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

Firmato digitalmente da

ARGENTESI ANTONIA

Firmato digitalmente da ARGENTESI ANTONIA
Data: 2026.02.04 15:47:09 +01'00'

BANCA D'ITALIA
EUROSISTEMA

PROVVEDIMENTO DELLA BANCA D'ITALIA

Disposizioni di vigilanza per gli istituti di pagamento e gli istituti di moneta elettronica

LA BANCA D'ITALIA

Visto l'articolo 114-*quaterdecies*, comma 2, del decreto legislativo 1° settembre 1993, n. 385, Testo Unico delle leggi in materia bancaria e creditizia (di seguito, TUB), in base al quale la Banca d'Italia detta disposizioni di carattere generale aventi ad oggetto, in particolare, il governo societario, l'organizzazione amministrativa e contabile e i controlli interni degli istituti di pagamento;

Visto l'articolo 114-*quinquies*.2, comma 2, TUB, in base al quale la Banca d'Italia detta disposizioni di carattere generale aventi ad oggetto, in particolare, il governo societario, l'organizzazione amministrativa e contabile e i controlli interni degli istituti di moneta elettronica;

Tenuto conto del regolamento (UE) 2022/2554 del Parlamento europeo e del Consiglio del 14 dicembre 2022, relativo alla resilienza operativa digitale per il settore finanziario (DORA), e dei relativi atti delegati;

Tenuto conto della direttiva (UE) 2022/2556 del Parlamento europeo e del Consiglio del 14 dicembre 2022 (direttiva DORA), recante modifiche, tra l'altro, alla direttiva 2015/2366/UE sui servizi di pagamento nel mercato interno (PSD2);

Tenuto conto degli Orientamenti dell'Autorità bancaria europea ("ABE") dell'11 febbraio 2025 (EBA/GL/2025/02), recanti modifiche agli Orientamenti sulla gestione dei rischi relativi alle tecnologie dell'informazione e di sicurezza del 28 novembre 2019 (EBA/GL/2019/04);

Considerata l'esigenza di modificare la disciplina applicativa degli istituti di pagamento e di moneta elettronica;

EMANA

Il presente provvedimento che modifica le "Disposizioni di vigilanza per gli istituti di pagamento e gli istituti di moneta elettronica" del 17 maggio 2016 per assicurare un riordino della disciplina sui sistemi informativi e gestione dei rischi operativi e di sicurezza alla luce delle previsioni del Regolamento DORA e dei relativi atti delegati, in un'ottica di chiarezza del complessivo quadro normativo, nonché per dare attuazione all'articolo 7 della direttiva (UE) 2022/2556 ("Direttiva DORA"), recante modifiche alla PSD2, e 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.

Le modifiche, ivi incluse quelle relative a interventi di raccordo, riguardano: il Capitolo I, Sezioni I (fonti normative) e II (definizioni); il Capitolo VI, Sezioni I, II, IV, e Allegati A, B, C, D, E.

Le modifiche sono di mero adeguamento ad atti di altre Autorità direttamente applicabili o vincolanti (*i.e.*, Regolamento DORA e relativi atti delegati; Direttiva DORA) e pertanto, in linea con quanto previsto nel Regolamento della Banca d'Italia sugli atti di natura normativa o di contenuto generale, non sono state sottoposte a consultazione pubblica e ad analisi di impatto della regolamentazione (AIR).

Con il presente provvedimento è abrogato il seguente procedimento amministrativo:

- divieto di esternalizzazione di funzioni operative relative ai servizi di pagamento o all'emissione di moneta elettronica nonché al sistema dei controlli interni o del sistema informativo o componenti critiche dello stesso.

Le nuove disposizioni entrano in vigore il giorno successivo a quello di pubblicazione nella Gazzetta Ufficiale della Repubblica Italiana.

Il presente provvedimento è pubblicato sul sito *web* della Banca d'Italia.

Roma, 3 febbraio 2026

IL GOVERNATORE
Fabio Panetta

CAPITOLO I
DISPOSIZIONI GENERALI

SEZIONE I
FONTI NORMATIVE

Gli istituti di pagamento sono regolati:

- dalla direttiva 2015/2366/UE, del 25 novembre 2015, relativa ai servizi di pagamento nel mercato interno;
- dal Titolo V–*ter* del decreto legislativo 1° settembre 1993, n. 385, recante il Testo Unico delle leggi in materia bancaria e creditizia (di seguito, TUB) e successive modifiche.

Gli istituti di moneta elettronica sono regolati:

- dalla direttiva comunitaria 2009/110/CE, del 16 settembre 2009, concernente l'avvio, l'esercizio e la vigilanza prudenziale dell'attività degli istituti di moneta elettronica e successive modifiche;
- dal Titolo V–*bis* del TUB.

La materia è inoltre direttamente regolata dai seguenti regolamenti della Commissione europea recanti le norme tecniche di regolamentazione in materia di:

- cooperazione tra le autorità competenti dello stato d'origine e dello stato ospitante per la vigilanza sugli istituti di pagamento su base transfrontaliera ai sensi dell'articolo 29, paragrafo 6, della direttiva 2015/2366/UE (PSD2);
- requisiti tecnici per lo sviluppo, la gestione e la manutenzione del registro elettronico centrale e accesso alle informazioni ivi contenute, ai sensi dell'articolo 15, paragrafo 4, della direttiva 2015/2366/UE (PSD2);
- dettagli e struttura delle informazioni che le autorità competenti inseriscono nei registri pubblici e notificano all'EBA ai sensi dell'articolo 15, paragrafo 5, della direttiva 2015/2366/UE (PSD2);
- punti di contatto centrale ai sensi dell'articolo 29, paragrafo 5, della direttiva 2015/2366/UE (PSD2);
- cooperazione e scambio di informazioni tra autorità competenti in relazione all'esercizio del diritto di stabilimento e della libera prestazione dei servizi degli istituti di pagamento ai sensi dell'articolo 28, paragrafo 5, della direttiva 2015/2366/UE (PSD2);

- autenticazione forte del cliente e standard aperti di comunicazione comuni e sicuri ai sensi dell'articolo 98 della direttiva 2015/2366/UE (PSD2);

Rilevano inoltre i seguenti provvedimenti:

- Regolamento (UE) in materia di requisiti di capitale per le banche e le imprese di investimento n. 575/2013;
- Regolamento (UE) 2022/2554 relativo alla resilienza operativa digitale per il settore finanziario (DORA);
- Regolamento delegato (UE) 2024/1774, che integra il regolamento (UE) 2022/2554 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;
- Regolamento delegato (UE) 2024/1773, che integra il regolamento (UE) 2022/2554 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;
- Regolamento delegato (UE) 2024/1772, 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;
- Regolamento delegato (UE) 2025/301, che integra il regolamento (UE) 2022/2554 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;
- Regolamento di esecuzione (UE) 2025/302, che stabilisce norme tecniche di attuazione per l'applicazione del regolamento (UE) 2022/2554 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;
- decreto legislativo 21 novembre 2007, n. 231, che detta disposizioni in materia di prevenzione dell'uso del sistema finanziario a scopo di riciclaggio dei proventi di attività criminose e di finanziamento al terrorismo e successive modifiche, nonché le relative disposizioni di attuazione;
- decreto legislativo 27 gennaio 2010, n. 11, che detta disposizioni di attuazione della direttiva 2007/64/CE relativa ai servizi di

pagamento nel mercato interno e successive, nonché le relative disposizioni di attuazione;

- decreto legislativo 13 agosto 2010, n. 141, che detta disposizioni di attuazione della direttiva 2008/48/CE, relativa ai contratti di credito ai consumatori, nonché modifiche del titolo V, VI, e VI-*bis* del TUB in merito alla disciplina dei soggetti operanti nel settore finanziario, degli agenti in attività finanziaria e dei mediatori creditizi, e successive modifiche;
- decreto-legge 6 dicembre 2011, n. 201, convertito con modificazioni dalla legge 22 dicembre 2011, n. 214, che detta disposizioni in materia di divieto di assumere o esercitare cariche tra imprese o gruppi di imprese concorrenti operanti nei mercati del credito, assicurativo e finanziario (c.d. divieto di *interlocking*);
- decreto legislativo 16 aprile 2012, n. 45, che detta disposizioni di attuazione della direttiva 2009/110/CE, concernente l'avvio, l'esercizio e la vigilanza prudenziale dell'attività degli istituti di moneta elettronica, che modifica le direttive 2005/60/CE e 2006/48/CE e che abroga la direttiva 2000/46/CE;
- decreto del Ministro del tesoro, del bilancio e della programmazione economica n. 144/1998, recante norme per la determinazione dei requisiti di onorabilità dei partecipanti al capitale sociale, applicabile agli istituti di pagamento e agli istituti di moneta elettronica in base agli articoli 114-*novies*, comma 1, lett. e) e 114-*undecies* del TUB, per quanto riguarda gli istituti di pagamento, e 114-*quinquies*, comma 1, lett. e) e 114-*quinquies* 3 del TUB per quanto riguarda gli istituti di moneta elettronica;
- decreto del Ministro del tesoro, del bilancio e della programmazione economica n. 169/2020, recante norme in materia di requisiti e criteri di idoneità allo svolgimento dell'incarico degli esponenti aziendali delle banche, degli intermediari finanziari, dei confidi, degli istituti di moneta elettronica, degli istituti di pagamento e dei sistemi di garanzia dei depositanti;
- 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;
- Orientamenti sui criteri per stabilire l'importo monetario minimo dell'assicurazione per la responsabilità civile professionale o analoga garanzia a norma dell'articolo 5, paragrafo 4, della

direttiva 2015/2366/UE (EBA/GL/2017/08), emanati dall'EBA il 12 settembre 2017;

