, detengono una quota di mercato superiore al 5 per cento in almeno uno dei seguenti segmenti del sistema finanziario italiano: regolamento lordo in moneta di banca centrale, liquidazione di strumenti finanziari, servizi di controparte centrale, sistemi multilaterali di scambio di depositi interbancari in euro, aste BCE, operazioni di finanziamento del Tesoro effettuate tramite asta, mercato dei pronti contro termine all'ingrosso su titoli di Stato, pagamento delle pensioni sociali, bollettini postali.

2. Fonti normative

La materia è regolata dalle seguenti disposizioni del TUB:

- art. 51, il quale prevede che le banche inviino alla Banca d'Italia, con le modalità e i tempi da essa stabiliti, le segnalazioni periodiche nonché ogni dato e documento richiesti;
 - art. 53, comma 1, lett. d), che attribuisce alla Banca d'Italia il potere di emanare disposizioni di carattere generale in materia di organizzazione amministrativa e contabile e controlli interni delle banche;
 - art. 67, comma 1, lett. d), il quale prevede che, al fine di esercitare la vigilanza consolidata, la Banca d'Italia impartisca alla capogruppo, con provvedimenti di carattere generale, disposizioni concernenti il gruppo complessivamente considerato o i suoi componenti aventi ad oggetto l'organizzazione amministrativa e contabile e i controlli interni;
- e inoltre:
- dal decreto legislativo 27 gennaio 2010, n. 11, Attuazione della direttiva 2007/64/CE, relativa ai servizi di pagamento nel mercato interno, recante modifica delle direttive 97/7/CE,

Parte Prima – Recepimento in Italia della CRD IV

Titolo IV – Governo societario, controlli interni e gestione dei rischi

Capitolo 5 – La continuità operativa

2002/65/CE, 2005/60/CE, 2006/48/CE, e che abroga la direttiva 97/5/CE, e successive modifiche e integrazioni (d.lgs. n. 11/2010);

- del decreto legislativo 5 dicembre 2017, n. 218, Recepimento della direttiva (UE) 2015/2366 relativa ai servizi di pagamento nel mercato interno (PSD2), che modifica le direttive 2002/65/CE, 2009/110/CE e 2013/36/UE e il regolamento (UE) n. 1093/2010, e abroga la direttiva 2007/64/CE, nonché adeguamento delle disposizioni interne al regolamento (UE) n. 751/2015 relativo alle commissioni interbancarie sulle operazioni di pagamento basate su carta.

Vengono inoltre in rilievo:

- la direttiva CRD;
- la direttiva (UE) 2015/2366 del Parlamento europeo e del Consiglio del 25 novembre 2015 relativa ai servizi di pagamento nel mercato interno, che modifica le direttive 2002/65/CE, 2009/110/CE e 2013/36/UE e il regolamento (UE) n.1093/2010, e abroga la direttiva 2007/64/CE (PSD2);
- gli Orientamenti sulla governance interna (EBA/GL/2017/11), emanati dall'EBA il 21 marzo 2018;
- gli Orientamenti dell'EBA in materia di esternalizzazione (EBA/GL/2019/02), emanati dall'EBA il 25 febbraio 2019;
- gli Orientamenti sulla gestione dei rischi relativi alle tecnologie dell'informazione (*Information and Communication Technology*, ICT) e di sicurezza (EBA/GL/2019/04) emanati dall'EBA il 28 novembre 2019.

