Riunione del 18 febbraio 2026

Alberto Balestreri

Materiale riservato ai membri della Commissione Banche, Intermediari Finanziari ed Assicurazione dell'ODCEC di Milano

Commissione Banche, Intermediari finanziari e Assicurazioni

1. Approvazione dei verbali delle precedenti riunioni

Verbali

1. 26 giugno 2025
2. 17 settembre 2025
3. 13 novembre 2025
4. 20 gennaio 2026

2. Regolamento DORA e Circolare 285

L'aggiornamento n. 51 della Circolare della Banca d'Italia n. 285/2013

al fine di:

1. assicurare un riordino della disciplina applicabile alla luce delle previsioni:

- del regolamento (UE) 2022/2554 sulla resilienza operativa digitale per il settore finanziario ("Regolamento DORA");
- dei relativi atti delegati;

2. dare attuazione all'articolo 4 della direttiva (UE) 2022/2556 ("Direttiva DORA"), recante modifiche alla direttiva 2013/36/UE:

ha modificato:

Parte Prima, Titolo IV

- Capitolo 4 “Il sistema informativo”
- Capitolo 5 “La continuità operativa”

ha effettuato alcuni interventi di raccordo e aggiornamento:

Parte Prima, Titolo I

- *Disposizioni introduttive*
- *Capitolo 1 “Autorizzazione all’attività bancaria”.*

Parte Prima, Titolo IV

- Capitolo 3 “Il sistema dei controlli interni”

2A. Parte Prima – Titolo IV – Capitolo 4 «Il sistema informativo»

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

Sono state abrogate le Sezioni del Capitolo 4 su:

1. governo del sistema informativo;
2. gestione del rischio ICT e di sicurezza;
3. gestione della sicurezza dell'informazione e delle operazioni ICT;
4. gestione dei progetti e dei cambiamenti ICT
5. esternalizzazione del sistema informativo e ricorso a soggetti terzi per la prestazione di servizi ICT.

In luogo di tali Sezioni, viene inserito un rinvio alle previsioni, direttamente applicabili, del Regolamento DORA e dei relativi atti delegati in materia di:

1. strumenti, metodi, processi e politiche per la gestione dei rischi informatici;
2. politica relativa agli accordi contrattuali per l'utilizzo di servizi ICT a supporto di funzioni essenziali o importanti prestati da fornitori terzi di servizi ICT;
3. incidenti ICT;
4. minacce informatiche significative.

TITOLO IV

Capitolo 4

IL SISTEMA INFORMATIVO

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 – Fonti normative

TITOLO IV - Capitolo 4

IL SISTEMA INFORMATIVO

SEZIONE I

FONTI NORMATIVE

La materia è direttamente regolata:

— dal regolamento (UE) 2022/2554 del Parlamento europeo e del Consiglio del 14 dicembre 2022 relativo alla resilienza operativa digitale per il settore finanziario e che modifica i regolamenti (CE) n. 1060/2009, (UE) n. 648/2012, (UE) n. 600/2014, (UE) n. 909/2014 e (UE) 2016/1011 (DORA);

— dal regolamento delegato (UE) 2024/1774 della Commissione del 13 marzo 2024 che integra il regolamento (UE) 2022/2554 del Parlamento europeo e del Consiglio per quanto riguarda le norme tecniche di regolamentazione che specificano gli strumenti, i metodi, i processi e le politiche per la gestione dei rischi informatici e il quadro semplificato per la gestione dei rischi informatici (RTS DORA sulla gestione dei rischi informatici);

— dal regolamento delegato (UE) 2024/1773 della Commissione del 13 marzo 2024 che integra il regolamento (UE) 2022/2554 del Parlamento europeo e del Consiglio per quanto riguarda le norme tecniche di regolamentazione che precisano il contenuto dettagliato della politica relativa agli accordi contrattuali per l'utilizzo di servizi TIC a supporto di funzioni essenziali o importanti prestati da fornitori terzi di servizi TIC;

— dal regolamento delegato (UE) 2025/532 della Commissione del 24 marzo 2025 che integra il regolamento (UE) 2022/2554 del Parlamento europeo e del Consiglio per quanto riguarda le norme tecniche di regolamentazione che specificano gli elementi che l'entità finanziaria deve determinare e valutare quando subappalta servizi TIC a supporto di funzioni essenziali o importanti;