- Orientamenti sulle informazioni che devono essere fornite per ottenere l'autorizzazione degli istituti di pagamento e degli istituti di moneta elettronica, nonché per la registrazione dei prestatori di servizi di informazione sui conti ai sensi dell'articolo 5, paragrafo 5, della direttiva 2015/2366/UE (EBA/GL/2017/09), emanati dall'EBA l'8 novembre 2017;
- 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 emendati l'11 febbraio 2025 (EBA/GL/2025/02);
- Orientamenti sulle condizioni per beneficiare dell'esenzione dal meccanismo di emergenza a norma dell'articolo 33, paragrafo 6, del regolamento (UE) 389/2018 (norme tecniche di regolamentazione per l'autenticazione forte del cliente e gli standard aperti di comunicazione comuni e sicuri) (EBA/GL/2018/07), emanati dall'EBA il 4 dicembre 2018;
- Provvedimento della Banca d'Italia del 21 luglio 2021, Regolamento recante l'individuazione dei termini e delle unità organizzative responsabili dei procedimenti amministrativi e delle fasi procedimentali di competenza della Banca d'Italia e della Unità di informazione finanziaria per l'Italia, ai sensi degli articoli 2 e 4 della legge 7 agosto 1990, n. 241, e successive modificazioni;
- Provvedimento della Banca d'Italia del 29 luglio 2009, in materia di trasparenza delle operazioni e dei servizi finanziari, e successive modifiche;
- Provvedimento della Banca d'Italia del 18 dicembre 2012 recante le "Disposizioni di vigilanza in materia di sanzioni e procedura sanzionatori amministrativa" e successive modifiche;
- Provvedimento della Banca d'Italia del 5 maggio 2021 recante le "Disposizioni di vigilanza in materia di procedura di valutazione dell'idoneità degli esponenti di banche, intermediari finanziari, istituti di moneta elettronica, istituti di pagamento e sistemi di garanzia dei depositanti";
- Provvedimento della Banca d'Italia del 26 ottobre 2021 recante le "Disposizioni sulle informazioni e i documenti da trasmettere per la presentazione dell'istanza di autorizzazione all'acquisizione di partecipazioni qualificate in banche, intermediari ex art. 106 del TUB, IMEL, IP, SGR, SICAV e SICAF;
- Provvedimento della Banca d'Italia del 26 luglio 2022 recante le "Disposizioni in materia di assetti proprietari di banche e altri intermediari".

Si tiene conto anche delle seguenti *Opinion* emanate dall'ABE:

- l'*Opinion on the implementation of the RTS on SCA and CSC*, del 13 giugno 2018;
- l'*Opinion on the use of eIDAS certificates under the RTS on SCA and CSC*, del 10 dicembre 2018;
- l'*Opinion on the elements of strong customer authentication under PSD2*, del 21 giugno 2019;
- l'*Opinion on obstacles to the provision of third-party provider services under the Payment Services Directive* (EBA/OP/2020/10), del 4 giugno 2020.

Viene altresì in rilievo la Comunicazione della Banca d'Italia del 30 dicembre 2024 sul Regolamento DORA.

SEZIONE II
DEFINIZIONI

Ai fini della presente disciplina si intende per:

- *"EBA"*: *European Banking Authority* – Autorità bancaria europea, istituita con il Regolamento (UE) n. 1093/2010 del Parlamento europeo e del Consiglio, del 24 novembre 2010;
- *"agente"*: il soggetto di cui all'art. 128-*quater* del TUB;
- *"clienti/clientela"*: una persona fisica o giuridica che si avvale di un servizio di pagamento in qualità di pagatore o di beneficiario o di entrambi ovvero la persona fisica o giuridica che detiene la moneta elettronica*;*
- *"conto di pagamento"*: un conto detenuto a nome di uno o più clienti che è utilizzato esclusivamente per l'esecuzione delle operazioni di pagamento;
- *"controllo":* le fattispecie previste dall'art. 23 del TUB;
- "*CRR*": il Regolamento (UE) n. 575/2013;
- "*dati sensibili relativi ai pagamenti*": dati di cui all'articolo 1, comma 2, lett. q-*quater*) del d.lgs. n. 11/2010;
- *"depositari abilitati"*: le banche centrali, le banche italiane, le banche dell'Unione europea e le banche di Stati terzi;
- "*DORA*": il Regolamento (UE) 2022/2554
- *"esponenti aziendali"*: i soggetti che svolgono funzioni di amministrazione, direzione e controllo, comunque siano denominate le cariche;
- *"gruppo di appartenenza dell'istituto di pagamento o dell'istituto di moneta elettronica"*: l'insieme delle società italiane o estere che, ai sensi dell'art. 2359 del codice civile:
  1. controllano l'istituto di pagamento o l'istituto di moneta elettronica;
  2. sono controllati dall'istituto di pagamento o dall'istituto di moneta elettronica;
  3. sono controllati dallo stesso soggetto che controlla l'istituto di pagamento o l'istituto di moneta elettronica;
- *"istituti di moneta elettronica":* gli istituti di cui all'1, co. 2, lett. h-*bis*), del TUB;
- *"istituti di moneta elettronica dell'Unione europea":* gli istituti di cui all'1, co. 2, lett. h-*ter*), del TUB; gli istituti di cui all'1, co. 2, lett. h-*bis*.1) del TUB;

- "*istituti di pagamento*": gli istituti di cui all'art. 1, co. 2, lett. h-*sexies*), del TUB;
- "*istituti di pagamento dell'Unione europea*": gli istituti di cui all'1, co. 2, lett. h-*septies*), del TUB;
- "*istituto o istituti*"*:* l'istituto di moneta elettronica e l'istituto di pagamento italiano;
- "*istituto dell'Unione europea*"*:* l'istituto di moneta elettronica e l'istituto di pagamento aventi sede legale e amministrazione centrale in uno stesso Stato dell'Unione europea diverso dall'Italia;
- "*organo con funzione di supervisione strategica*": l'organo aziendale a cui - ai sensi del codice civile o per disposizione statutaria - sono attribuite funzioni di indirizzo della gestione dell'impresa, mediante, tra l'altro, esame e delibera in ordine ai piani industriali o finanziari ovvero alle operazioni strategiche;
- "*organo con funzione di gestione*": l'organo aziendale o i componenti di esso a cui - ai sensi del codice civile o per disposizione statutaria - spettano o sono delegati compiti di gestione corrente, intesa come attuazione degli indirizzi deliberati nell'esercizio della funzione di supervisione strategica. Il direttore generale rappresenta il vertice della struttura interna e come tale partecipa alla funzione di gestione;
- "*organo con funzione di controllo*": il collegio sindacale, il consiglio di sorveglianza o il comitato per il controllo sulla gestione;
- "*organi aziendali*": il complesso degli organi con funzioni di supervisione strategica, di gestione e di controllo. La funzione di supervisione strategica e quella di gestione attengono, unitariamente, alla gestione dell'impresa e possono quindi essere incardinate nello stesso organo aziendale. Nei sistemi dualistico e monistico, in conformità delle previsioni legislative, l'organo con funzione di controllo può svolgere anche quella di supervisione strategica;
- "*partecipazione*": ai sensi dell'articolo 1, comma 2, lett. h-*quater,* del TUB, le azioni, le quote e gli altri strumenti finanziari che attribuiscono diritti amministrativi o comunque i diritti previsti dall'articolo 2351, ultimo comma, del codice civile;
- "*partecipazione indiretta*": le partecipazioni acquisite o comunque possedute per il tramite di società controllate, di società fiduciarie o per interposta persona;
- "*partecipazione qualificata*": la partecipazione non inferiore al 10 per cento del capitale sociale o dei diritti di voto, oppure che comporti la possibilità di esercitare un'influenza notevole o il controllo sulla gestione dell'impresa partecipata;

- "*prestatori del servizio di disposizione di ordini di pagamento*"*:* gli istituti di pagamento autorizzati a prestare esclusivamente il servizio di cui all'art. 1, comma 2, lett. h-*septies*.1) n. 7, del TUB;
- "*prestatori del servizio di informazione sui conti*"*:* gli istituti di pagamento autorizzati a prestare esclusivamente il servizio di cui all'art. 1, comma 2, lett. h-*septies*.1) n. 8, del TUB;
- "*punto di contatto centrale*": il soggetto o la struttura di cui all'art. 1, co. 2, lett. i), del TUB;
- "*rischi operativi*": il rischio di perdite derivanti dalla inadeguatezza o dalla disfunzione di procedure, risorse umane e sistemi interni, oppure da eventi esogeni. È compreso il rischio legale, ossia il rischio di perdite derivanti da violazioni di leggi o regolamenti, da responsabilità contrattuale o extra-contrattuale ovvero da altre controversie;
- "*risk appetite (obiettivo di rischio o propensione al rischio)*": il livello complessivo e le tipologie di rischio che gli istituti sono disposti ad assumere per conseguire gli obiettivi strategici che si sono prefissati, in funzione della loro capacità di tollerare il rischio, in linea con il proprio modello di business;
- *"soggetti convenzionati con gli istituti di moneta elettronica"***:** le persone fisiche o giuridiche che, ai sensi dell'art. 114-*bis*.1 del TUB, distribuiscono o rimborsano la moneta elettronica per conto di un istituto di moneta elettronica;
- *"servizi di pagamento*": i servizi indicati nell'art. 1, comma 2, lett. h-*septies*.1), del TUB ([1]);
- *"stretti legami"*: le fattispecie riportate nell'art. 1, comma 2, lett. h), del TUB;
- *"titoli di debito qualificati"*: i titoli di debito inclusi nella tabella di cui all'articolo 336, paragrafo 1, del CRR, per i quali è prevista una ponderazione pari o inferiore all'1,6 per cento ad esclusione delle "altre posizioni qualificate" come definite dal paragrafo 4 del medesimo articolo del CRR.