3. Banche soggette ai requisiti applicabili a tutti gli operatori (Allegato A, Sezione II)

Fermo restando quanto previsto nell'Allegato A, Sezione II, si precisa quanto segue:

- i gruppi bancari – coerentemente con quanto previsto nel Capitolo 3, Sezione V (il RAF e il sistema dei controlli interni nei gruppi bancari) – possono definire e gestire i piani di continuità operativa 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. A livello di gruppo sono stabiliti controlli sul raggiungimento degli obiettivi di continuità operativa definiti per l'intero gruppo e le singole componenti;
- i compiti e le responsabilità degli organi aziendali indicati ai punti a), b), c), d), ed e) dell'Allegato A, Sezione II, par. 3.1, rientrano nelle competenze dell'organo con funzione di supervisione strategica; i compiti e le responsabilità indicati nei punti f) e g) del menzionato paragrafo, spettano all'organo con funzione di gestione;
- le banche segnalano alla Banca d'Italia, tra le “cariche rilevanti a fini di Vigilanza” previste nella procedura “organi sociali” (Or.So.), il nome del responsabile del piano di continuità operativa (cfr. Allegato A, Sezione II, par.0);
- la procedura per la dichiarazione dello stato di crisi (cfr. Allegato A, Sezione II, par. 3.1) è definita in raccordo con il processo di gestione degli incidenti operativi o di sicurezza (cfr. Capitolo 4, Sezione IV) e delle altre tipologie di incidenti;

DISPOSIZIONI DI VIGILANZA PER LE BANCHE

Parte Prima – Recepimento in Italia della CRD IV

Titolo IV – Governo societario, controlli interni e gestione dei rischi

Capitolo 5 – La continuità operativa

- le verifiche annuali dei sistemi informativi (cfr. Allegato A, Sezione II, par. 3.5) prevedono anche l'operatività on-line di almeno una succursale;
- le previsioni in materia di esternalizzazione e ricorso a soggetti terzi, infrastrutture e controparti rilevanti (cfr. Allegato A, Sezione II, par. 3.7), si applicano coerentemente con quanto previsto dalle disposizioni in materia di esternalizzazione previste nel Capitolo 3 e dalle disposizioni in materia di esternalizzazione e ricorso a soggetti terzi per la prestazione di servizi ICT previste nel Capitolo 4;
- in caso di situazione di crisi che non assumano rilevanza sistemica per il sistema finanziario, le banche e i gruppi bancari contattano, al fine di agevolare il coordinamento degli interventi, la Banca d'Italia e la Banca centrale europea.

4. Banche soggette ai requisiti particolari per i processi a rilevanza sistemica (Allegato A, Sezione III)

Fermo restando quanto previsto nell'Allegato A, Sezione III, si precisa quanto segue:

- 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 da parte di tutte le controllate interessate dei requisiti previsti per i processi a rilevanza sistemica. Nomina un responsabile unico di tali attività, con competenze estese all'intero gruppo (cfr. Allegato A, Sezione III, par. 2.2);
- per le succursali italiane di intermediari esteri, 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.

Parte Prima – Recepimento in Italia della CRD IV

Titolo IV – Governo societario, controlli interni e gestione dei rischi

Capitolo 5 – La continuità operativa

Allegato A – Requisiti per la continuità operativa

Sezione I – Disposizioni di carattere generale

ALLEGATO A

REQUISITI PER LA CONTINUITÀ OPERATIVA

SEZIONE I

DISPOSIZIONI DI CARATTERE GENERALE

1. Premessa

La crescente complessità dell'attività finanziaria, l'intenso utilizzo della tecnologia dell'informazione e i nuovi scenari di rischio richiedono che gli operatori rafforzino l'impegno a garantire adeguati livelli di continuità operativa.

A tal fine, essi adottano un approccio esteso che, partendo dalla identificazione dei processi aziendali critici, definisca per ciascuno di essi presidi organizzativi e misure di continuità operativa commisurati ai livelli di rischio.

Le concrete misure da adottare tengono conto degli standard e *best practice* definiti a livello internazionale e/o definiti nell'ambito degli organismi di categoria.