— dal regolamento delegato 2025/1190 della Commissione del 13 febbraio 2025 che integra il regolamento (UE) 2022/2554 del Parlamento europeo e del Consiglio per quanto riguarda le norme tecniche di regolamentazione che specificano i criteri utilizzati per identificare le entità finanziarie che hanno l'obbligo di svolgere test di penetrazione guidati dalla minaccia, i requisiti e le norme che disciplinano il ricorso a soggetti incaricati dello svolgimento dei test interni, i requisiti concernenti l'ambito, l'approccio e la metodologia da seguire per i test in ciascuna fase dei test, i risultati, la chiusura e le fasi correttive e il tipo di cooperazione di vigilanza e altri tipi di cooperazione pertinenti necessari per svolgere i TLPT e per la facilitazione del riconoscimento reciproco;

— dal regolamento delegato (UE) 2024/1772 della Commissione, del 13 marzo 2024, che integra il regolamento (UE) 2022/2554 del Parlamento europeo e del Consiglio per quanto riguarda le norme tecniche di regolamentazione che specificano i criteri per la classificazione degli incidenti connessi alle TIC e delle minacce informatiche, stabiliscono le soglie di rilevanza e specificano i dettagli delle segnalazioni di gravi incidenti;

— dal regolamento delegato (UE) 2025/301 della Commissione, del 23 ottobre 2024 che integra il regolamento (UE) 2022/2554 del Parlamento europeo e del Consiglio per quanto riguarda le norme tecniche di regolamentazione che specificano il contenuto e i termini della notifica iniziale, della relazione intermedia e della relazione finale per gli incidenti gravi connessi alle TIC nonché il contenuto della notifica volontaria per le minacce informatiche significative;

— dal regolamento di esecuzione 2024/2956 della Commissione del 29 novembre 2024 che stabilisce norme tecniche di attuazione per l'applicazione del regolamento (UE) 2022/2554 del Parlamento europeo e del Consiglio per quanto riguarda i modelli standard in relazione al registro delle informazioni;

— dal regolamento di esecuzione (UE) 2025/302 della Commissione, del 23 ottobre 2024 che stabilisce norme tecniche di attuazione per l'applicazione del regolamento (UE) 2022/2554 del Parlamento europeo e del Consiglio per quanto riguarda i formati, i modelli e le procedure standard con cui le entità finanziarie devono segnalare un incidente grave connesso alle TIC e notificare una minaccia informatica significativa.

La materia è altresì disciplinata:

— dalla direttiva (UE) 2022/2556 del Parlamento europeo e del Consiglio del 14 dicembre 2022 che modifica le direttive 2009/65/CE, 2009/138/CE, 2011/61/UE, 2013/36/UE, 2014/59/UE, 2014/65/UE, (UE) 2015/2366 e (UE) 2016/2341 per quanto riguarda la resilienza operativa digitale per il settore finanziario (Direttiva DORA);

— dal decreto legislativo 10 marzo 2025, n. 23, Adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2022/2554 (DORA), relativo alla resilienza operativa digitale per il settore finanziario e che modifica i regolamenti (CE) n. 1060/2009, (UE) n. 648/2012, (UE) n. 600/2014, (UE) n. 909/2014 e (UE) 2016/1011, e per il recepimento della direttiva (UE) 2022/2556 (direttiva DORA), che modifica le direttive 2009/65/CE, 2009/138/CE, 2011/61/UE, 2013/36/UE, 2014/59/UE, 2014/65/UE, (UE) 2015/2366 e (UE) 2016/2341 per quanto riguarda la resilienza operativa digitale per il settore finanziario;

— dall'art. 146, comma 2, lett. b), del TUB, 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;

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 – Fonti normative

— 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:

— 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 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 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, come modificati dagli Orientamenti emanati dall'EBA l'11 febbraio 2025 (EBA/GL/2025/02);

— la Comunicazione della Banca d'Italia del 30 dicembre 2024 sul Regolamento DORA.

Si è anche tenuto conto di:

— 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.