Ove non diversamente specificato, ai fini delle presenti disposizioni valgono le altre definizioni contenute nel TUB e nel d.lgs. 27 gennaio 2010, n. 11.

[*omissis*]

([1]) Resta fermo quanto previsto dall'art. 2, comma 2, del d.lgs. 27 gennaio 2010, n. 11.

CAPITOLO VI
ORGANIZZAZIONE AMMINISTRATIVA E CONTABILE E CONTROLLI INTERNI

SEZIONE I
PRINCIPI GENERALI

1. Premessa

Il presente Capitolo attua quanto previsto dagli articoli 114-*quaterdecies*, comma 2, e 114-*quinquies*.2, comma 2, TUB, in base ai quali la Banca d'Italia detta disposizioni di carattere generale aventi ad oggetto il governo societario, l'organizzazione amministrativa e contabile e i controlli interni degli istituti.

Gli istituti applicano le disposizioni del presente Capitolo in maniera proporzionata alla dimensione e alla complessità dell'attività svolta nonché alla tipologia e alla gamma dei servizi prestati.

Resta fermo quanto previsto da DORA relativamente ai sistemi informativi e alla gestione dei rischi informatici.

2. Requisiti generali di organizzazione

La gestione aziendale sana e prudente, l'affidabilità e l'efficienza dei servizi di pagamento prestati e dell'attività di emissione di moneta elettronica dipendono anche da un assetto organizzativo adeguato alla dimensione, alla complessità e alla vocazione operativa dell'istituto.

In tal senso, gli istituti definiscono e applicano:

a) dispositivi di governo societario solidi, che comprendono processi decisionali e una struttura organizzativa che specifichino in forma chiara e documentata i rapporti gerarchici e la suddivisione delle funzioni;

b) politiche di governo e procedure per la gestione e il controllo di tutti i rischi aziendali e un efficace sistema dei controlli interni;

c) misure che assicurino che il personale e gli agenti dell'istituto o i soggetti convenzionati dall'istituto di moneta elettronica conoscano le procedure da seguire per il corretto esercizio delle proprie funzioni;

d) politiche e procedure volte ad assicurare che il personale, gli agenti e i soggetti convenzionati siano provvisti delle qualifiche, delle conoscenze e delle competenze necessarie per l'esercizio delle responsabilità loro attribuite;

e) efficaci flussi interni di comunicazione delle informazioni;

f) sistemi e procedure diretti a conservare registrazioni adeguate e ordinate dei fatti di gestione dell'istituto e della sua organizzazione interna;

g) criteri e procedure volti a garantire che l'affidamento al personale, agli agenti o ai soggetti convenzionati di funzioni multiple non sia tale da impedire all'istituto di svolgere in modo adeguato e professionale una qualsiasi di tali funzioni;

h) politiche di governo e procedure per la gestione della sicurezza relativa alla prestazione dei servizi di pagamento e di emissione della moneta elettronica, inclusa la gestione degli incidenti relativi alla sicurezza e dei reclami dei clienti in materia;

i) procedure e sistemi idonei a: 1) tutelare la sicurezza, l'integrità e la riservatezza delle informazioni, tenendo conto della natura delle informazioni medesime; 2) archiviare e gestire i dati sensibili relativi ai pagamenti, con gli opportuni limiti di accesso; e 3) acquisire dati statistici relativi ai risultati della gestione, alle operazioni di pagamento effettuate e alle frodi ([1]);

j) politiche, sistemi, risorse e procedure per la continuità e la regolarità dei servizi, volte anche ad assicurare la regolare esecuzione delle operazioni di pagamento in corso e la chiusura dei contratti in essere in caso di cessazione dell'operatività.

k) politiche e procedure contabili che consentano di fornire tempestivamente alle autorità di vigilanza documenti che presentino un quadro fedele della posizione finanziaria ed economica e che siano conformi a tutti i principi e a tutte le norme anche contabili applicabili.

Gli istituti controllano e valutano con regolarità l'adeguatezza, l'efficacia e l'applicazione di tali requisiti organizzativi e adottano le misure adeguate per rimediare a eventuali carenze.

L'organo con funzione di controllo informa tempestivamente la Banca d'Italia di tutti gli atti o fatti, di cui venga a conoscenza nell'esercizio dei propri compiti, che possano costituire una irregolarità nella gestione o una violazione delle norme che disciplinano l'attività dell'istituto.

Negli allegati A e C si definiscono i requisiti, di carattere minimo, a cui il sistema di governo, il sistema dei controlli interni, i sistemi informativi e la gestione dei rischi operativi e di sicurezza si devono uniformare.

Le presenti disposizioni formano parte integrante del complesso di norme concernenti gli assetti organizzativi, governo e di controllo degli intermediari, quali i controlli sugli assetti proprietari, i requisiti degli esponenti aziendali, gli obblighi di trasparenza e correttezza delle relazioni tra intermediari e clienti, la prevenzione dei fenomeni di usura, riciclaggio e del finanziamento al terrorismo.

([1]) Non sono tenuti all'adozione di sistemi e procedure finalizzati alla registrazione e conservazione dei dati statistici relativi alle frodi, gli istituti che svolgono in via esclusiva il servizio di informazione sui conti.

SEZIONE II

ESTERNALIZZAZIONE DI FUNZIONI OPERATIVE E ACCORDI PER LA DISTRIBUZIONE E IL RIMBORSO DELLA MONETA ELETTRONICA

1. Esternalizzazione di funzioni operative

Fermo restando quanto previsto da DORA, l'istituto che intende esternalizzare funzioni operative relative ai servizi di pagamento o all'emissione di moneta elettronica o importanti (es. relative al sistema dei controlli interni) ne informa la Banca d'Italia dopo l'approvazione da parte degli organi competenti e prima di dare corso all'esternalizzazione. È facoltà per gli istituti avviare un confronto preliminare con la Banca d'Italia sui progetti di esternalizzazione più rilevanti e/o innovativi, prima di conferire l'incarico. Restano in ogni caso fermi tutti i poteri, anche di intervento e sanzionatori, spettanti alla Banca d'Italia.

L'esternalizzazione di funzioni operative relative ai servizi di pagamento o all'emissione di moneta elettronica o importanti, tra cui i sistemi TIC (tecnologie dell'informazione e della comunicazione), non può mettere materialmente a repentaglio la qualità del controllo interno dell'istituto né impedire alla Banca d'Italia di controllare che gli istituti si conformino alle disposizioni loro applicabili (nell'allegato B sono riportati gli obblighi a carico dell'istituto in caso di esternalizzazione delle funzioni operative relative a servizi di pagamento, all'emissione di moneta elettronica o importanti diverse dai sistemi TIC; il ricorso a fornitori terzi di servizi TIC è disciplinato direttamente da DORA).

Gli istituti comunicano senza ritardo alla Banca d'Italia eventuali modifiche di rilievo delle informazioni relative ad accordi di esternalizzazione precedentemente comunicate.

1.1. Esternalizzazione di funzioni operative in altri Stati membri dell'Unione europea

L'istituto che intende per la prima volta prestare servizi di pagamento o emettere moneta elettronica in un altro Stato membro dell'Unione europea in virtù del diritto di stabilimento o della libera prestazione dei servizi e intende esternalizzare funzioni operative relative ai servizi di pagamento o all'emissione di moneta elettronica nello Stato membro ospitante ne informa la Banca d'Italia nell'ambito delle comunicazioni previste dal cap. VII delle presenti disposizioni. Si applica quanto previsto nell'allegato B.

2. Accordi per la distribuzione e il rimborso della moneta elettronica

L'istituto di moneta elettronica che intende avvalersi di soggetti convenzionati per la distribuzione e il rimborso della moneta elettronica trasmette alla Banca d'Italia, dopo l'approvazione da parte degli organi

competenti e prima di dare corso all'accordo, uno schema generale di accordo redatto secondo le indicazioni contenute nell'allegato B. I singoli accordi di convenzionamento redatti secondo lo schema non sono oggetto di comunicazione specifica alla Banca d'Italia. Gli istituti di moneta elettronica conservano la relativa documentazione e tengono apposite evidenze aggiornate di tutti i soggetti convenzionati di cui si avvalgono a disposizione della Banca d'Italia.

Gli istituti di moneta elettronica comunicano alla Banca d'Italia eventuali variazioni significative apportate allo schema contrattuale di convenzionamento.

SEZIONE III

RELAZIONE SULLA STRUTTURA ORGANIZZATIVA E DOCUMENTO DESCRITTIVO DEI SERVIZI DI PAGAMENTO, DELLA MONETA ELETTRONICA E DELLE RELATIVE CARATTERISTICHE

L'istituto invia alla Banca d'Italia entro il 30 aprile di ogni anno una relazione sulla struttura organizzativa redatta secondo lo schema indicato nell'allegato D e un documento descrittivo dei servizi di pagamento e/o dell'attività di emissione di moneta elettronica e delle relative caratteristiche, redatto secondo lo schema indicato nell'allegato E.

Il contenuto delle informazioni contenute nei documenti redatti secondo l'allegato E deve essere coerente con le disposizioni europee in materia direttamente applicabili, nonché con quelle emanate dalla Banca d'Italia ai sensi dell'art. 146 del TUB, al fine di assicurare l'affidabilità e l'efficienza dei servizi di pagamento offerti e della moneta elettronica emessa.

La relazione e/o i documenti descrittivi non sono dovuti qualora non siano intervenute variazioni rispetto alle informazioni comunicate con l'ultima relazione e/o documenti descrittivi trasmessi.

SEZIONE IV

PROCEDIMENTI AMMINISTRATIVI

Si indicano di seguito, a soli fini riepilogativi, i procedimenti amministrativi, e le corrispondenti unità organizzative responsabili, rilevanti ai sensi del presente Capitolo:

- *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 (Servizio Rapporti Istituzionali di Vigilanza);
- *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 (Servizio Rapporti Istituzionali di Vigilanza).