2. Definizioni

- “*CODISE (continuità di servizio)*”: struttura per il coordinamento delle crisi operative della piazza finanziaria italiana presieduta dalla Banca d'Italia;
- “*crisi*”: situazione formalmente dichiarata di interruzione o deterioramento di uno o più processi critici o a rilevanza sistemica in seguito a incidenti o catastrofi;
- “*escalation*”: conduzione della gestione di un incidente caratterizzata da un aumento progressivo dei livelli aziendali coinvolti, fino a giungere, ove necessario, all'organo di amministrazione;
- “*emergenza*”: situazione originata da incidenti o catastrofi che colpiscono l'operatore, caratterizzata dalla necessità di adottare misure tecniche e gestionali eccezionali, finalizzate al tempestivo ripristino della normale operatività;
- “*gestione della continuità operativa*”: insieme delle iniziative volte a ridurre a un livello ritenuto accettabile i danni conseguenti a incidenti o catastrofi che colpiscono direttamente o indirettamente un operatore;
- “*piano di continuità operativa*”: documento che formalizza i principi, fissa gli obiettivi, descrive le procedure e individua le risorse, per la gestione della continuità operativa dei processi aziendali critici e a rilevanza sistemica. Esso è generalmente articolato in piani settoriali;
- “*piano di disaster recovery*”: documento che stabilisce le misure tecniche e organizzative per fronteggiare eventi che provochino la indisponibilità dei centri di elaborazione dati. Il piano di

DISPOSIZIONI DI VIGILANZA PER LE BANCHE

Parte Prima – Recepimento in Italia della CRD IV

Titolo IV – Governo societario, controlli interni e gestione dei rischi

Capitolo 5 – La continuità operativa

Allegato A – Requisiti per la continuità operativa

Sezione I – Disposizioni di carattere generale

disaster recovery, finalizzato a consentire il funzionamento delle procedure informatiche rilevanti in siti alternativi a quelli di produzione, costituisce parte integrante del piano di continuità operativa;

- “*punto di ripristino*”: istante di salvataggio dei dati fino al quale è garantita l’integrità degli stessi nei siti primari e alternativi;
- “*obiettivo di punto di ripristino*”: il periodo massimo durante il quale è accettabile che i dati vadano persi in caso di incidente;
- “*sito alternativo*”: infrastruttura che consente all’operatore di continuare a svolgere i propri processi critici e a rilevanza sistemica, anche in caso di incidenti o disastri che rendano indisponibile il sito primario;
- “*sito primario*”: infrastruttura presso la quale sono normalmente svolte le attività dell’operatore;
- “*tempo di ripristino di un processo*”: periodo che intercorre fra il momento in cui l’operatore dichiara lo stato crisi e l’istante in cui il processo è ripristinato a un livello di servizio predefinito. Esso è costituito dai tempi di:
 - analisi degli eventi e decisione delle azioni da intraprendere, prima di effettuare gli interventi;
 - ripartenza del processo, attraverso l’attuazione degli interventi tecnici e organizzativi e la successiva verifica sulla possibilità di rendere nuovamente disponibili i servizi senza danni e in condizioni di sicurezza.

Parte Prima – Recepimento in Italia della CRD IV

Titolo IV – Governo societario, controlli interni e gestione dei rischi

Capitolo 5 – La continuità operativa

Allegato A – Requisiti per la continuità operativa

Sezione II – Requisiti per tutti gli operatori

- interruzione del funzionamento delle infrastrutture (tra cui energia elettrica, reti di telecomunicazione, reti interbancarie, mercati finanziari);
- alterazione o perdita di dati e documenti critici.

Il piano di continuità operativa indica le procedure per il rientro dall'emergenza, con particolare attenzione alla rilevazione dei danni, alla gestione di tutte le operazioni di rientro, alla verifica dell'operatività per i servizi ripristinati.

2. Analisi di impatto

L'analisi di impatto (*Business Impact Analysis*, BIA), preliminare alla stesura del piano di continuità operativa e periodicamente aggiornata (3), individua il livello di rischio relativo ai singoli processi aziendali sulla base di un approccio quantitativo e qualitativo e pone in evidenza le conseguenze dell'interruzione del servizio (4). I rischi residui, non gestiti dal piano di continuità operativa, sono documentati ed esplicitamente accettati dagli organi aziendali competenti. 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*) e il livello di ricorso a soggetti terzi per la prestazione di servizi ICT;
- l'assetto organizzativo in termini di accentramento o decentramento di processi critici;
- i vincoli derivanti da interdipendenze, anche tra e con fornitori, clienti, altri operatori.

