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

Firmato digitalmente da

MARANGONI
MARIO

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 "Governo 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**. Modificati 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).

INDICE

Indice

Indice

TITOLO IV

Capitolo 4

IL SISTEMA INFORMATIVO

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 - e delle risorse umane dedicate alla loro amministrazione) 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, 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 e complessità operative, della natura dell'attività svolta, della tipologia dei servizi prestati nonché del livello di automazione dei processi e servizi della banca.

A tal proposito, le banche valutano l'opportunità di avvalersi degli standard e *best practices* 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 tramite il canale internet (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:

— dalla delibera del CICR del 2 agosto 1996, come modificata dalla delibera del 23 marzo 2004, in materia di organizzazione amministrativa e contabile e controlli interni delle banche e dei gruppi bancari;

— dal decreto del Ministro dell'Economia e delle finanze, Presidente del CICR del 5 agosto 2004 in materia, tra l'altro, di compiti e poteri degli organi sociali delle banche e dei gruppi bancari;

— dagli Orientamenti finali sulla sicurezza dei pagamenti via Internet, emanati dall'ABE il 19 dicembre 2014 ([1]).

Viene altresì in rilievo la CRD IV.

Si è anche tenuto conto del documento *Principles for effective risk data aggregation and risk reporting*, pubblicato dal Comitato di Basilea per la vigilanza bancaria nel gennaio 2013 (2).

([1]) https://www.eba.europa.eu/documents/10180/1004450/EBA_2015_IT+Guidelines+on+Internet+Payments.pdf/b9c5dee9-78bd-47c5-a80c-4d2f3f8a1de2

(2) http://www.bis.org/publ/bcbs239.pdf.

3. Definizioni

Ai fini della presente disciplina si definisce:

— "*accountability*": l'assegnazione della responsabilità di un'attività o processo aziendale, con il conseguente compito di rispondere delle operazioni svolte e dei risultati conseguiti, a una determinata figura aziendale; in ambito tecnico, si intende la garanzia di poter attribuire ciascuna operazione a soggetti (utenti o applicazioni) univocamente identificabili;

— "*autenticazione*": la procedura di verifica dell'identità di un utente da parte di un sistema o servizio;

— "*autorizzazione*": la procedura che verifica se un cliente o un altro soggetto interno o esterno ha il diritto di compiere una certa azione, ad es. di trasferire fondi o accedere a dati sensibili;

— "*componente critica del sistema informativo*": il sistema o l'applicazione per i quali un incidente di sicurezza informatica può pregiudicare il regolare e sicuro svolgimento di funzioni operative importanti (cfr. Capitolo 3, par. 3) per l'intermediario, tra cui l'efficace espletamento dei compiti degli organi aziendali e delle funzioni di controllo; l'analisi dei rischi definisce le funzioni aziendali e le componenti del sistema informativo che presentano rischi rilevanti per la banca;

— "*credenziali*": le informazioni – generalmente riservate – utilizzate da un utente a fini di autenticazione ad un sistema o servizio. Sono inclusi nella definizione gli strumenti fisici che forniscono o memorizzano le informazioni (ad es., generatori di *password* non riutilizzabili, *smart card*) o qualcosa che l'utente ricorda (ad es., password) o rappresenta (ad es., caratteristiche biometriche);

— "*incidente di sicurezza informatica*": ogni evento che implica la violazione o l'imminente minaccia di violazione delle norme e delle prassi aziendali in materia di sicurezza delle informazioni (ad es., frodi informatiche, attacchi attraverso internet e malfunzionamenti e disservizi);

— "*grave incidente di sicurezza informatica*": un incidente di sicurezza informatica da cui derivi almeno una delle seguenti conseguenze:

  a. perdite economiche elevate o prolungati disservizi per l'intermediario, anche a seguito di ripetuti incidenti di minore entità;

  b. disservizi rilevanti sulla clientela e altri soggetti (ad es., intermediari o infrastrutture di pagamento); la valutazione della gravità considera il numero dei clienti o controparti potenzialmente coinvolti e l'ammontare a rischio;

  c. il rischio di inficiare la capacità della banca di conformarsi alle condizioni e agli obblighi di legge o previsti dalla disciplina di vigilanza;

— "*minimo privilegio* (*least privilege*)": il principio che stabilisce che a ciascun utente o amministratore di sistema siano assegnate le abilitazioni strettamente necessarie allo svolgimento dei compiti assegnati;

— "*no single point of failure*": il principio architetturale 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 operative 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 fallback*": 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;

— "*rischio informatico* (*o ICT*)": il rischio di incorrere in perdite economiche, di reputazione e di quote di mercato in relazione all'utilizzo di tecnologia dell'informazione e della comunicazione (*Information and Communication Technology* – ICT). 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 informatico residuo*": il rischio informatico a cui l'intermediario è esposto una volta applicate le misure di attenuazione individuate nel processo di analisi dei rischi;

— "*risorsa informatica* (*o ICT*)": un bene dell'azienda afferente all'ICT che concorre alla ricezione, archiviazione, elaborazione, trasmissione e fruizione dell'informazione gestita dall'intermediario;

— "*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;

— "*utente responsabile*": la figura aziendale identificata per ciascun sistema o applicazione e che ne assume formalmente la responsabilità, in rappresentanza degli utenti e nei rapporti con le funzioni preposte allo sviluppo e alla gestione tecnica;

— "*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.

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 (3); queste

(3) Alle banche che prestano attività e servizi di investimento si applicano anche le disposizioni contenute nel Regolamento della Banca d'Italia e della Consob del 29 ottobre 2007, come successivamente modificato e integrato, in materia di organizzazione e procedure degli intermediari che prestano servizi di investimento o di gestione collettiva del risparmio.

ultime si attengono esclusivamente a quanto previsto dalla Sezione VII, par. 1, con riferimento alla prestazione di servizi di pagamento tramite internet;

— alle capogruppo di gruppi bancari;

— alle imprese di riferimento, secondo quanto previsto dalla Sezione VI del Capitolo 3.