Allegato A

Ruolo degli organi aziendali e sistema dei controlli interni

1. RUOLO DEGLI ORGANI AZIENDALI

Gli organi aziendali assumono un ruolo fondamentale per la definizione di un sistema organizzativo e dei controlli interni adeguato e efficace.

La composizione degli organi aziendali, per numero e professionalità, assicura l'efficace assolvimento dei loro compiti ed è calibrata in funzione delle caratteristiche operative e dimensionali dell'istituto. La ripartizione di competenze tra gli organi aziendali è definita in modo chiaro e garantisce una costante dialettica interna, evitando sovrapposizioni di competenze che possano incidere sulla funzionalità aziendale.

Il presidente dell'organo con funzione di supervisione strategica promuove la dialettica interna e l'effettivo funzionamento del sistema di governo societario; lo stesso non riveste un ruolo esecutivo né svolge, neppure di fatto, funzioni gestionali.

L'operato degli organi aziendali è documentato, per consentire un controllo sugli atti gestionali e sulle decisioni assunte; a questo fine, i verbali delle riunioni degli organi aziendali illustrano in modo dettagliato il processo di formazione delle decisioni e le loro motivazioni.

In questo ambito, l'organo con funzione di supervisione strategica:

a) definisce e approva gli obiettivi, le strategie, il profilo e i livelli di rischio dell'istituto, definendo le politiche aziendali e quelle del sistema dei controlli interni; ne verifica periodicamente la corretta attuazione e coerenza con l'evoluzione dell'attività aziendale;

b) approva le politiche di gestione dei rischi (operativi, di credito, di liquidità, ecc.), nonché le relative procedure e modalità di rilevazione e controllo;

c) approva e verifica periodicamente, con cadenza almeno annuale, la politica per il governo e la gestione dei rischi di sicurezza;

d) approva i criteri in base ai quali sono scelti gli strumenti finanziari in cui investire i fondi ricevuti dalla clientela;

e) approva i processi relativi alla prestazione dei servizi di pagamento e, per gli istituti di moneta elettronica, all'attività di emissione di moneta elettronica e ne verifica periodicamente l'adeguatezza;

f) verifica che l'assetto delle funzioni aziendali di controllo sia definito in coerenza con il principio di proporzionalità e con gli indirizzi

strategici e che le funzioni medesime siano dotate di risorse qualitativamente e quantitativamente adeguate;

g) approva la struttura organizzativa e l'attribuzione di compiti e responsabilità e ne verifica, con cadenza almeno annuale, l'adeguatezza; in questo ambito, si assicura, tra l'altro, che:

   - i compiti e le responsabilità, formalizzati in un apposito regolamento interno, siano allocati in modo chiaro e appropriato e che siano separate le funzioni operative da quelle di controllo;
   - gli agenti e i soggetti convenzionati siano dotati di meccanismi di controllo interno adeguati al fine di conformarsi ai rispettivi obblighi in materia di lotta al riciclaggio e finanziamento al terrorismo;
   - l'esternalizzazione delle funzioni aziendali sia coerente con le strategie dell'istituto e i livelli di rischio definiti;
   - sia garantita la separatezza amministrativo-contabile tra l'attività di prestazione di servizi di pagamento e di emissione di moneta elettronica rispetto alle altre attività eventualmente svolte dall'istituto;

h) verifica che il sistema di flussi informativi sia adeguato, completo e tempestivo;

i) stabilisce i principi e gli obiettivi della gestione della continuità operativa.

L'organo con funzione di gestione:

a) attua le politiche aziendali e quelle del sistema dei controlli interni, definite dall'organo con funzione di supervisione strategica;

b) verifica nel continuo l'adeguatezza del sistema dei controlli interni, provvedendo al suo adeguamento alla luce dell'evoluzione dell'operatività;

c) definisce i flussi informativi volti ad assicurare agli organi aziendali la conoscenza dei fatti di gestione rilevanti;

d) definisce in modo chiaro i compiti e le responsabilità delle strutture e delle funzioni aziendali, in modo, tra l'altro, di prevenire potenziali conflitti di interesse e di assicurare che le strutture siano dirette da personale qualificato in relazione alle attività da svolgere;

e) in coerenza con le politiche di governo dei rischi, definisce e attua il processo di gestione dei rischi aziendali;

f) definisce e attua gli standard per la gestione dei dati sensibili relativi ai pagamenti e le procedure di gestione della sicurezza, assicurandone la coerenza con la politica di governo e gestione della sicurezza e la propensione al rischio dell'istituto;

g) definisce e attua la politica aziendale in materia di esternalizzazione di funzioni aziendali;

h) assicura che il personale e gli agenti utilizzati per la prestazione di servizi di pagamento, nonché il personale e i soggetti convenzionati utilizzati per la distribuzione e il rimborso della moneta elettronica, siano adeguatamente formati con riferimento ai prodotti commercializzati e ai servizi prestati, agli adempimenti in materia di prevenzione dei fenomeni di riciclaggio e di finanziamento al terrorismo, alla normativa in materia di trasparenza;

i) assicura che le politiche aziendali e le procedure siano tempestivamente comunicate a tutto il personale interessato;

j) adotta tempestivamente le misure necessarie nel caso in cui emergano carenze o anomalie dall'insieme delle verifiche svolte sul sistema dei controlli;

k) definisce il piano aziendale di emergenza e continuità operativa e ne promuove il controllo periodico (di norma annuale) e l'aggiornamento.

L'organo con funzione di controllo, nel rispetto delle attribuzioni degli altri organi e collaborando con essi:

a) vigila sull'osservanza delle norme di legge, regolamentari e statutarie, sulla corretta amministrazione, sull'adeguatezza degli assetti organizzativi e contabili dell'istituto;

b) vigila sulla funzionalità del complessivo sistema dei controlli interni e accerta l'efficacia delle strutture e funzioni coinvolte nel sistema dei controlli e l'adeguato coordinamento tra le stesse;

c) valuta il grado di adeguatezza e il regolare funzionamento delle principali aree organizzative;

d) promuove interventi correttivi delle carenze e delle irregolarità rilevate.

L'organo con funzione di controllo può avvalersi per lo svolgimento delle proprie funzioni di tutte le unità delle strutture organizzative che assolvono funzioni di controllo e, in particolare, della funzione di revisione interna. L'attività di controllo può determinare la formulazione di osservazioni e proposte di modifica volte alla rimozione di eventuali anomalie riscontrate. Di tali osservazioni e proposte, nonché della successiva attività di verifica dell'organo con funzione di controllo sull'attuazione di eventuali provvedimenti, è conservata adeguata evidenza.

L'organo con funzione di controllo mantiene il coordinamento con le funzioni di controllo interno e con il soggetto incaricato della revisione legale dei conti, al fine di incrementare il grado di conoscenza sull'andamento della gestione aziendale, avvalendosi anche delle risultanze degli accertamenti effettuati da tali unità operative.

L'interazione tra l'attività dell'organo con funzione di controllo e l'attività di vigilanza contribuisce al rafforzamento del complessivo sistema di supervisione sull'istituto.

2. SISTEMA DEI CONTROLLI INTERNI

Premessa

Il sistema dei controlli interni è costituito dall'insieme delle risorse, delle strutture organizzative, delle regole e delle procedure per assicurare il conseguimento delle strategie aziendali e dell'efficacia ed efficienza dei processi aziendali, della salvaguardia del valore delle attività e della protezione dalle perdite, dell'affidabilità e integrità delle informazioni contabili e gestionali, della conformità delle operazioni con la legge, la normativa di vigilanza e di sorveglianza sul sistema dei pagamenti e le disposizioni interne dell'istituto.

Nel sistema dei controlli interni rientrano le strategie, le politiche, i processi e i meccanismi riguardanti la gestione dei rischi a cui l'istituto è o potrebbe essere esposto e per determinare e controllare il livello di rischio tollerato. In questo contesto, la gestione dei rischi include le funzioni di individuazione, assunzione, misurazione, sorveglianza e attenuazione dei rischi.

Per gli istituti, in relazione alla prestazione dei servizi di pagamento e all'emissione di moneta elettronica, assumono particolare rilievo i rischi operativi e di sicurezza e quelli di natura legale e reputazionale, che possono discendere dai rapporti con la clientela. A tal fine, gli istituti sono tenuti, tra l'altro, ad approntare specifici presidi organizzativi per assicurare il rispetto delle prescrizioni normative e di autoregolamentazione, pianificando, in tale ambito, specifici controlli sulle succursali, sugli agenti e sui soggetti convenzionati.

Gli istituti valutano attentamente le implicazioni derivanti dai mutamenti dell'operatività aziendale (ingresso in nuovi mercati o in nuovi settori operativi, offerta di nuovi prodotti, utilizzo di canali distributivi innovativi, partecipazione a nuovi sistemi di pagamento), con preventiva individuazione dei rischi e definizione di procedure di controllo adeguate, approvate dagli organi aziendali competenti.

Nella predisposizione dei presidi organizzativi, gli istituti tengono conto dell'esigenza di prevenire fenomeni di riciclaggio e di finanziamento al terrorismo.