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

(3) L'analisi di impatto ed i conseguenti piani per la continuità operativa sono rivisti annualmente e aggiornati sulla base di quanto appreso dalle verifiche effettuate, dall'individuazione di nuovi rischi e minacce, nonché dai cambiamenti degli obiettivi e dalle priorità di ripristino.

(4) Le banche considerano il grado di criticità delle funzioni aziendali, dei processi di supporto, dei soggetti terzi e delle risorse informatiche individuate e classificate, nonché le loro interdipendenze, conformemente a quanto previsto dal Capitolo 4, Sezione III (cfr., in particolare, il rinvio alla Sezione 1.3.3, degli Orientamenti dell'EBA sulla gestione dei rischi ICT e di sicurezza).

Parte Prima – Recepimento in Italia della CRD IV

Titolo IV – Governo societario, controlli interni e gestione dei rischi

Capitolo 5 – La continuità operativa

Allegato A – Requisiti per la continuità operativa

Sezione II – Requisiti per tutti gli operatori

3. Definizione del piano di continuità operativa e gestione delle crisi

3.1 Ruolo degli organi aziendali

Il tema della continuità operativa è adeguatamente valutato a tutti i livelli di responsabilità. In tale ambito, l'organo di amministrazione:

- a) stabilisce gli obiettivi e le strategie di continuità operativa del servizio;
- b) assicura risorse umane, tecnologiche e finanziarie adeguate per il conseguimento degli obiettivi fissati;
- c) approva il piano di continuità operativa e le successive modifiche a seguito di adeguamenti tecnologici ed organizzativi, accettando i rischi residui non gestiti dal piano di continuità operativa;
- d) è informato, con frequenza almeno annuale, sugli esiti dei controlli sull'adeguatezza del piano nonché delle verifiche delle misure di continuità operativa;
- e) nomina il responsabile del piano di continuità operativa;
- f) promuove lo sviluppo, il controllo periodico del piano di continuità operativa e l'aggiornamento dello stesso a fronte di rilevanti innovazioni organizzative, tecnologiche e infrastrutturali nonché nel caso di lacune o carenze riscontrate ovvero di nuovi rischi sopravvenuti;
- g) approva il piano annuale delle verifiche delle misure di continuità operativa ed esamina i risultati delle prove documentati in forma scritta.

L'organo con funzione di controllo ha la responsabilità di vigilare sulla completezza, adeguatezza, funzionalità e affidabilità del piano di continuità operativa.

L'attività svolta e le decisioni assunte sono adeguatamente documentate.

3.2 I processi critici

Gli operatori identificano in modo circostanziato i processi relativi a funzioni aziendali di particolare rilevanza che, per l'impatto dei danni conseguenti alla loro indisponibilità, necessitano di elevati livelli di continuità operativa da conseguire mediante misure di prevenzione e con soluzioni di continuità operativa da attivare in caso di incidente.

A tal fine, sono 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, in accordo con gli indirizzi strategici e con le regole stabilite nel piano di continuità operativa, il tempo di ripristino del processo e l'obiettivo di punto di ripristino e collabora attivamente alla realizzazione delle misure di continuità operativa.

Parte Prima – Recepimento in Italia della CRD IV

Titolo IV – Governo societario, controlli interni e gestione dei rischi

Capitolo 5 – La continuità operativa

Allegato A – Requisiti per la continuità operativa

Sezione II – Requisiti per tutti gli operatori

3.3 La responsabilità del piano di continuità operativa

Il responsabile del piano di continuità operativa aziendale ha una posizione gerarchico – funzionale adeguata. Il responsabile cura lo sviluppo del piano di continuità operativa, ne assicura l’aggiornamento nel continuo, a fronte di cambiamenti organizzativi o tecnologici rilevanti, e ne verifica l’adeguatezza, con cadenza almeno annuale. Tale figura tiene inoltre i contatti con la Banca d’Italia e con la Banca centrale europea in caso di crisi.