1. **regolamento (UE) 2022/2554** del Parlamento europeo e del Consiglio del 14 dicembre 2022 relativo alla resilienza operativa digitale per il settore finanziario e che modifica i regolamenti (CE) n. 1060/2009, (UE) n. 648/2012, (UE) n. 600/2014, (UE) n. 909/2014 e (UE) 2016/1011 (DORA);
2. **regolamento delegato (UE) 2024/1774** della Commissione del 13 marzo 2024 che integra il regolamento (UE) 2022/2554 del Parlamento europeo e del Consiglio per quanto riguarda le norme tecniche di regolamentazione che specificano gli strumenti, i metodi, i processi e le politiche per la gestione dei rischi informatici e il quadro semplificato per la gestione dei rischi informatici (RTS DORA sulla gestione dei rischi informatici);
3. **regolamento delegato (UE) 2024/1773** della Commissione del 13 marzo 2024 che integra il regolamento (UE) 2022/2554 del Parlamento europeo e del Consiglio per quanto riguarda le norme tecniche di regolamentazione che precisano il contenuto dettagliato della politica relativa agli accordi contrattuali per l'utilizzo di servizi TIC a supporto di funzioni essenziali o importanti prestati da fornitori terzi di servizi TIC;
4. **regolamento delegato (UE) 2025/532** della Commissione del 24 marzo 2025 che integra il regolamento (UE) 2022/2554 del Parlamento europeo e del Consiglio per quanto riguarda le norme tecniche di regolamentazione che specificano gli elementi che l'entità finanziaria deve determinare e valutare quando subappalta servizi TIC a supporto di funzioni essenziali o importanti;
5. **regolamento delegato 2025/1190** della Commissione del 13 febbraio 2025 che integra il regolamento (UE) 2022/2554 del Parlamento europeo e del Consiglio per quanto riguarda le norme tecniche di regolamentazione che specificano i criteri utilizzati per identificare le entità finanziarie che hanno l'obbligo di svolgere test di penetrazione guidati dalla minaccia, i requisiti e le norme che disciplinano il ricorso a soggetti incaricati dello svolgimento dei test interni, i requisiti concernenti l'ambito, l'approccio e la metodologia da seguire per i test in ciascuna fase dei test, i risultati, la chiusura e le fasi correttive e il tipo di cooperazione di vigilanza e altri tipi di cooperazione pertinenti necessari per svolgere i TLPT e per la facilitazione del riconoscimento reciproco;

6. **regolamento delegato (UE) 2024/1772** della Commissione, del 13 marzo 2024, che integra il regolamento (UE) 2022/2554 del Parlamento europeo e del Consiglio per quanto riguarda le norme tecniche di regolamentazione che specificano i criteri per la classificazione degli incidenti connessi alle TIC e delle minacce informatiche, stabiliscono le soglie di rilevanza e specificano i dettagli delle segnalazioni di gravi incidenti;
7. **regolamento delegato (UE) 2025/301** della Commissione, del 23 ottobre 2024 che integra il regolamento (UE) 2022/2554 del Parlamento europeo e del Consiglio per quanto riguarda le norme tecniche di regolamentazione che specificano il contenuto e i termini della notifica iniziale, della relazione intermedia e della relazione finale per gli incidenti gravi connessi alle TIC nonché il contenuto della notifica volontaria per le minacce informatiche significative;
8. **regolamento di esecuzione 2024/2956** della Commissione del 29 novembre 2024 che stabilisce norme tecniche di attuazione per l'applicazione del regolamento (UE) 2022/2554 del Parlamento europeo e del Consiglio per quanto riguarda i modelli standard in relazione al registro delle informazioni;
9. **regolamento di esecuzione (UE) 2025/302** della Commissione, del 23 ottobre 2024 che stabilisce norme tecniche di attuazione per l'applicazione del regolamento (UE) 2022/2554 del Parlamento europeo e del Consiglio per quanto riguarda i formati, i modelli e le procedure standard con cui le entità finanziarie devono segnalare un incidente grave connesso alle TIC e notificare una minaccia informatica significativa.che specificano i criteri per la classificazione degli incidenti connessi alle TIC e delle minacce informatiche, stab

10. **direttiva (UE) 2022/2556** del Parlamento europeo e del Consiglio del 14 dicembre 2022 che modifica le direttive 2009/65/CE, 2009/138/CE, 2011/61/UE, 2013/36/UE, 2014/59/UE, 2014/65/UE, (UE) 2015/2366 e (UE) 2016/2341 per quanto riguarda la resilienza operativa digitale per il settore finanziario (Direttiva DORA);

11. **decreto legislativo 10 marzo 2025, n. 23**, Adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2022/2554 (DORA), relativo alla resilienza operativa digitale per il settore finanziario e che modifica i regolamenti (CE) n. 1060/2009, (UE) n. 648/2012, (UE) n. 600/2014, (UE) n. 909/2014 e (UE) 2016/1011, e per il recepimento della direttiva (UE) 2022/2556 (direttiva DORA), che modifica le direttive 2009/65/CE, 2009/138/CE, 2011/61/UE, 2013/36/UE, 2014/59/UE, 2014/65/UE, (UE) 2015/2366 e (UE) 2016/2341 per quanto riguarda la resilienza operativa digitale per il settore finanziario;

12. art. 146, comma 2, lett. b), del TUB, 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;

13. **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);

14. **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;

15. **regolamento delegato (UE) 2018/389 del 27 novembre 2017-** 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;
16. **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);
17. **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;
18. **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, come modificati dagli […]
19. **Orientamenti emanati dall'EBA l'11 febbraio 2025** (EBA/GL/2025/02);
20. Comunicazione della Banca d'Italia del 30 dicembre 2024 sul Regolamento DORA.