SEZIONE II

GOVERNO E ORGANIZZAZIONE 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, nel rispetto del principio della separazione delle funzioni di controllo da quelle di supervisione e gestione.

2. 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:

— approva le strategie di sviluppo del sistema informativo, in considerazione dell'evoluzione del settore di riferimento e in coerenza con l'articolazione in essere e a tendere dei settori di operatività, dei processi e dell'organizzazione aziendale; in tale contesto approva il modello di riferimento per l'architettura del sistema informativo;

— approva la *policy* di sicurezza informatica (1);

— approva le linee di indirizzo in materia di selezione del personale con funzioni tecniche e di acquisizione di sistemi, software e servizi, incluso il ricorso a fornitori esterni (cfr. Sezione VI);

— promuove lo sviluppo, la condivisione e l'aggiornamento di conoscenze in materia di ICT all'interno dell'azienda;

— è informato 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; è informato tempestivamente in caso di gravi problemi per l'attività aziendale derivanti da incidenti e malfunzionamenti del sistema informativo.

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

— approva il quadro di riferimento organizzativo e metodologico per l'analisi del rischio informatico, 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);

(1) 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 analoga documentazione prodotta dal fornitore.

— approva la propensione al rischio informatico, 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 con cadenza almeno annuale sulla situazione di rischio informatico rispetto alla propensione al rischio.

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.

3. 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 la struttura organizzativa della funzione ICT (ove presente) (2) assicurandone nel tempo la rispondenza alle strategie e ai modelli architetturali definiti dall'organo con funzione di supervisione strategica; garantisce il corretto dimensionamento quali-quantitativo delle risorse umane;

— definisce l'assetto organizzativo, metodologico e procedurale per il processo di analisi del rischio informatico, perseguendo un opportuno livello di raccordo con la funzione di *risk management* per i processi di stima del rischio operativo;

— tranne che nel caso di *full outsourcing*, approva il disegno dei processi di gestione del sistema informativo, garantendo l'efficacia ed efficienza dell'impianto nonché la complessiva completezza e coerenza, con particolare riguardo ad 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 misurazione delle prestazioni (3), assumendo gli opportuni interventi e iniziative di miglioramento;

(2) 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.

(3) 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*).

— 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 informatico 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 di sicurezza informatica (cfr. Sezione IV) e fornisce informazioni all'organo con funzione di supervisione strategica in caso di gravi problemi per l'attività aziendale derivanti da incidenti e malfunzionamenti.

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.

4. Organizzazione della funzione ICT

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 (4) a garanzia dell'unitarietà della visione gestionale e del rischio informatico nonché dell'uniformità di applicazione delle norme riguardanti il sistema informativo; eventuali unità di sviluppo decentrato sotto il controllo delle linee di *business* sono comunque inquadrate nel più generale disegno architetturale 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 informatici, con il governo dell'evoluzione dell'architettura e dell'innovazione tecnologica nonché con le attività di gestione del sistema informativo (5);

— la realizzazione degli opportuni meccanismi di raccordo con le linee di *business*, con particolare riguardo alle attività di individuazione e pianificazione delle iniziative

(4) 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.

(5) Nel caso di *full outsourcing* della funzione ICT, al "referente per l'attività esternalizzata" (cfr. Capitolo 3, Sezione IV, par. 1) 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*.

informatiche (regolare rilevazione delle esigenze di servizi informatici e promozione delle opportunità tecnologiche offerte dall'evoluzione del sistema informativo).

5. La sicurezza informatica

La funzione di sicurezza informatica è deputata allo svolgimento dei compiti specialistici in materia di sicurezza delle risorse ICT. In particolare:

— segue la redazione e l'aggiornamento delle *policy* di sicurezza e delle istruzioni operative;

— assicura la coerenza dei presidi di sicurezza con le *policy* approvate;

— partecipa alla progettazione, realizzazione e manutenzione dei presidi di sicurezza dei *data center*;

— partecipa alla valutazione del rischio potenziale nonché all'individuazione dei presidi di sicurezza nell'ambito del processo di analisi del rischio informatico (cfr. Sezione III);

— assicura il monitoraggio nel continuo delle minacce applicabili alle diverse risorse informatiche (cfr. Sezione IV, par. 3);

— segue lo svolgimento dei test di sicurezza prima dell'avvio in produzione di un sistema nuovo o modificato (cfr. Sezione IV, par. 5).

Nelle realtà più complesse, l'indipendenza di giudizio rispetto alle funzioni operative è assicurata da un'adeguata collocazione organizzativa.

6. Il controllo del rischio informatico e la *compliance* ICT

Nell'ambito del sistema dei controlli interni sono chiaramente assegnate responsabilità in merito allo svolgimento dei seguenti compiti di controllo di secondo livello:

— il controllo dei rischi, basato su flussi informativi continui in merito all'evoluzione del rischio informatico e sul monitoraggio dell'efficacia delle misure di protezione delle risorse ICT. La gestione del complessivo rischio informatico si raccorda con il processo di analisi sulle singole risorse ICT (cfr. Sezione III). Le valutazioni svolte sono documentate e riviste in rapporto ai risultati del monitoraggio e comunque almeno una volta l'anno.