Laddove il piano di continuità operativa sia articolato in piani settoriali, gli operatori individuano i referenti per ciascuno di essi. I referenti dei piani settoriali (5) coordinano, per gli aspetti di competenza, i lavori per la definizione e la manutenzione dei piani, per l’attuazione delle misure previste nello stesso e per la conduzione delle verifiche. Prima dell’attivazione di nuovi sistemi o processi operativi, essi definiscono le opportune modifiche dei piani.

3.4 Il contenuto del piano di continuità operativa

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

Il piano di continuità operativa attribuisce l’autorità di dichiarare lo stato di crisi e stabilisce la catena di comando incaricata di gestire l’azienda in circostanze eccezionali. Sono previste misure di *escalation* rapide che consentano, una volta assunta consapevolezza della portata dell’incidente, di dichiarare lo stato di crisi in tempi brevi.

I processi per la gestione degli incidenti e per la dichiarazione e gestione dello stato di crisi sono formalizzati e strettamente integrati fra loro. Anche a tal fine, sono esplicitamente individuati i membri della struttura preposta alla gestione della crisi (ad es., comitato di crisi), il responsabile della stessa struttura, la catena di comando, le modalità interne di comunicazione e le responsabilità attribuite alle funzioni aziendali interessate.

Il piano di continuità operativa stabilisce i tempi di ripristino e gli obiettivi di punto di ripristino dei processi critici (6).

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

Il piano di continuità operativa considera anche opzioni alternative nel caso in cui il ripristino non sia attuabile nel breve periodo a causa di costi, rischi, fattori logistici o circostanze impreviste.

(5) Ove il piano di continuità operativa non sia articolato in piani settoriali, tali attività sono svolte dal responsabile del piano di continuità operativa.

(6) Per i profili ICT, il piano di continuità operativa stabilisce, in particolare, il ripristino dell’operatività delle funzioni aziendali critiche, dei processi di supporto e delle risorse informatiche e tiene conto delle loro interdipendenze. Nei casi di gravi interruzioni dell’operatività che attivano specifici piani di continuità operativa, i piani definiscono la priorità delle azioni di continuità operativa secondo un approccio basato sul rischio, che può a sua volta tenere conto delle valutazioni dei rischi effettuate ai sensi del Capitolo 4. Con riguardo alla prestazione di servizi di pagamento ciò può comprendere, ad esempio, facilitare il successivo trattamento delle transazioni critiche mentre proseguono le azioni correttive.

Parte Prima – Recepimento in Italia della CRD IV

Titolo IV – Governo societario, controlli interni e gestione dei rischi

Capitolo 5 – La continuità operativa

Allegato A – Requisiti per la continuità operativa

Sezione II – Requisiti per tutti gli operatori

Con riferimento ai sistemi informativi centrali e periferici, il piano di continuità operativa integra il piano di *disaster recovery* (7). In quest'ultimo sono fornite indicazioni su modalità e frequenza di generazione delle copie degli archivi di produzione, nonché sulle procedure per il ripristino presso i siti alternativi.

La frequenza dei *back-up* è correlata alle dimensioni e alle funzioni (8) dell'operatore; gli archivi di produzione dei processi critici sono duplicati almeno giornalmente. Sono assunte cautele per il tempestivo trasporto e la conservazione delle copie elettroniche in siti a elevata sicurezza fisica posti in luoghi remoti rispetto ai sistemi di produzione (9).

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

I siti alternativi possono dover essere utilizzati, in caso di necessità, anche per periodi prolungati.

3.5 Le verifiche

Gli intermediari sottopongono periodicamente a verifica i propri piani per la continuità operativa delle funzioni, dei servizi, dei sistemi, delle transazioni e delle interdipendenze riferite ai processi critici.

Le modalità di verifica delle misure di continuità operativa dipendono dalla criticità dei processi e dai rischi ravvisati; di conseguenza sono ipotizzabili differenti frequenze e livelli di dettaglio delle prove. In alcuni casi può essere sufficiente la simulazione parziale dell'incidente o della catastrofe che può causare la crisi.