Si è anche tenuto conto di:

1. Opinion on the implementation of the RTS on SCA and CSC (EBA-Op-2018-04), emanata dall'EBA in data 13 giugno 2018;
2. 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;
3. Opinion on the elements of strong customer authentication under PSD2 (EBA-Op-2019-06), emanata dall'EBA il 21 giugno 2019;
4. 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.

SEZIONE II

DISPOSIZIONI SPECIFICHE
IN MATERIA DI PRESTAZIONE DI SERVIZI DI PAGAMENTO

1. Sicurezza dei servizi di pagamento

La presente sezione si applica:

— alle banche italiane e alle succursali di banche extracomunitarie;

— alle capogruppo di gruppi bancari;

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

Fermo restando quanto previsto dal DORA e dall'RTS DORA sulla gestione dei rischi informatici, le banche si dotano di sistemi e misure di mitigazione e di meccanismi di controllo adeguati per gestire i rischi operativi e di sicurezza relativi ai servizi di pagamento prestati 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).

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 i paragrafi da 92 a 98 degli Orientamenti dell'EBA sulla gestione dei rischi ICT e di sicurezza, come modificati dagli Orientamenti emanati dall'EBA l'11 febbraio 2025.

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

(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.

("interfaccia di *fall-back*") previsto dall'art. 33, par. 4, del Regolamento delegato (2) 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) (3).

4. Procedimenti amministrativi

Si indicano di seguito i procedimenti amministrativi relativi alla presente sezione:

— *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).

(2) Per "meccanismo di emergenza" si intende 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.
(3) 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-rts-on-sca-csc- .

La sezione sulle disposizioni specifiche in materia di prestazione di servizi di pagamento è oggetto di modifiche volte a dare attuazione agli Orientamenti dell'EBA dell'11 febbraio 2025 (EBA/GL/2025/02), che hanno abrogato in larga parte gli Orientamenti dell'EBA sulla gestione dei rischi relativi alle tecnologie dell'informazione e di sicurezza (EBA/GL/2019/04), mantenendo esclusivamente i paragrafi relativi alla gestione del rapporto con gli utenti dei servizi di pagamento.

2B. Parte Prima – Titolo IV – Capitolo 5 «La continuità operativa»

Le modifiche del Capitolo 5 “La continuità operativa” hanno in particolare interessato i requisiti di continuità operativa applicabili a tutti gli operatori, allo scopo di:

- dare attuazione alle modifiche apportate dalla Direttiva DORA alle norme della direttiva 2013/36/UE in materia di continuità operativa;
- di rimuovere le previsioni sulla continuità operativa in ambito ICT, sostituite dalle previsioni direttamente applicabili del Regolamento DORA e dei relativi atti delegati.

Con l’occasione, si è perseguito l’obiettivo di coordinare, per quanto possibile, le regole sulla politica generale di continuità operativa con il framework DORA.

2C. Parte Prima – Titolo IV – Capitolo 3 «Il sistema dei controlli interni»

La sezione sul sistema di gestione dei dati, non ricompresa nel framework DORA, viene spostata nel capitolo 3 “Il sistema dei controlli interni” (Allegato D)

Il capitolo 3 contiene comunque (Sezione IV) il quadro di norme da applicare alla «esternalizzazioni di funzioni aziendali (outsourcing)»

Allegato D

IL SISTEMA DI GESTIONE DEI DATI

Il sistema di gestione dei dati soddisfa i seguenti requisiti:

— la registrazione delle operazioni aziendali e dei fatti di gestione 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 indicator* 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; 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, 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);

(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", Parte prima, Sezione I, Capitolo 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.

(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.

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 D – Il sistema di gestione dei dati

— il sistema di *reporting* consente di produrre informazioni tempestive e di qualità elevata per l'autorità di vigilanza e per il mercato.

3. Varie ed eventuali.

Ruolo della Commissione Banche, Intermediari Finanziari ed Assicurazioni

1. Come ridisegnare le attività della Commissione in ambito tecnologico?
2. Quale interesse e livelli di supporto da parte del nuovo Consiglio dell'ODCEC di Milano?
3. Quale ruolo della Commissione e dell'ODCEC di Milano nell'ambito della piazza finanziaria milanese?
4. Si desidera, o meno, formare almeno 100 professionisti/e under 40 specializzati in ambito finanziario? Se si, con quali strumenti e con quali metodi?