  Con riferimento alle banche con un modello interno validato sul rischio operativo, i dati sulle perdite operative in ambito ICT sono integrati con i dati e gli scenari relativi alle altre funzioni aziendali, e ne sono presidiati la qualità e completezza;

— il rispetto dei regolamenti interni e delle normative esterne in tema di ICT (ICT *compliance*) garantendo, tra l'altro:

  - l'assistenza su aspetti tecnici in caso di questioni legali relative al trattamento dei dati personali;
  - la coerenza degli assetti organizzativi alle normative esterne, per le parti relative al sistema informativo;

- l'analisi di conformità dei contratti di *outsourcing* e con fornitori (inclusi i contratti infra-gruppo).

7. Compiti della funzione di revisione interna

L'internal audit dispone - al suo interno o mediante il ricorso a risorse esterne (6) - delle competenze specialistiche necessarie per assolvere ai propri compiti di *assurance* attinenti al sistema informativo aziendale (ICT *audit*).

La pianificazione degli interventi ispettivi assicura nel tempo un'adeguata copertura delle varie applicazioni, infrastrutture e processi di gestione, incluse le eventuali componenti esternalizzate (7). 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), l'*internal audit* è in grado di fornire valutazioni sui principali rischi tecnologici identificabili e sulla complessiva gestione del rischio informatico dell'intermediario.

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

(7) 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

L'ANALISI DEL RISCHIO INFORMATICO

L'analisi del rischio informatico costituisce uno strumento a garanzia dell'efficacia ed efficienza delle misure di protezione delle risorse ICT, permettendo di graduare le misure di mitigazione nei vari ambienti in funzione del profilo di rischio dell'intermediario.

Il processo di analisi è svolto con il concorso dell'utente responsabile (1), del personale della funzione ICT, delle funzioni di controllo dei rischi, di sicurezza informatica e, ove opportuno, dell'*audit*, secondo metodologie e responsabilità formalmente definite dall'organo con funzione di gestione. Esso si compone delle seguenti fasi:

— la valutazione del rischio potenziale cui sono esposte le risorse informatiche esaminate; tale attività interessa tutte le iniziative di sviluppo di nuovi progetti e di modifica rilevante del sistema informativo (2).

  Tale fase prende l'avvio con la classificazione delle risorse ICT (3) in termini di rischio informatico (4);

— il trattamento del rischio, volto a individuare, se necessario, misure di attenuazione – di tipo tecnico o organizzativo – idonee a contenere il rischio potenziale.

  L'analisi determina il rischio residuo da sottoporre ad accettazione formale dell'utente responsabile (5). Qualora il rischio residuo ecceda la propensione al rischio informatico, approvato dall'organo con funzione di supervisione strategica (cfr. Sezione II, par. 2), l'analisi propone l'adozione di misure alternative o ulteriori di trattamento del rischio (6), definite con il coinvolgimento della funzione di controllo dei rischi e sottoposte all'approvazione dell'organo con funzione di gestione.

Per le procedure in esercizio, per le quali non è stata svolta un'analisi del rischio in fase di sviluppo, è comunque prevista una valutazione integrativa, al fine di individuare eventuali presidi in aggiunta a quelli già in essere, da attuare secondo uno specifico piano di implementazione. I tempi di attuazione del piano e i presidi compensativi di tipo organizzativo o

(1) 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 (cfr. Capitolo 3, Sezione IV, par. 1) 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).

(2) 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 (cfr. Sezione IV, par. 6).

(3) La classificazione delle informazioni gestite mediante strumenti ICT è opportunamente raccordata con il trattamento delle informazioni aziendali in formato diverso da quello elettronico, onde conseguire uniformi livelli di protezione indipendentemente dalle modalità di trattamento.

(4) Ad esempio, con riferimento alla sicurezza informatica, va assegnato un indicatore di criticità in relazione al potenziale impatto di eventuali violazioni dei livelli di riservatezza, integrità, disponibilità richiesti dall'utente responsabile e alla probabilità di accadimento delle minacce che potrebbero causare tali violazioni.

(5) 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.

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

procedurale nelle more dell'attuazione, sono documentati e sottoposti all'accettazione formale dell'utente responsabile.

I risultati del processo (livelli di classificazione, rischi potenziali e residui, lista delle minacce considerate, elenco dei presidi individuati), ogni loro aggiornamento successivo, le assunzioni operate e le decisioni assunte, sono documentati e portati a conoscenza dell'organo con funzione di gestione.

Il processo di analisi del rischio è ripetuto con periodicità adeguata alla tipologia delle risorse ICT e dei rischi e, comunque, in presenza di situazioni che possono influenzare il complessivo livello di rischio informatico (7).

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

SEZIONE IV

LA GESTIONE DELLA SICUREZZA INFORMATICA

1. Premessa

La gestione della sicurezza informatica comprende i processi e le misure volti, in raccordo con la generale azione aziendale per preservare la sicurezza delle informazioni e dei beni aziendali, a garantire a ciascuna risorsa informatica una protezione, in termini di riservatezza, integrità, disponibilità, verificabilità e *accountability*, appropriata e coerente lungo l'intero ciclo di vita.

Obiettivo di tale processo è anche di contribuire alla conformità del sistema informativo alle norme di legge e a regolamenti interni ed esterni.

La struttura dei processi e l'intensità dei presidi da porre in atto dipende dalle risultanze del processo di analisi dei rischi (cfr. Sezione III).

2. *Policy* di sicurezza

La *policy* di sicurezza informatica è approvata dall'organo con funzione di supervisione strategica e comunicata a tutto il personale e alle terze parti coinvolte nella gestione di informazioni e componenti del sistema informativo. Essa riporta:

— gli obiettivi del processo di gestione della sicurezza informatica in linea con la propensione al rischio informatico definito a livello aziendale (cfr. Sezione II, par. 2); tali obiettivi sono espressi in termini di esigenze di protezione e di controllo del rischio tecnologico;

— i principi generali di sicurezza sull'utilizzo e la gestione del sistema informativo da parte dei diversi profili aziendali;

— i ruoli e le responsabilità connessi alla funzione di sicurezza informatica nonché all'aggiornamento e verifica delle *policy*;

— il quadro di riferimento organizzativo e metodologico dei processi di gestione dell'ICT deputati a garantire l'appropriato livello di protezione;

— le linee di indirizzo per le attività di comunicazione, formazione e sensibilizzazione delle diverse classi di utenti;

— un richiamo alle norme interne che disciplinano le conseguenze di violazioni rilevate della *policy* da parte del personale;

— un richiamo alle norme di legge e alle altre normative esterne applicabili inerenti alla sicurezza di informazioni e risorse ICT, incluse le norme riportate nella presente Sezione.