Con frequenza almeno annuale sono svolte verifiche complessive del ripristino della operatività delle funzioni, dei servizi, dei sistemi, delle transazioni e delle interdipendenze riferite ai processi critici, basate su scenari il più possibile realistici, con l'obiettivo di riscontrare la capacità della banca di sostenere la *viability* delle proprie attività fino a quando le operazioni critiche non sono ristabilite e dell'organizzazione di attuare nei tempi previsti le misure definite nel piano di continuità operativa. Queste verifiche prevedono il coinvolgimento degli utenti finali, dei fornitori di servizi e, qualora possibile, delle controparti rilevanti.

In particolare, le verifiche annuali dei sistemi informativi prevedono l'attivazione dei collegamenti di rete presso il sito alternativo e l'esecuzione delle procedure *batch* con controllo della funzionalità e delle prestazioni dei siti alternativi. Le prove sono preferibilmente realizzate con dati di produzione.

I risultati delle verifiche sono documentati per iscritto, portati all'attenzione degli organi aziendali competenti 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.

(7) In caso di outsourcing di componenti critiche del sistema informativo si applica quanto indicato al par. 3.7.

(8) Ad esempio, nel caso in cui svolga il ruolo di tramite per partecipanti indiretti.

(9) Per i processi non critici sono comunque realizzati meccanismi per acquisire e gestire regolarmente copie di riserva dei dati e del software, al fine di assicurare l'integrità e la disponibilità delle informazioni. Per i siti alternativi *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 per l'allineamento con i sistemi di produzione dopo il loro ripristino.

Parte Prima – Recepimento in Italia della CRD IV

Titolo IV – Governo societario, controlli interni e gestione dei rischi

Capitolo 5 – La continuità operativa

Allegato A – Requisiti per la continuità operativa

Sezione II – Requisiti per tutti gli operatori

3.6 Le risorse umane

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

Le procedure di continuità operativa sono chiare e dettagliate, in modo da poter essere eseguite anche da risorse non impegnate nell'ordinaria attività nei processi cui si riferiscono.

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

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.

3.7 Ricorso a soggetti esterni per la prestazione di servizi ICT, esternalizzazione, infrastrutture e controparti rilevanti

In caso di ricorso a soggetti esterni per la prestazione di servizi ICT e di esternalizzazione di funzioni aziendali connesse allo svolgimento di processi critici, il piano di continuità operativa prevede le misure da attuare in caso di crisi con impatto rilevante sull'operatore, sul soggetto terzo o sul fornitore di servizi esternalizzati.

Nel contratto sono formalizzati i livelli di servizio assicurati in caso di crisi e le soluzioni di continuità operativa poste in atto dal soggetto terzo o dal fornitore di servizi esternalizzati, adeguati al conseguimento degli obiettivi aziendali e coerenti con le prescrizioni della Banca d'Italia. Sono altresì stabilite le modalità di partecipazione, diretta o per il tramite di comitati utente, alle verifiche dei piani di continuità operativa dei fornitori.

L'operatore acquisisce i piani di continuità operativa del soggetto terzo o del fornitore di servizi esternalizzati o dispone di informazioni adeguate, al fine di valutare la qualità delle misure previste e di integrarle con le soluzioni di continuità operativa realizzate all'interno. Il soggetto terzo o il fornitore di servizi esternalizzati comunica tempestivamente all'operatore il verificarsi di incidenti al fine di consentire la pronta attivazione delle relative procedure di continuità operativa.

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

Per i servizi essenziali dell'operatore, va valutata la possibilità di prevedere il ricorso, in casi di emergenza, a fornitori alternativi.

Nel caso in cui il soggetto terzo o il fornitore di servizi esternalizzati 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.