Tipologie di controllo

Si descrivono di seguito alcune tipologie di controllo, indipendentemente dalle strutture organizzative in cui sono collocate:

1) *controlli di linea* (c.d. *controlli di primo livello*), diretti ad assicurare il corretto svolgimento delle operazioni connesse con la prestazione dei servizi di pagamento e con l'emissione di moneta elettronica. Essi sono effettuati dalle stesse strutture operative (es. controlli di tipo gerarchico, sistematici e a campione), incorporati nelle procedure (anche automatizzate) ovvero eseguiti nell'ambito dell'attività di *back office*;

2) *controlli sulla gestione dei rischi e di conformità alle norme* (c.d. *controlli di secondo livello*) ([1]), che hanno l'obiettivo di assicurare: (i) il rispetto dei limiti assegnati alle varie funzioni operative; e (ii) la coerenza dell'operatività delle singole aree produttive con gli obiettivi di rischio-rendimento assegnati, nonché la conformità dell'operatività aziendale alle norme, incluse quelle di autoregolamentazione. Essi sono affidati a strutture diverse da quelle produttive; le funzioni di controllo concorrono alla definizione delle politiche di governo e del processo di gestione dei rischi aziendali;

3) *revisione interna* (*internal audit,* c.d. *controlli di terzo livello*). In tale ambito rientra la valutazione periodica della completezza, della funzionalità e dell'adeguatezza del sistema dei controlli interni, con cadenza prefissata in relazione alla natura e all'intensità dei rischi. L'attività è condotta da funzioni diverse e indipendenti da quelle produttive, anche attraverso verifiche *in loco.*

Ferma l'esigenza di gestire tutti i rischi aziendali, gli istituti, in considerazione della natura dell'attività svolta, prestano particolare attenzione ai rischi operativi e di sicurezza e al rischio di reputazione ([2]).

Pertanto, gli istituti:

- prestano particolare attenzione agli eventi di maggiore gravità e scarsa frequenza e individuano le varie forme e modalità con cui possono manifestarsi i rischi operativi e di sicurezza, in relazione alle specifiche caratteristiche organizzative ed operative;
- valutano i rischi operativi e di sicurezza e i rischi reputazionali, connessi con l'introduzione di nuovi prodotti, attività, reti distributive, processi e sistemi rilevanti e con la partecipazione, anche indiretta, a nuovi sistemi di pagamento;
- si dotano di piani di emergenza e di continuità operativa che assicurano la propria capacità di operare su base continuativa e di limitare le perdite operative in caso di gravi interruzioni dell'operatività.

Nel caso in cui gli istituti, nella prestazione dei servizi di pagamento, eroghino finanziamenti ai clienti, essi definiscono adeguati processi decisionali e operativi connessi con la gestione del rischio di credito ([3]).

L'attività di concessione di finanziamenti ha natura accessoria ai servizi di pagamento prestati: gli istituti adottano sistemi e procedure per monitorare

([1]) Tra le funzioni aziendali di controllo di secondo livello rientra la funzione di controllo a cui è attribuita la responsabilità della gestione e della sorveglianza dei rischi informatici come disciplinata dall'art. 6, paragrafo 4, del DORA ("funzione di controllo ICT")

([2]) Il rischio di reputazione può scaturire direttamente da determinati eventi o comportamenti (ad es. politiche commerciali percepite dalla clientela come poco attente ai propri interessi) o indirettamente da altre tipologie di rischio (operativo, credito, liquidità) rispetto alle quali gli effetti reputazionali possono amplificare l'impatto economico. Il rischio di reputazione può pertanto conseguire sia da comportamenti irregolari sia da errate percezioni da parte della clientela o del mercato.

([3]) Tale obbligo è previsto anche con riferimento all'attività di emissione e gestione di carte di credito con saldo mensile.

i finanziamenti e identificano criteri, di natura anche quantitativa, che tengano conto dei flussi di pagamento effettuati su base annuale.

Gli istituti hanno in ogni momento conoscenza della propria esposizione nei confronti di ogni cliente o gruppo di clienti connessi ([4]), anche al fine di procedere, se del caso, ad una tempestiva revisione delle linee di credito.

Poiché l'insolvenza di un grande prenditore può avere effetti di rilievo sulla solidità patrimoniale, gli istituti si dotano di regole volte ad assicurare la corretta rilevazione, valutazione della qualità e dell'andamento nel tempo delle esposizioni assunte nei confronti di un singolo cliente o gruppo di clienti connessi che siano di importo rilevante rispetto ai fondi propri. Gli istituti adottano misure adeguate a limitare o presidiare opportunamente i rischi derivanti dall'assunzione di esposizioni di importo rilevante nei confronti di singoli clienti o gruppi di clienti connessi.

Il processo riguardante l'erogazione del credito comprende le seguenti fasi: 1) istruttoria; 2) erogazione; 3) monitoraggio delle posizioni; 4) interventi in caso di anomalia; 5) revisione delle linee di credito. Il processo risulta dal regolamento interno ed è periodicamente sottoposto a verifica. Il regolamento, approvato dall'organo con funzione di gestione, definisce, tra l'altro: la documentazione minimale da acquisire per effettuare una adeguata valutazione del merito creditizio del prenditore; le eventuali deleghe in materia di erogazione del credito; le modalità di rinnovo degli affidamenti; le procedure e gli adempimenti riferiti alla fase di monitoraggio del credito nonché le modalità e i tempi di attivazione in caso di rilevazione di crediti anomali; criteri di classificazione, gestione e valutazione dei crediti anomali.

Tutti gli affidamenti sono concessi al termine di un procedimento istruttorio documentato, ancorché basato su procedure automatizzate.

([4]) A tali fini si identificano due tipologie di connessioni tra uno o più soggetti:

a) giuridica - se uno dei soggetti in esame ha, direttamente o indirettamente, un potere di controllo sull'altro o sugli altri;
b) economica - quando, indipendentemente dall'esistenza dei rapporti di controllo di cui alla lettera a), esistono, tra i soggetti considerati, legami tali che, con tutta probabilità, se uno di essi si trova in difficoltà finanziarie, in particolare difficoltà di raccolta di fondi o rimborso dei debiti, l'altro, o tutti gli altri, potrebbero incontrare analoghe difficoltà.

Con riferimento alla lettera a) il controllo sussiste – salvo che l'istituto dimostri il contrario – quando ricorre anche una sola delle seguenti circostanze:

1) uno dei soggetti in esame possiede - direttamente o indirettamente - più del 50% del capitale o delle azioni con diritto di voto di un altro dei soggetti in esame;
2) uno dei soggetti in esame possiede il 50% o meno del 50% del capitale o dei diritti di voto in un altro dei soggetti in esame ed è in grado di esercitare il controllo congiunto su di esso in virtù delle azioni e dei diritti posseduti, di clausole statutarie e di accordi con gli altri partecipanti.

Nell'ipotesi di cui al punto 2, ovvero indipendentemente da possessi azionari, costituisce indice di controllo la disponibilità di uno o più dei seguenti poteri: i) indirizzare l'attività di un'impresa in modo da trarne benefici; ii) decidere operazioni significative, quali ad esempio il trasferimento dei profitti e delle perdite; iii) nominare o rimuovere la maggioranza dei componenti degli organi amministrativi; iv) disporre della maggioranza dei voti negli organi amministrativi o della maggioranza dei voti nell'assemblea dei soci o in altro organo equivalente; v) coordinare la gestione di un'impresa con quella di altre imprese ai fini del perseguimento di uno scopo comune.

In caso di ricorso ad agenti per la prestazione di servizi di pagamento o, per i soli IMEL, a soggetti convenzionati per la distribuzione e il rimborso della moneta elettronica, gli istituti assicurano il rispetto delle proprie disposizioni interne da parte di questi soggetti, nonché delle disposizioni ad essi applicabili (ad esempio trasparenza, usura, antiriciclaggio, diritti e obblighi delle parti). Gli istituti effettuano controlli, *in loco* o a distanza, sulla rete con cadenza almeno annuale. Gli istituti assicurano altresì che siano resi riconoscibili all'utenza i soggetti di cui si avvalgono (agenti, soggetti convenzionati, punti operativi abilitati all'incasso ai sensi dell'art. 12, comma 4, del d.lgs. 141/2010).

Gli istituti controllano e gestiscono i rischi connessi con gli investimenti dei fondi ricevuti dai clienti in modo da assicurare la pronta disponibilità delle somme per l'esecuzione delle operazioni di pagamento. Essi approntano procedure operative volte ad assicurare il rispetto dei termini fissati dalla normativa per il deposito o l'investimento dei fondi e per la sistemazione di eventuali sbilanci tra valore di tali attività e fondi ricevuti ([5]).

Funzioni aziendali di controllo

Gli istituti istituiscono funzioni indipendenti di controllo di conformità alle norme, di gestione del rischio, e di revisione interna ([6]), in modo proporzionato alla dimensione e alla complessità dell'attività svolta nonché alla tipologia e alla gamma dei servizi di pagamento prestati.

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

a) tali funzioni dispongano dell'autorità, delle risorse e delle competenze necessarie per lo svolgimento dei loro compiti;

b) i responsabili non siano gerarchicamente subordinati ai responsabili delle funzioni sottoposte a controllo e siano nominati dall'organo con funzione di supervisione strategica, sentito l'organo con funzione di controllo. Essi riferiscono direttamente agli organi aziendali;

c) coloro che partecipano alle funzioni aziendali di controllo non partecipino direttamente alla prestazione dei servizi che essi sono chiamati a controllare. Ferma restando tale previsione, in applicazione del principio di proporzionalità, i responsabili delle funzioni di controllo possono avvalersi di soggetti aventi anche funzioni operative, incardinati in strutture aziendali diverse da quelle di controllo, a condizione che l'affidamento a tali soggetti di altri compiti oltre a quelli di controllo non impedisca loro di svolgere in modo adeguato e professionale i compiti di controllo;

d) le funzioni aziendali di controllo siano tra loro separate sotto un profilo organizzativo;

([5]) Gli istituti adottato, tra l'altro, presidi idonei a fronteggiare il rischio di disconoscimenti in relazione a operazioni di accreditamento della moneta elettronica o dei conti di pagamento via web, ad es. con addebito di carte di credito (fenomeni di *phishing*, ecc.).

([6]) Per la funzione di controllo a cui è attribuita la responsabilità della gestione e della sorveglianza dei rischi informatici, cfr. art. 6, paragrafo 4, del DORA

e) il metodo per la determinazione della remunerazione di coloro che partecipano alle funzioni aziendali di controllo non ne comprometta l'obiettività.