La *policy* di sicurezza può fare riferimento a documenti di maggiore dettaglio, ad es. linee guida o manuali operativi in tema di configurazioni e procedure di sicurezza per particolari componenti e applicazioni; *policy* dedicata per i servizi di pagamento via internet; norme per il

corretto utilizzo di applicazioni aziendali trasversali, quali la posta elettronica e la navigazione internet.

La regolare revisione della *policy* di sicurezza tiene conto dell'evoluzione del campo di attività, dei prodotti forniti, delle tecnologie e dei rischi fronteggiati dall'intermediario (cfr. Sezione III).

3. La sicurezza delle informazioni e delle risorse ICT

La sicurezza delle informazioni e delle risorse informatiche è garantita attraverso misure di protezione a livello fisico e logico, la cui intensità di applicazione è graduata in relazione alle risultanze della valutazione del rischio (classificazione delle risorse informatiche in termini di sicurezza). Tali misure sono distribuite su diversi strati, così che un'eventuale falla in una linea di difesa sia coperta dalla successiva ("difesa in profondità"), comprendendo:

— i presidi fisici di difesa e le procedure di autorizzazione e controllo per l'accesso fisico a sistemi e dati (ad es., barriere perimetrali con punti di ingresso vigilati, locali ad accesso controllato con registrazione degli ingressi e delle uscite);

— la regolamentazione dell'accesso logico a reti, sistemi, basi di dati sulla base delle effettive esigenze operative (principio del *need to know)*; i diritti di accesso sono accordati, mediante ricorso ad opportuni profili abilitativi, previa formale autorizzazione; l'elenco degli utenti abilitati è sottoposto a verifica con periodicità definita;

— la procedura di autenticazione per l'accesso alle applicazioni e ai sistemi; in particolare sono garantiti l'univoca associazione a ciascun utente delle proprie credenziali di accesso, il presidio della riservatezza dei fattori di autenticazione (1), l'osservanza degli standard definiti all'interno nonché delle normative applicabili, ad es. in materia di composizione e gestione della password, di limiti ai tentativi di accesso, di lunghezza di chiavi crittografiche;

— la segmentazione della rete di telecomunicazione, con controllo dei flussi scambiati, in particolare tra domini connotati da diversi livelli di sicurezza (ad es., sistemi e utenti interni, applicazioni *core*, sistemi e utenti esterni); l'accesso a sistemi e servizi critici tramite canali pubblici (ad es., nel caso dell'*e-banking* tramite internet) sono presidiati in modo da soddisfare rigorosi requisiti di sicurezza e fornire un livello di protezione conforme ai rischi da fronteggiare; con riferimento ai servizi di pagamento tramite internet si applicano gli "Orientamenti finali in materia di sicurezza dei pagamenti via internet" emanati dall'ABE, secondo quanto specificato nella Sezione VII;

— l'adozione di metodologie e tecniche per lo sviluppo sicuro del software quale possibile presidio di difesa per componenti valutate nell'analisi del rischio informatico a un livello di rischio potenziale elevato;

— la separazione degli ambienti di sviluppo, collaudo e produzione, con adeguata formalizzazione del passaggio di moduli software tra di essi (par. 5), al fine di evitare – di

(1) La procedura di generazione e di gestione fattori delle credenziali di autenticazione (ad es., password, *smart card*, *token*) garantisce che essi siano unici e nella disponibilità esclusiva del legittimo utente assegnatario, fatta salva la possibilità di definire procedure sicure per permettere all'intermediario di accedere a dati aziendali in caso di necessità, in assenza degli utenti abilitati.

norma – l'accesso a dati riservati e componenti critiche da parte del personale addetto allo sviluppo (2); l'ambiente di produzione è sottoposto a misure più restrittive di controllo degli accessi e delle modifiche;

— i criteri per la selezione e la gestione del personale adibito al trattamento dei dati e allo svolgimento di operazioni critiche (amministratori di sistema e utenti privilegiati) con particolare riguardo alla valutazione delle competenze e dell'affidabilità del personale, alla stipula di specifici impegni di riservatezza nonché alla gestione nel continuo delle mansioni assegnate (ad es., per mezzo di verifiche periodiche degli elenchi del personale abilitato e di misure di *job rotation*);

— le procedure per lo svolgimento delle operazioni critiche, garantendo il rispetto dei principi del minimo privilegio e della segregazione dei compiti (ad es., specifiche procedure di abilitazione e di autenticazione, controlli di tipo *four eyes* (3), o di verifica giornaliera *ex post*);

— il monitoraggio, anche attraverso l'analisi di log e tracce di *audit*, di accessi, operazioni e altri eventi al fine di prevenire e gestire gli incidenti di sicurezza informatica; le attività degli amministratori di sistema e altri utenti privilegiati delle componenti critiche sono sottoposte a stretto controllo;

— il monitoraggio continuativo delle minacce e delle vulnerabilità di sicurezza;

— le regole di tracciabilità delle azioni svolte, finalizzate a consentire la verifica a posteriori delle operazioni critiche, con l'archiviazione dell'autore, data e ora (4), contesto operativo e altre caratteristiche salienti della transazione. Le tracce elettroniche sono conservate per un periodo non inferiore a 24 mesi in archivi non modificabili o le cui modifiche sono puntualmente registrate.