Parte Prima – Recepimento in Italia della CRD IV

Titolo IV – Governo societario, controlli interni e gestione dei rischi

Capitolo 5 – La continuità operativa

Allegato A – Requisiti per la continuità operativa

Sezione II – Requisiti per tutti gli operatori

3.8 Controlli

Il piano di continuità operativa e il relativo processo di aggiornamento sono oggetto di regolare verifica da parte della funzione di revisione interna. L'*internal audit* prende visione dei programmi di verifica, assiste alle prove e ne controlla i risultati, proponendo modifiche al piano di continuità operativa sulla base delle mancanze riscontrate.

In tale ambito, particolare attenzione è posta all'analisi dei criteri di *escalation*. In caso di incidenti, la funzione di *audit* verifica la congruità dei tempi rilevati per la dichiarazione dello stato di crisi. La funzione di revisione interna è anche coinvolta nel controllo dei piani di continuità operativa dei fornitori di servizi esternalizzati e dei soggetti terzi critici; essa può decidere di fare affidamento sulle strutture di questi ultimi se ritenute professionali, indipendenti e trasparenti quanto ai risultati dei controlli. L'*internal audit* esamina i contratti per accertare che il livello di tutela sia adeguato agli obiettivi e agli standard aziendali.

Gli operatori considerano l'opportunità di sottoporre il piano di continuità operativa alla revisione da parte di competenti terze parti indipendenti.

3.9 Comunicazioni alla Banca d'Italia e alla Banca centrale europea

In caso di crisi, successivamente al ripristino dei processi critici, l'operatore fornisce alla Banca d'Italia e alla Banca centrale europea valutazioni circa l'impatto dell'evento sulla operatività delle strutture centrali e periferiche e sui rapporti con la clientela e le controparti.

Parte Prima – Recepimento in Italia della CRD IV

Titolo IV – Governo societario, controlli interni e gestione dei rischi

Capitolo 5 – La continuità operativa

Allegato A – Requisiti per la continuità operativa

Sezione III – Requisiti particolari per i processi a rilevanza sistemica

SEZIONE III

REQUISITI PARTICOLARI PER I PROCESSI A RILEVANZA SISTEMICA

1. Premessa

L'operatività del sistema finanziario nel suo complesso si basa sul corretto funzionamento dei maggiori operatori e sulla loro capacità 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 operatori, in particolare con riferimento ai tempi di ripristino per i processi a rilevanza sistemica (cfr. par. 2.1), alla localizzazione dei siti alternativi, alle risorse previste per gestire le situazioni di crisi.

La Banca d'Italia individua nominativamente gli operatori ai quali si applicano i requisiti particolari, richiede adeguamenti dei piani di continuità operativa, verifica le soluzioni adottate. Tali operatori partecipano alle iniziative per il coordinamento della continuità operativa del sistema finanziario del CODISE.

2. Definizione del piano di continuità operativa e gestione delle crisi

2.1 Processi a rilevanza sistemica

I processi ad alta criticità nel sistema finanziario italiano che, per un effetto di contagio, 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 sono denominati, ai fini delle presenti disposizioni, "processi a rilevanza sistemica" per la continuità operativa del sistema finanziario italiano. La Banca d'Italia comunica a ciascun operatore i processi a rilevanza sistemica di pertinenza. 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: regolamento lordo in moneta di banca centrale (Target 2), liquidazione di strumenti finanziari (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: sistemi multilaterali di scambio di depositi interbancari in euro (e-Mid), aste BCE, operazioni di finanziamento del Tesoro effettuate tramite asta, Mercato dei pronti contro termine all'ingrosso su titoli di Stato (MTS comparto PCT);
- 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

Parte Prima – Recepimento in Italia della CRD IV

Titolo IV – Governo societario, controlli interni e gestione dei rischi

Capitolo 5 – La continuità operativa

Allegato A – Requisiti per la continuità operativa

Sezione III – Requisiti particolari per i processi a rilevanza sistemica

stessi. Sono inclusi: gestione delle infrastrutture telematiche per l'erogazione del contante tramite terminale ATM, supporto ad applicazioni e servizi rientranti nell'ambito della "Convenzione per la partecipazione al Sistema per la trasmissione telematica di dati" (SITRAD).