Gli istituti possono non applicare i requisiti di cui alla lett. d) del precedente capoverso, qualora dimostrino che, in applicazione del principio di proporzionalità, gli obblighi in questione non sono proporzionati ai rischi da essi assunti e che le funzioni di controllo continuano ad essere efficaci ([7]).

Le funzioni aziendali di controllo svolgono i compiti di seguito indicati.

La funzione di gestione del rischio:

a) collabora alla definizione delle politiche di governo e del processo di gestione del rischio e delle relative procedure e modalità di rilevazione e controllo, verificandone l'adeguatezza nel continuo;

b) verifica nel continuo l'adeguatezza del sistema di controllo dei rischi e ne verifica il rispetto da parte dell'istituto;

c) verifica l'adeguatezza e l'efficacia delle misure prese per rimediare alle carenze riscontrate nel sistema di controllo dei rischi.

La funzione di controllo di conformità (*compliance*) valuta l'adeguatezza delle procedure interne rispetto all'obiettivo di prevenire la violazione di leggi, regolamenti e norme di autoregolamentazione applicabili all'istituto; a questo fine:

a) identifica le norme applicabili all'istituto e ai servizi da esso prestati e ne misura/valuta l'impatto sui processi e procedure aziendali;

b) propone modifiche organizzative e procedurali volte ad assicurare adeguato presidio dei rischi di non conformità alle norme;

c) predispone flussi informativi diretti agli organi aziendali e alle altre funzioni aziendali di controllo;

d) verifica l'efficacia degli adeguamenti organizzativi suggeriti per la prevenzione del rischio di non conformità.

La funzione di revisione interna:

a) definisce e applica un piano di *audit*, approvato dall'organo con funzione di supervisione strategica, per l'esame e la valutazione dell'adeguatezza e dell'efficacia del sistema dei controlli interni, incluso il sistema per la gestione del rischio di sicurezza, e dei meccanismi adottati dagli agenti utilizzati per la prestazione dei servizi di pagamento e dai soggetti convenzionati per la distribuzione e il rimborso della moneta elettronica per conformarsi agli obblighi in materia di lotta al riciclaggio e finanziamento al terrorismo. Il piano di

([7]) Per la funzione di controllo a cui è attribuita la responsabilità della gestione e della sorveglianza dei rischi informatici resta fermo quanto previsto dall'art. 6, paragrafo 4, del DORA.

audit prevede, tra l'altro, specifici controlli sull'intera rete di succursali, agenti utilizzati per la promozione e conclusione dei contratti relativi alla prestazione dei servizi di pagamento e soggetti convenzionati per la distribuzione e il rimborso di moneta elettronica;

b) formula raccomandazioni agli organi aziendali basate sui risultati delle verifiche effettuate in base al piano di *audit* e ne verifica l'osservanza.

Le funzioni aziendali di controllo presentano agli organi aziendali, almeno una volta all'anno, relazioni sull'attività svolta e forniscono agli stessi organi consulenza per i profili che attengono ai compiti di controllo svolti.

Allegato B

Obblighi a carico degli istituti nel caso di esternalizzazione di funzioni operative relative ai servizi di pagamento, all'emissione di moneta elettronica o importanti.

Una funzione operativa si considera importante nel caso in cui un'anomalia nella sua esecuzione o la sua mancata esecuzione possano:

- mettere a repentaglio la capacità dell'istituto di continuare a conformarsi ai requisiti relativi alla sua autorizzazione o agli altri obblighi ad esso applicabili ai sensi delle presenti disposizioni;
- compromettere gravemente i suoi risultati finanziari o la solidità o la continuità dei suoi servizi di pagamento o dell'attività di emissione di moneta elettronica;
- costituire un pregiudizio per il regolare funzionamento del sistema dei pagamenti.

Gli istituti che esternalizzano funzioni operative relative a servizi di pagamento, all'emissione di moneta elettronica o importanti assicurano che:

a) l'esternalizzazione non determini la delega della responsabilità da parte degli organi aziendali;

b) non siano alterati il rapporto e gli obblighi dell'istituto nei confronti dei suoi clienti nella prestazione dei servizi di pagamento o nell'attività di emissione di moneta elettronica;

c) non sia messo a repentaglio il rispetto delle condizioni che l'istituto deve soddisfare per poter essere autorizzato alla prestazione dei servizi di pagamento o all'attività di emissione di moneta elettronica e per conservare tale autorizzazione.

In relazione a ciò, gli istituti, quando concludono o applicano accordi di esternalizzazione di funzioni operative relative a servizi di pagamento, di emissione di moneta elettronica o importanti, assicurano che siano soddisfatte le condizioni seguenti:

a) il fornitore di servizi disponga della competenza, della capacità e di qualsiasi autorizzazione richiesta dalla legge per esercitare le funzioni esternalizzate in maniera professionale e affidabile;

b) il fornitore di servizi presti i servizi esternalizzati in maniera efficace; a questo scopo l'istituto si dota di metodi per la valutazione del livello dei servizi di tale fornitore;

c) il fornitore sorvegli adeguatamente l'esecuzione delle funzioni esternalizzate e gestisca in modo appropriato i rischi connessi con l'esternalizzazione;

d) l'istituto conservi la competenza richiesta per controllare efficacemente le funzioni esternalizzate e per gestire i rischi connessi all'esternalizzazione e controlli tali funzioni e gestisca tali rischi; in tale ambito individua all'interno della propria organizzazione un responsabile del controllo delle funzioni esternalizzate ("referente per le attività esternalizzate");

e) il fornitore di servizi informi l'istituto di qualsiasi sviluppo che potrebbe incidere in modo rilevante sulla sua capacità di eseguire le funzioni esternalizzate in maniera efficace e in conformità con la normativa e i requisiti vigenti;

f) vi siano clausole risolutive espresse che consentano all'istituto di porre termine all'accordo di esternalizzazione in presenza di eventi che possano compromettere la capacità del fornitore di garantire il servizio ovvero quando si verifichi il mancato rispetto del livello di servizio concordato;

g) il fornitore di servizi collabori con le autorità di vigilanza per quanto riguarda le attività esternalizzate;

h) l'istituto, i suoi revisori contabili e le autorità di vigilanza abbiano effettivo accesso ai dati relativi alle attività esternalizzate e ai locali in cui opera il fornitore di servizi; le autorità di vigilanza siano in grado di esercitare i predetti diritti di accesso;

i) il fornitore di servizi garantisca la protezione delle informazioni riservate relative all'istituto e ai suoi clienti;

j) l'istituto e il fornitore di servizi adottino, applichino e mantengano un piano di emergenza per il ripristino dell'operatività dei sistemi in caso di disastro e la verifica periodica dei dispositivi di *back-up*, quando ciò sia necessario in considerazione della funzione esternalizzata;

k) i diritti e gli obblighi rispettivi dell'istituto e del fornitore di servizi siano chiaramente definiti e specificati in un accordo scritto.

Distribuzione e rimborso di moneta elettronica

Gli istituti di moneta elettronica, quando concludono o applicano accordi di distribuzione e rimborso della moneta elettronica, assicurano che siano soddisfatte, ove applicabili, le condizioni di cui al precedente paragrafo.

Fermo restando il rispetto delle condizioni sopra elencate, nel caso in cui il soggetto convenzionato che distribuisce la moneta elettronica riceve direttamente dal cliente le somme a fronte della moneta elettronica da emettere e rilascia contestualmente lo strumento di pagamento

rappresentativo (fisico o virtuale) della stessa, l'accordo di esternalizzazione definisce anche:

- le modalità e i termini mediante i quali gli importi ricevuti sono riconosciuti all'istituto di moneta elettronica, anche al fine di determinare il momento di emissione della moneta elettronica;
- i presidi adottati a fronte del rischio connesso con comportamenti del soggetto distributore in violazione delle disposizioni vigenti.

Il servizio di distribuzione della moneta elettronica può includere la stipula del contratto con il cliente, previo assolvimento degli obblighi di adeguata verifica della clientela nel rispetto delle vigenti disposizioni in materia di prevenzione del riciclaggio e del finanziamento al terrorismo.

Allegato C

Sistemi informativi e gestione dei rischi operativi e di sicurezza

1. Disposizioni di carattere generale

L'affidabilità dei sistemi informativi rappresenta un pre-requisito essenziale per il buon funzionamento dell'istituto e consente agli organi aziendali di assumere decisioni consapevoli e coerenti con gli obiettivi aziendali.

I sistemi di registrazione contabile hanno un elevato grado di attendibilità, registrano correttamente e con la massima tempestività i fatti di gestione, consentono di ricostruire l'attività dell'istituto a qualsiasi data, partitamente per ciascuno dei servizi di pagamento prestati e, per gli istituti di moneta elettronica, anche in relazione all'attività di emissione di moneta elettronica.

La circostanza che l'istituto utilizzi diverse procedure settoriali (contabilità, segnalazioni, antiriciclaggio, ecc.) non inficia la qualità e l'integrità dei dati né comporta la creazione di archivi non coerenti.

Fermo restando quanto previsto dal DORA e dai relativi atti delegati in materia di sistemi informativi e gestione dei rischi informatici, gli istituti 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.

In particolare, gli istituti:

i) nel trattamento dei dati sensibili relativi ai pagamenti, definiscono e formalizzano i processi di raccolta, instradamento, trattamento, memorizzazione e/o archiviazione nonché di accesso degli stessi, al fine di garantirne l'integrità e la riservatezza. In tale ambito gli istituti istituiscono e aggiornano un registro dei soggetti che hanno accesso ai dati sensibili relativi ai pagamenti;

ii) svolgono, con cadenza almeno annuale, una valutazione dei "rischi operativi e di sicurezza" relativi ai servizi di pagamento che essi prestano e dell'adeguatezza delle misure di mitigazione e dei meccanismi di controllo messi in atto per affrontarli ([1]). Una relazione contenente le risultanze di tale valutazione è trasmessa alla Banca d'Italia entro il 30 aprile di ogni anno ([2]).