4. La sicurezza delle applicazioni sviluppate dalle unità operative e di controllo

Lo sviluppo di applicazioni direttamente in carico alle unità operative e di controllo è sottoposto a misure di natura organizzativa e metodologica, tese a garantire un livello di sicurezza comparabile con le applicazioni sviluppate dalla funzione ICT.

Un periodico monitoraggio censisce le applicazioni sviluppate con strumenti di informatica d'utente e ne verifica la rispondenza alla *policy* di sicurezza, in particolare se utilizzate in attività rilevanti quali la predisposizione dei dati di bilancio, del *risk management*, della finanza e del *reporting* direzionale, al fine di contenere il rischio operativo (5).

(2) Tale accesso può essere concesso agli sviluppatori in casi specificamente disciplinati, in via temporanea e previa autorizzazione dell'utente responsabile.

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

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

(5) Tale censimento è anche utile a verificare il grado di copertura delle esigenze garantito dalle procedure messe a disposizione dalla funzione ICT.

5. La gestione dei cambiamenti

La procedura di gestione dei cambiamenti delle applicazioni e risorse ICT è formalmente definita e garantisce il controllo su modifiche, sostituzioni o adeguamenti tecnologici, in particolare nell'ambiente di produzione. Il processo 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:

— la predisposizione e il costante aggiornamento nel tempo di un inventario o mappa del patrimonio ICT (hardware, software, dati, procedure) (6);

— la valutazione dell'impatto dei cambiamenti sul sistema e dei rischi correlati con le proposte di modifica;

— l'autorizzazione formale di ogni cambiamento in ambiente di produzione (7); tale procedura comprende l'accettazione, nei casi critici individuati nell'analisi dei rischi, nel nuovo rischio residuo;

— la pianificazione, il coordinamento e la documentazione degli interventi di modifica, prevedendo attività di collaudo e test di sicurezza, in un ambiente deputato e distinto da quello di produzione;

— il ricorso a un idoneo sistema di gestione della configurazione di sistema (hardware, software, procedure di gestione e utilizzo, modalità di interconnessione), per il controllo dell'implementazione dei cambiamenti, inclusa la possibilità di ripristino della situazione *ex ante*.

Le modifiche in caso di emergenza possono essere gestite con presidi non pienamente conformi alle *policy* ordinarie ma comunque adeguati alla particolare situazione. Tali modifiche sono comunque sottoposte a tracciamento e notificate *ex post* all'utente responsabile.

Le iniziative di ampio impatto sul sistema informativo (ad es., 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 e prevedono, in aggiunta a quanto sopra specificato, idonee misure, tecniche, organizzative e procedurali, volte a garantire un avvio in esercizio controllato e con limitati impatti sui servizi forniti alla clientela (ad es., implementazione per stadi successivi, periodi di esercizio in parallelo con la precedente procedura, procedure di *fallback* e *contingency*). Flussi informativi verso i vari livelli manageriali e gli organi aziendali consentono il monitoraggio dell'avanzamento del progetto.

(6) L'inventario aggiornato del sistema e delle risorse ICT è funzionale anche alle attività di analisi del rischio informatico (cfr. Sezione III).

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

6. La gestione degli incidenti di sicurezza informatica

La gestione degli incidenti di sicurezza informatica segue procedure formalmente definite, con l'obiettivo di minimizzare l'impatto di eventi avversi e garantire il tempestivo ripristino del regolare funzionamento dei servizi e delle risorse ICT coinvolti. Le funzioni a cui comunicare l'incidente sono individuate secondo un'opportuna procedura di *escalation*; i casi più gravi che comportino rischi di interruzione della continuità operativa sono segnalati alla struttura preposta a dichiarare lo stato di crisi (cfr. Capitolo 5).

A seguito dell'analisi degli incidenti di sicurezza informatica e dei relativi rilievi delle funzioni di *audit* e della *compliance* sono definite e monitorate le azioni correttive.

In ogni caso, le informazioni salienti dell'evento e i passi seguiti nella gestione dello stesso sono documentati.

Il processo si raccorda con il monitoraggio di sistemi, accessi e operazioni (cfr. par. 3) nonché con la gestione dei malfunzionamenti e delle segnalazioni di problemi da parte degli utenti interni ed esterni, favorendo l'assunzione di iniziative di prevenzione (8).

Le procedure definite per gravi incidenti di sicurezza informatica includono la cooperazione con le forze dell'ordine preposte e con gli altri operatori o enti coinvolti, anche in caso di fuoriuscite di informazioni.

I gravi incidenti di sicurezza informatica sono comunicati tempestivamente alla Banca centrale europea o 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 i seguenti dati, accertati o presunti: i) data e ora dell'accadimento o della manifestazione dell'incidente; ii) risorse e servizi coinvolti; iii) cause, tempi e modalità previsti per il pieno ripristino dei livelli di disponibilità e sicurezza definiti e per il completo accertamento dei fatti connessi; iv) descrizione delle azioni intraprese e dei risultati ottenuti; v) una valutazione dei danni delle perdite economiche o danni d'immagine.