2.2 Responsabilità

L'operatore:

- attua gli interventi di adeguamento dei piani di continuità operativa relativi ai processi a rilevanza sistemica;
- garantisce nel continuo il rispetto dei requisiti particolari;
- nomina un responsabile unico di tali attività.

2.3 Scenari di rischio

Gli scenari di rischio rilevanti per la continuità operativa dei processi a rilevanza sistemica sono documentati e costantemente aggiornati. Essi includono, in aggiunta a quanto previsto per tutti gli operatori: eventi catastrofici con distruzioni fisiche su larga scala, a dimensione metropolitana o superiore, che investano infrastrutture essenziali dell'operatore e di soggetti terzi; situazioni di crisi gravi anche non connesse ad eventi con distruzioni materiali (ad es., pandemie, attacchi biologici, attacchi informatici su larga scala).

2.4 Siti alternativi

I siti alternativi per i 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 alternativi 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 alternativi è trascurabile.

I siti alternativi 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.

2.5 Tempi di ripristino e percentuali di disponibilità

Il tempo di ripristino per i processi a rilevanza sistemica non supera le quattro ore. Il tempo di ripartenza per i processi a rilevanza sistemica non supera le due ore.

Se un evento catastrofico che colpisce un operatore determina un blocco dei processi a rilevanza sistemica di altri operatori, questi ultimi ripristinano i propri processi sistemici entro due ore dalla ripartenza dell'operatore colpito in prima istanza.

Parte Prima – Recepimento in Italia della CRD IV

Titolo IV – Governo societario, controlli interni e gestione dei rischi

Capitolo 5 – La continuità operativa

Allegato A – Requisiti per la continuità operativa

Sezione III – Requisiti particolari per i processi a rilevanza sistemica

Nel caso in cui gli scenari (cfr. par. 2.3) determinino impatti particolarmente gravi, gli obiettivi di ripristino indicati possono subire un adattamento che sarà segnalato agli operatori interessati dalla Banca d'Italia, tenuto conto delle indicazioni condivise nel CODISE.

Con riferimento ai sistemi informativi, sono considerate adeguate le soluzioni basate su architetture tecnologiche che effettuino la duplicazione in linea dei dati operativi in modo da eliminare o ridurre al minimo la perdita di informazioni. A tal fine l'intervallo di tempo che intercorre fra il punto di ripristino e il momento dell'incidente è pari o prossimo a zero.

È previsto, anche in caso di situazioni estreme, un ripristino quanto più possibile immediato dei processi a rilevanza sistemica, anche facendo ricorso a procedure a bassa integrazione nei processi aziendali, purché presidiate dal punto di vista della sicurezza (ad es., mediante l'utilizzo di PC *off-line*, fax, contatti telefonici con controparti selezionate), in particolare per gestire le esigenze essenziali di liquidità.

2.6 Risorse

Il piano di continuità operativa individua 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 alternativi, 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.

2.7 Verifiche

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

3. Comunicazioni alla Banca d'Italia e alla Banca centrale europea

In caso di incidenti che possano avere impatti rilevanti sui processi a rilevanza sistemica, la dichiarazione dello stato di crisi prevede l'immediata richiesta di attivazione del CODISE con una prima valutazione degli operatori potenzialmente danneggiati.

In caso di crisi, successivamente al ripristino dei processi a rilevanza sistemica, l'operatore fornisce con tempestività alla Banca d'Italia e alla Banca centrale europea valutazioni circa l'impatto dell'evento sulla operatività delle strutture centrali e periferiche e sui rapporti con la clientela e le controparti.

Gli operatori sistemici inviano alla Banca d'Italia e alla Banca centrale europea un'informativa annuale sulle principali caratteristiche del piano di continuità operativa, sugli adeguamenti e integrazioni intervenuti in corso d'anno, sulle verifiche da parte dell'*internal audit*, sui principali incidenti e sulle criticità ricorrenti.