([1]) Questa valutazione è anche necessaria in caso di previste modifiche nelle infrastrutture, processi e procedure che possono riguardare la sicurezza dell'istituto.

([2]) Gli istituti 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

iii) definiscono le misure da adottare in caso di cessazione dei propri servizi di pagamento e/o dei contratti vigenti, per evitare effetti negativi sui sistemi di pagamento e sugli utenti e per garantire l'esecuzione delle operazioni di pagamento in corso. Queste misure sono descritte in un'apposita sezione del piano di emergenza e di continuità operativa.

Nella gestione del rapporto con gli utenti dei servizi di pagamento, gli istituti applicano i paragrafi da 92 a 98 degli Orientamenti dell'EBA sulla gestione dei rischi relativi alle tecnologie dell'informazione (*Information and Communication Technology*, ICT) e di sicurezza (EBA/GL/2019/04) come emendati il 11/02/2025 (EBA/GL/2025/02).

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

Nel rispetto di quanto previsto dal Regolamento delegato (UE) 2018/389 della Commissione, gli istituti che prestano servizi di pagamento di radicamento di conti di pagamento che intendono richiedere l'esenzione dalla predisposizione del meccanismo di emergenza ("interfaccia di *fall-back*") previsto dall'art. 33, par. 4, del regolamento delegato si attengono a quanto previsto dagli Orientamenti dell'ABE 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) del 4 dicembre 2018.

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.

Allegato D

Schema della relazione sulla struttura organizzativa

PARTE I

Organi aziendali

1. Descrivere sinteticamente i compiti assegnati agli organi aziendali.
2. Indicare la periodicità abituale delle riunioni degli organi aziendali.
3. Descrivere i processi che conducono all'ingresso in nuovi mercati o settori o all'introduzione di nuovi prodotti.
4. Indicare tempistica, forma, contenuti della documentazione da trasmettere agli organi aziendali ai fini dell'adempimento delle rispettive funzioni, con specifica identificazione dei soggetti responsabili. Evidenziare responsabili, tempistica e contenuto minimo dei flussi informativi da presentare agli organi aziendali su base regolare.

PARTE II

Struttura organizzativa e sistema dei controlli interni

1. Descrivere (anche mediante grafico) l'organigramma/funzionigramma aziendale (includendo anche l'eventuale rete periferica, degli agenti e dei soggetti convenzionati).
2. Descrivere le deleghe attribuite ai vari livelli dell'organizzazione aziendale, i relativi limiti operativi, le modalità di controllo del delegante sull'azione del delegato.
3. Con riferimento alle funzioni operative relative a servizi di pagamento, all'emissione di moneta elettronica o alle funzioni importanti per cui l'istituto si avvale di un fornitore terzo e alle procedure adottate per il controllo di tali funzioni:
    i. indicare le funzioni esternalizzate e il referente responsabile delle attività esternalizzate;
    ii. descrivere il contenuto degli accordi di esternalizzazione inclusa l'identità e la localizzazione geografica del fornitore e le procedure adottate per il controllo delle funzioni esternalizzate nonché il contenuto degli accordi per l'utilizzo di servizi TIC a norma del DORA.
4. Per le funzioni aziendali di controllo, indicare il responsabile e descrivere le risorse umane e tecnologiche a disposizione, il contenuto e la periodicità delle attività di controllo, specificando i

ruoli e le responsabilità connesse con lo svolgimento dei processi di controllo.

5. Con riferimento all'eventuale rete periferica, agli agenti e ai soggetti convenzionati:
    i. descrivere le modalità e la frequenza dei controlli in loco e fuori sede su succursali, agenti e soggetti convenzionati;
    ii. illustrare i sistemi informativi, i processi e le infrastrutture impiegati dagli agenti e soggetti convenzionati per svolgere le attività per conto dell'istituto;
    iii. indicare i sistemi di pagamento nazionali e/o internazionali a cui l'istituto ha accesso, se del caso.

PARTE III

Gestione dei rischi

1. Indicare per ciascuna tipologia di rischio rilevante i presidi organizzativi approntati per la loro gestione e i meccanismi di controllo.

2. Illustrare i presidi e le cautele previsti con riferimento alla distribuzione dei servizi di pagamento, di emissione di moneta elettronica e di eventuali altri servizi, con particolare riguardo sia alla propria rete periferica che alla rete costituita da agenti e da soggetti convenzionati.

3. Descrivere i presidi organizzativi e di controllo per assicurare il rispetto delle normative in materia di prevenzione del riciclaggio e di finanziamento al terrorismo.

4. Descrivere i presidi organizzativi approntati per garantire il rispetto della disciplina in materia di trasparenza e correttezza delle relazioni con la clientela, anche con riferimento alle procedure adottate per la trattazione dei reclami.

PARTE IV

Sistemi informativi e sicurezza

1. Descrivere sinteticamente le procedure informatiche utilizzate nei vari comparti (contabilità, segnalazioni, ecc.), ivi inclusa la procedura utilizzata per il monitoraggio, la gestione e il controllo degli incidenti relativi alla sicurezza compreso un meccanismo di notifica degli incidenti che tenga conto degli obblighi di notifica dell'istituto di cui al capo III del DORA e dei reclami dei clienti in merito alla sicurezza, il processo di alimentazione delle stesse, ponendo in evidenza le operazioni automatizzate e quelle effettuate manualmente, il grado di integrazione tra le procedure.

2. Indicare i controlli (compresi quelli generati automaticamente dalle procedure) effettuati sulla qualità dei dati.
3. Illustrare i presidi logici e fisici approntati per garantire la sicurezza del sistema informativo e la riservatezza dei dati (individuazione dei soggetti abilitati, gestione di *userid* e *password*, sistemi di *back-up* e di *recovery*, ecc.). Con particolare riferimento ai dati sensibili relativi ai pagamenti:
    i. descrivere la *policy* in materia gestione e controllo degli accessi ([1]) ai componenti e ai sistemi dell'infrastruttura informatica utilizzati per il trattamento di questi dati, inclusi i *database* e i sistemi di *back up*, e
    ii. indicare i soggetti che hanno accesso ai dati sensibili relativi ai pagamenti;
4. Descrivere le disposizioni adottate in materia di continuità operativa, tra cui l'individuazione chiara delle operazioni critiche, politica e piani di continuità operativa delle TIC e piani di risposta e di ripristino relativi alle TIC efficaci nonché una procedura per testare periodicamente e riesaminare l'adeguatezza e l'efficacia di tali piani a norma del DORA; descrivere le procedure e le misure adottate per mitigare i rischi in caso di cessazione dei propri servizi di pagamento, al fine di evitare effetti negativi sui sistemi di pagamento e sugli utenti dei servizi, nonché per garantire l'esecuzione delle operazioni in corso.
5. Descrivere il sistema di gestione dei rischi operativi e di sicurezza ([2]) indicando come le misure di controllo e di mitigazione in materia di sicurezza garantiscono un elevato livello di resilienza operativa digitale conformemente al capo II del DORA, in particolare, in relazione alla sicurezza tecnica e protezione dei dati, anche per il software e i sistemi TIC utilizzati dall'istituto o dalle imprese alle quali questi esternalizza la totalità o parte delle sue attività. Tali misure comprendono anche le misure di sicurezza di cui all'articolo 95, paragrafo 1, della direttiva 2015/2366/UE (PSD2), come individuate nei paragrafi da 92 a 98 degli Orientamenti dell'EBA sulla gestione dei rischi relativi alle tecnologie dell'informazione (Information and Communication Technology, ICT) e di sicurezza (EBA/GL/2019/04) come emendati il 11/02/2025 (EBA/GL/2025/02).

([1]) Cfr. articoli 20, 21 e 33 del Regolamento Delegato (UE) 2024/1774 relativo alle 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.

([2]) Per il dettaglio delle informazioni da comunicare, cfr. Orientamento n. 13 concernente il "Documento relativo alla politica di sicurezza" dei già citati Orientamenti finali sulle informazioni che devono essere fornite per ottenere l'autorizzazione degli istituti di pagamento e degli istituti di moneta elettronica, nonché per la registrazione dei prestatori di servizi di informazione sui conti (EBA/GL/2017/09) emanati dall'EBA l'8 novembre 2017.

Allegato E

Descrizione dei servizi di pagamento, dell'attività di emissione della moneta elettronica e delle relative caratteristiche

Sezione A – Elenco dei servizi di pagamento

L'istituto indica i servizi di pagamento che intende offrire, tra quelli previsti nell'articolo 1, comma 2, lett. h-*septies*.1, del TUB.

Sezione B – Caratteristiche dei servizi di pagamento

L'istituto descrive per ciascuno dei servizi di pagamento prestati le informazioni previste dal pertinente schema di compilazione, come di seguito indicato.

B.1 – Servizi di pagamento di cui ai nn. da 1 a 5 dell'art. 1, comma 2, lett. h-septies.1, del TUB

PARTE I

1 - Contrattualizzazione

Caratteristiche del servizio offerto all'utenza, incluse le modalità di registrazione delle operazioni di sottoscrizione e estinzione del rapporto con l'utente e le relazioni contrattuali con le altre parti eventualmente coinvolte.

Caratteristiche dei conti di pagamento, inclusi eventuali importi massimi di avvaloramento e/o tempi massimi di gestione dei fondi

2 - Circuito

Caratteristiche del circuito di accettazione dello strumento di pagamento e dei meccanismi di collegamento tra l'istituto e il circuito. A tal fine, è indicato se l'istituto che emette lo strumento di pagamento: i) è proprietario del circuito di accettazione; ii) aderisce a un circuito di pagamento gestito da terzi (es. schema carte di pagamento ovvero rete interbancaria di pagamento); iii) ha aggiunto funzioni proprie a un circuito di pagamento di terzi.