7. La disponibilità delle informazioni e delle risorse ICT

La disponibilità dell'accesso a dati e dei servizi telematici è garantita agli utenti autorizzati in orari e con modalità conformi alle esigenze (9). A tal fine, i processi interessati (definizione dei modelli architetturali, sviluppo di applicazioni e infrastrutture, gestione dei problemi tecnici, monitoraggio e pianificazione della capacità elaborativa e trasmissiva, gestione dei fornitori) tengono conto delle seguenti indicazioni:

— con riguardo alle applicazioni di maggiore criticità e ai servizi ICT rivolti alla clientela sono formalmente definiti i livelli di servizio che l'intermediario si impegna ad osservare; le prestazioni delle componenti critiche rispetto a tali livelli sono regolarmente monitorate e formano oggetto di sintetici rapporti disponibili periodicamente a tutte le parti interessate; è assicurata la congruità tra i livelli di servizio definiti per le componenti tra loro dipendenti;

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

(9) Si tiene conto del profilo di utilizzo (noto o stimato) nell'arco del calendario e per l'orario di operatività, con particolare attenzione a eventuali picchi elaborativi.

— in relazione alle esigenze di disponibilità delle singole applicazioni, sono definite procedure di *backup* (di dati, software e configurazione) e di ripristino su sistemi alternativi, in precedenza individuati;

— le architetture sono disegnate in considerazione dei profili di sicurezza informatica delle applicazioni ospitate, tenendo conto di tutte le risorse ICT e di supporto interessate (alimentazione elettrica, impianti di condizionamento, ecc.); a tale riguardo, l'intermediario valuta la necessità di predisporre piattaforme particolarmente robuste e ridondate (ad es., applicando il principio del *no single point of failure*) volte a garantire l'alta disponibilità delle applicazioni maggiormente critiche, in sinergia con le procedure e il sistema di *disaster recovery;*

— in funzione dei profili di rischio delle comunicazioni, delle applicazioni e dei servizi acceduti, i collegamenti telematici interni alla banca o al gruppo sono opportunamente ridondati; in relazione al rischio di incidenti di sicurezza informatica che possono determinare l'interruzione dei servizi (ad es., mediante attacchi di tipo *denial of service o distributed denial of service*), oltre a soluzioni specifiche per l'individuazione e il blocco del traffico malevolo, la banca valuta l'opportunità di sfruttare procedure e strumenti per l'allocazione dinamica di capacità trasmissiva ed elaborativa;

— la gestione del sistema informativo è opportunamente automatizzata e si avvale, per quanto possibile, di procedure standardizzate; le operazioni di manutenzione ordinaria e straordinaria sono pianificate e comunicate con congruo anticipo agli utenti interessati;

— le informazioni raccolte attraverso il processo di monitoraggio delle risorse ICT alimentano il regolare processo di *capacity planning* (10) e sono utilizzate nella progettazione dell'evoluzione del sistema informativo.

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

SEZIONE V

IL SISTEMA DI GESTIONE DEI DATI

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

In particolare, il sistema di gestione dei dati soddisfa i seguenti requisiti:

— la registrazione dei fatti aziendali è completa, corretta e tempestiva, al fine di consentire la ricostruzione dell'attività svolta (1);

— è definito uno standard aziendale di *data governance*, che individua ruoli e responsabilità delle funzioni coinvolte nell'utilizzo e nel trattamento, a fini operativi e gestionali delle informazioni aziendali (2); in considerazione della loro rilevanza nel sistema informativo, sono definite le misure atte a garantire e a misurare la qualità (3), ad es. attraverso *key quality indicato*r riportati periodicamente agli utenti di *business*, alle funzioni di controllo e all'organo con funzione di gestione;

— la identificazione, la misurazione o la valutazione, il monitoraggio, la prevenzione o l'attenuazione dei rischi connessi con la qualità dei dati fa parte del processo di gestione dei rischi (cfr. Capitolo 3); in caso di acquisizione o incorporazione di soggetti esterni, la *due diligence* comprende la valutazione dell'impatto dell'operazione sulle procedure di gestione e aggregazione dei dati; l'utilizzo di procedure settoriali (contabilità, segnalazioni, antiriciclaggio, ecc.) non compromette la qualità e la coerenza complessiva dei dati aziendali; a livello consolidato, il sistema di gruppo assicura l'integrazione tra le informazioni provenienti da tutte le componenti del gruppo;

— nel caso di ricorso a un *data warehouse* aziendale a fini di analisi e *reporting*, le procedure di estrazione dei dati, di trasformazione, controllo e caricamento negli archivi accentrati – così come le funzioni di sfruttamento dei dati – sono dettagliatamente documentate, al fine di consentire la verifica sulla qualità dei dati;

— le procedure di gestione e aggregazione dei dati sono documentate, con specifica previsione delle circostanze in cui è ammessa l'immissione o la rettifica manuale di dati aziendali,

(1) I controlli sulle registrazioni contabili verificano, tra l'altro, le procedure per l'individuazione e sistemazione delle divergenze tra saldi dei sottosistemi sezionali e quelli della contabilità generale, i processi di quadratura tra i documenti di *front-office* e le registrazioni giornaliere; la conferma periodica dei rapporti con controparti e clienti. Le verifiche riguardano anche l'allineamento tra i dati utilizzati per la gestione dei rischi e per la rendicontazione finanziaria.

(2) Le banche classificate, a fini SREP, nelle macro-categorie 1 e 2 (cfr. Circolare 269 del 7 maggio 2008, "Guida per l'attività di vigilanza", Sezione I, Capito I.5) individuano per i dati rilevanti (informazione al mercato, segnalazioni all'Organo di Vigilanza, valutazione dei rischi, ecc.) una o più figure aziendali responsabili di assicurare lo svolgimento dei controlli previsti e della validazione della qualità dei dati (c.d. "*data owner*"). Le procedure di aggregazione dei dati a fini di valutazione dei rischi aziendali sono sottoposte a validazione indipendente (ad es., da parte dell'*internal audit).*

(3) La qualità dei dati è valutata, in termini di completezza (registrazione di tutti gli eventi, operazioni e informazioni con i pertinenti attributi necessari per le elaborazioni), di accuratezza (assenza di distorsione nei processi di registrazione, raccolta e di successivo trattamento dei dati) e di tempestività.

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

1. Tipologie di esternalizzazione

L'esternalizzazione delle risorse e servizi ICT può assumere diverse forme a seconda del modello architetturale adottato: dall'*outsourcing* verticale (relativo a determinati processi operativi) all'*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.

Le norme nella presente Sezione si applicano ai casi di *full outsourcing* o di esternalizzazione di componenti critiche del sistema informativo, a complemento di quanto disposto in materia di *outsourcing* di funzioni aziendali nel Capitolo 3, Sezioni IV e V.

L'intermediario valuta la possibilità di ricorrere all'esternalizzazione considerando attentamente tutti i rischi (tra cui: operativi, di *compliance*, strategici e reputazionali) inerenti tale opzione, e tenendo conto della necessità, nel caso, di mettere in atto le idonee misure di contenimento.

Con particolare riferimento all'esternalizzazione di parte o tutto il sistema presso fornitori al di fuori del gruppo di appartenenza, la scelta è basata su un'analisi del rischio, che considera in primo luogo la stima dei rischi delle risorse e servizi da esternalizzare (ad es., tiene conto della classificazione dei dati e della criticità dell'operatività interessata, valutando in particolare i rischi derivanti dalla perdita del controllo diretto su componenti del sistema informativo e personale critici, nonché dei volumi delle operazioni) e quindi valuta i rischi dei possibili fornitori (ad es., condizioni finanziarie, posizionamento sul mercato, qualità e *turnover* del management e del personale, capacità di gestire la continuità operativa e di fornire accurati e tempestivi *report* direzionali sull'attività svolta, competenza ed esperienza, qualità e sicurezza nonché economicità e maturità, in un adeguato orizzonte temporale, della fornitura), la qualità dei sub-fornitori, la ridondanza delle linee di comunicazione utilizzate nonché l'affidabilità, la sicurezza e la scalabilità delle tecnologie adottate.

Nell'elaborazione del modello architetturale e delle strategie di esternalizzazione vanno considerati approcci tesi a contenere, per quanto possibile, il grado di dipendenza da specifici fornitori e partner tecnologici esterni al gruppo bancario (c.d. *vendor lock-in*), salvaguardando la possibilità di sostituire la fornitura con un'altra funzionalmente equivalente (ad es., privilegiando il ricorso a standard aperti per le connessioni, la memorizzazione e lo scambio di dati, la cooperazione applicativa) e prevedendo opportune *exit strategies* (1). Tali valutazioni tengono conto del principio di proporzionalità e dell'opportunità, per le banche di maggiore

(1) Anche l'acquisizione di licenze software per prodotti installati sul proprio sistema, a supporto di importanti processi aziendali trasversali, può introdurre forme di dipendenza dal fornitore, a seguito di vincoli tecnologici o contrattuali che impongano il ricorso al fornitore o a società collegate per la manutenzione o rendano assai ardua la sostituzione del prodotto. Tali considerazioni rientrano tra gli elementi essenziali nel processo di selezione delle soluzioni software.

dimensione, di mantenere all'interno della banca o del gruppo competenze professionali per gestire una transizione tra modelli di *sourcing* in caso di grave necessità.

Il mantenimento nel tempo da parte del fornitore delle condizioni necessarie a fornire un servizio rispondente alle esigenze e conforme alle norme è assicurato attraverso idonei strumenti contrattuali e procedure di controllo.

2. Accordi con i fornitori e altri requisiti

Nel caso di esternalizzazione del sistema informativo e di risorse ICT critiche, la comunicazione preventiva alla Banca centrale europea o alla Banca d'Italia (cfr. Capitolo 3, Sezioni IV e V) include i risultati dell'analisi dei rischi e – limitatamente agli intermediari delle macro-categorie 1 e 2 a fini SREP – la descrizione delle *exit strategies* previste.

Il referente per l'attività esternalizzata possiede le competenze idonee per esercitare il proprio ruolo di controllo sulle componenti gestite dal fornitore di servizi.

Nei contratti con i fornitori di sistemi e servizi ICT, in aggiunta alle richiamate disposizioni del Capitolo 3, sono disciplinati al minimo i seguenti aspetti:

— l'obbligo per il fornitore di servizi di osservare la *policy* di sicurezza informatica aziendale, per quanto applicabile; il fornitore provvede al trattamento dei dati in accordo con il loro livello di classificazione, con particolare riferimento alla riservatezza;

— la proprietà di dati, software, documentazione tecnica e altre risorse ICT, con l'esclusiva per l'intermediario sui dati inerenti la clientela e i servizi ad essa forniti;

— la periodica produzione delle copie di *backup* del sistema informativo (database, transazioni, log applicativi e di sistema); l'intermediario può accedere alle copie di *backup* su richiesta;

— la ripartizione dei compiti e delle responsabilità attinenti i presidi di sicurezza per la tutela di dati, applicazioni e sistemi; i presidi sono riferiti alle principali minacce interne ed esterne, anche attraverso internet;

— le procedure di comunicazione e coordinamento in caso di incidenti di sicurezza informatica e di continuità operativa;

— la definizione di livelli di servizio coerenti con le esigenze delle applicazioni e dei processi aziendali che si avvalgono dei servizi esternalizzati;

— la predisposizione di misure di tracciamento idonee a garantire l'*accountability* e la ricostruibilità delle operazioni effettuate, almeno con riferimento alle operazioni critiche e agli accessi a dati riservati;

— il raccordo con i ruoli e le procedure definite all'interno dell'intermediario per il processo di analisi dei rischi (cfr. Sezione III) e per il sistema di gestione dei dati (cfr. Sezione V);

— la possibilità per l'intermediario di conoscere l'ubicazione dei *data center* e una indicazione del numero di addetti con accesso ai dati riservati o alle componenti critiche; tali informazioni sono periodicamente aggiornate dal fornitore di servizi;

— 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 capacità tecniche, debitamente documentati – qualsiasi copia o stralcio di dati riservati di proprietà dell'intermediario e presente su propri sistemi o supporti, in modo da escludere qualunque accesso successivo da parte del proprio personale o di terzi.

3. Indicazioni particolari

L'intermediario pone particolare cautela nella valutazione di offerte di servizi in *outsourcing* erogati secondo modelli innovativi che prevedono la fruizione delle risorse informatiche nella forma di servizi accessibili via rete e configurabili in modo flessibile dall'utente (*cloud computing*).

Il *cloud computing* può essere implementato secondo diverse tipologie:

— *cloud privato*: ambienti interni alla società o al gruppo che permettono la condivisione di risorse ICT tra più aree e realtà aziendali; questo caso non rientra nella definizione di servizio esternalizzato;

— *community*: i servizi sono utilizzati da un ristretto numero di organizzazioni, tipicamente operanti nello stesso settore economico, che condividono analoghe necessità e obiettivi. La condivisione delle risorse informatiche è ristretta a dette organizzazioni;

— *cloud pubblico*: i servizi sono erogati a un vasto numero di utenti con funzionalità offerte in maniera aperta e condivisa. I fornitori in genere sfruttano la possibilità di condividere in modo flessibile le proprie risorse tra i diversi utenti e applicano di norma tariffe proporzionali all'utilizzo (*pay-per-use*).

Nel caso dell'acquisizione di servizi in *community* o *in cloud* pubblici i maggiori rischi potenziali possono richiedere una più elevata complessità dei controlli da predisporre, in particolare in caso di esternalizzazione di componenti critiche.

A causa della possibilità tecnica per il fornitore di spostare rapidamente e in modo trasparente all'utente le risorse dedicate ai vari clienti, è importante che le locazioni dei *data center* utilizzabili siano preventivamente comunicate. E' necessario prevedere adeguati meccanismi di isolamento dei dati di un intermediario rispetto agli altri clienti, a garanzia della loro riservatezza e integrità. Il fornitore garantisce contrattualmente il rispetto dei livelli di servizio stabiliti, anche in casi di emergenza o di contesa delle risorse da parte di altri suoi clienti, e assicura la piena ricostruzione degli accessi e delle modifiche effettuate sui dati, anche per finalità ispettive. Sono concordate con il fornitore di servizi modalità di *audit* adeguate alla criticità delle risorse esternalizzate e in considerazione dell'architettura del fornitore.

SEZIONE VII

PRINCIPI ORGANIZZATIVI RELATIVI A SPECIFICHE ATTIVITÀ O PROFILI DI RISCHIO

1. Sicurezza dei pagamenti via internet

Le banche che prestano alla propria clientela servizi di pagamento tramite canale internet si attengono agli "Orientamenti finali sulla sicurezza dei pagamenti via internet" emanati dall'ABE ([1]). In linea con quanto previsto dagli Orientamenti, è rimessa alla valutazione di ogni banca la scelta se attenersi anche agli esempi di Migliori Prassi di cui all'Allegato 1 dei citati Orientamenti.

Gli obblighi imposti integrano e specificano le disposizioni sul Sistema informativo con riferimento alla *governance* e all'organizzazione del sistema informativo; la gestione del rischio informatico; i requisiti per assicurare la sicurezza informatica e il sistema di gestione dei dati.

In linea con l'impostazione generale della disciplina in materia di controlli interni e gestione dei rischi e fermi restando i casi in cui gli Orientamenti prescrivono obblighi specifici (come nel caso dell'utilizzo dell' "autenticazione forte"), le banche applicano le disposizioni contenute negli Orientamenti secondo il principio di proporzionalità, cioè tenuto conto della dimensione e complessità operative, della natura dell'attività svolta, della tipologia dei servizi prestati.

([1]) https://www.eba.europa.eu/documents/10180/1004450/EBA_2015_IT+Guidelines+on+Internet+Payments.pdf/b9c5dee9-78bd-47c5-a80c-4d2f3f8a1de2

Allegato A

DOCUMENTI AZIENDALI PER LA GESTIONE E IL CONTROLLO DEL SISTEMA INFORMATIVO

Documento	Approvazione	Aggiornamento	Note
DOCUMENTI DI *POLICY* 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): - modello di riferimento architetturale - strategie di *sourcing* - propensione al rischio informatico
Metodologia di analisi del rischio informatico	Organo con funzione di supervisione strategica	In base alla necessità	
Policy di sicurezza informatica	Organo con funzione di supervisione strategica	In base alla necessità	
Organigramma della funzione ICT	Organo con funzione di supervisione strategica	In base alla necessità	Include il disegno dei processi di gestione dell'ICT (cfr. Sezione II, par. 2)
Standard di *data governance*	Organo con funzione di gestione	Periodicità definita	
ALTRI DOCUMENTI ESSENZIALI PER LA GESTIONE E LO SVILUPPO DEI SISTEMI ICT			
Procedura di gestione dei cambiamenti	Organo con funzione di gestione	In base alla necessità	
Procedura di gestione degli incidenti	Organo con funzione di gestione	In base alla necessità	
Piano operativo	Organo con funzione di gestione	Annuale	
VALUTAZIONI AZIENDALI			
Rapporto sintetico su adeguatezza e costi dell'ICT	Organo con funzione di supervisione	Annuale	

Documento	Approvazione	Aggiornamento	Note
	strategica		
Rapporto sintetico sulla situazione del rischio informatico	Organo con funzione di supervisione strategica	Annuale	
Rapporti dell'*internal audit* e delle altre funzioni responsabili della valutazione della sicurezza	Organo con funzione di supervisione strategica	Almeno annuale	