Aspetti di dettaglio:

- modalità di funzionamento del circuito e, in particolare, ruolo e responsabilità dei diversi soggetti coinvolti;
- meccanismi di tutela dell'integrità del circuito, con particolare riguardo ai sistemi di controllo, alle misure atte ad assicurare la continuità e l'adeguatezza dei livelli del servizio, nonché indicazione dei soggetti responsabili per l'amministrazione della sicurezza del circuito;

- misure di sicurezza dell'informazione adottate, in particolare modalità di identificazione/autenticazione degli utenti e di gestione di eventuali sistemi di crittografia, misure dirette a preservare l'integrità e la riservatezza dei dati e ad assicurare la protezione dei dispositivi fisici.

3 – Meccanismi di autenticazione

Caratteristiche del dispositivo personalizzato e/o insieme di procedure concordate tra l'utente e il prestatore di servizi di pagamento e di cui l'utente di servizi di pagamento si avvale per impartire un ordine di pagamento.

Modalità di acquisizione dell'eventuale dispositivo personalizzato e presidi di sicurezza tecnici adottati.

PARTE II

1 – Clearing and settlement

Modalità di clearing e settlement dei pagamenti, modalità di accesso a procedure di scambio e di regolamento delle operazioni (ad es. adesione a procedure interbancarie, ricorso a tramite operativo, canale di regolamento prescelto) con descrizione dei flussi monetari e/o contabili relativi.

Presidi di sicurezza tecnici posti a tutela dell'affidabilità e della disponibilità dei servizi utilizzati dall'istituto per l'accesso alle procedure di clearing e settlement gestite da terzi.

Presidi a tutela del rispetto dei *cut-off time* previsti.

2 - Gestione e controllo frodi

Misure dirette alla prevenzione e alla rilevazione di comportamenti anomali, di tentativi di manipolazione o di utilizzi fraudolenti.

3 - Gestione reclami

Procedure per la gestione dei reclami degli utenti a seguito di disservizi, malfunzionamenti o frodi inerenti al servizio di pagamento prestato.

4 - Erogazione credito

Servizi in relazione ai quali viene accordato il credito.

Caratteristiche principali del contratto di erogazione del credito (esempio: durata del finanziamento, tipologia del finanziamento).

PARTE III

1 - Informazioni ulteriori da fornire per i servizi di cui ai nn. 1 e 2

Funzioni di deposito/prelievo

Caratteristiche dei servizi che permettono di depositare e/o prelevare il contante da un conto di pagamento, nonché delle operazioni richieste per la gestione di un conto di pagamento.

Presidi di sicurezza tecnica adottati per assicurare l'affidabilità e la disponibilità del servizio.

2 - Informazioni ulteriori da fornire per i servizi di cui ai nn. 3, 4

Ordini di pagamento

Procedura per il perfezionamento dell'ordine di pagamento (ad es. trasferimento fondi, addebito diretto anche una tantum, bonifici, ordini permanenti, operazioni disposte mediante carte di pagamento o dispositivi analoghi), incluse le modalità di autenticazione dell'utente, accettazione dell'ordine e completamento della transazione.

Presidi di sicurezza tecnici adottati per assicurare l'affidabilità e la disponibilità del servizio.

3 - Informazioni ulteriori da fornire per i servizi di cui al n. 5

Emissione di strumenti di pagamento

Caratteristiche tecniche e di funzionamento dello strumento di pagamento (esempio: carte fisiche ovvero dispositivi virtuali, dispositivi di autenticazione), inclusi i presidi di sicurezza tecnici adottati.

Modalità di produzione, personalizzazione, conservazione, distribuzione e distruzione dei dispositivi utilizzati e relativi presidi di sicurezza tecnici adottati.

Gli emittenti di strumenti di pagamento basati su carta forniscono anche, ove rilevanti, le informazioni previste dal seguente Paragrafo B.3, Sezione 2 "Accesso ai conti di pagamento" e Sezione 3 "Autenticazione e consenso".

Acquiring

Caratteristiche del servizio di acquiring, incluse modalità di convenzionamento del *merchant*, caratteristiche dei flussi informativi e monetari con i punti di accettazione degli strumenti di pagamento

Caratteristiche tecniche e di funzionamento dei dispositivi di accettazione dello strumento di pagamento (ad esempio, terminali POS fisici e virtuali, ATM e servizi di *acquiring* remoto attraverso reti pubbliche o private) e relativi presidi di sicurezza tecnici adottati.

Modalità di produzione, personalizzazione, installazione e rimozione dei dispositivi di accettazione dello strumento di pagamento e relativi presidi di sicurezza tecnici adottati.

4 - Informazioni ulteriori da fornire per i servizi che includono l'offerta e l'amministrazione di un conto di pagamento accessibile *on-line*

Descrizione delle caratteristiche delle interfacce che consentono l'interconnessione tra il prestatore di servizi di pagamento di radicamento del conto e il prestatore del servizio di disposizione di ordini di pagamento, di informazione sui conti o di emissione di strumenti di pagamento basati su carta in conformità con i requisiti previsti dal Regolamento delegato della Commissione del 27 novembre 2017 n. 2018/389. Nel caso di adesione a piattaforme:

- modalità di integrazione della piattaforma nei sistemi informativi aziendali e, in particolare, ruoli e responsabilità dei diversi soggetti coinvolti;
- meccanismi di tutela dell'integrità della piattaforma, con particolare riguardo ai sistemi di controllo, alle misure atte ad assicurare la continuità e l'adeguatezza dei livelli del servizio, nonché indicazione dei soggetti responsabili per l'amministrazione della sicurezza della piattaforma.

B.2. Servizi di pagamento di cui all'art. 1, comma 2, lett. h-septies.1, n. 6 del TUB (Rimesse)

1 - Circuito

Eventuale circuito al quale si aderisce e/o i principali paesi verso cui vengono inviate e/o ricevute le rimesse di denaro.

2 - Modalità di funzionamento del servizio

Caratteristiche del servizio, inclusi:

a) livelli di servizio garantiti, vincoli procedurali e di importo, ulteriori caratteristiche peculiari;
b) procedure e presidi di sicurezza nella fase di invio (controlli di linea, verifica identità, generazione codici di controllo e loro sicurezza, ecc.);
c) procedure e presidi di sicurezza nella fase di ricezione (controlli sulle identità e sui parametri della transazione, verifica codici di controllo).

3 - Modalità di gestione dei flussi monetari e informativi.

Descrizione dei seguenti aspetti:

a) caratteristiche e presidi di sicurezza dei sistemi informativi degli agenti che erogano il servizio alla clientela;

b) caratteristiche e presidi di sicurezza delle reti di interconnessione degli agenti con i sistemi elaborativi centrali;

c) procedure di controllo sugli agenti, inclusa la verifica delle procedure tecnico-operative di sicurezza;

d) caratteristiche e presidi di sicurezza adottati per l'accesso alle reti interbancarie nazionali e internazionali.

4 - Clearing e settlement

Modalità di clearing e settlement dei pagamenti, modalità di accesso a procedure di scambio e di regolamento delle operazioni (ad es. adesione a procedure interbancarie, ricorso a tramite operativo, canale di regolamento prescelto) con descrizione dei flussi monetari e/o contabili relativi.

Presidi di sicurezza tecnici posti a tutela dell'affidabilità e della disponibilità dei servizi utilizzati dall'istituto per l'accesso alle procedure di clearing e settlement gestite da terzi.

Presidi a tutela del rispetto dei *cut-off time* previsti.

5 - Gestione e controllo frodi

Misure dirette alla prevenzione e rilevazione di comportamenti anomali, di tentativi di manipolazione o di utilizzi fraudolenti.

6 - Gestione reclami

Procedure per la gestione dei reclami degli utenti a seguito di disservizi, malfunzionamenti o frodi inerenti al servizio di pagamento prestato.

B.3. Servizio di pagamento di cui all'art. 1, comma 2, lett. h-septies.1) n. 7, del TUB (Servizio di disposizione di ordini di pagamento)

PARTE I

1 - Contrattualizzazione

Caratteristiche del servizio offerto all'utenza, incluse le modalità di registrazione delle operazioni di sottoscrizione ed estinzione del rapporto con l'utente e le relazioni contrattuali con le altre parti eventualmente coinvolte.

Caratteristiche dei conti di pagamento cui il prestatore accede ed eventuali limiti di importo degli ordini di pagamento disposti.

Modalità di convenzionamento del *merchant*, caratteristiche dei flussi informativi con i punti di accettazione degli strumenti di pagamento.

2 – Accesso ai conti di pagamento

Descrizione delle modalità e delle procedure di accesso ai conti di pagamento.

- Descrizione delle procedure interne per la richiesta di rilascio, gestione, revoca e aggiornamento dei certificati con cui il prestatore del servizio di disposizione di ordini di pagamento si identifica presso il prestatore di servizi di pagamento di radicamento del conto.;

Descrizione delle misure di sicurezza delle TIC adottate, in particolare modalità di identificazione/autenticazione degli utenti e di gestione di eventuali sistemi di crittografia, misure dirette a preservare l'integrità e la riservatezza dei dati e ad assicurare la protezione dei dispositivi fisici.

3 – Autenticazione e consenso

Descrizione delle caratteristiche dei dispositivi personalizzati e/o delle procedure eventualmente concordate tra il prestatore di servizi di disposizione di ordini di pagamento e l'utente, anche ulteriori rispetto a quelle fornite dal prestatore di servizi di pagamento di radicamento del conto.

Descrizione delle modalità di gestione dell'ordine di pagamento.

Presidi di sicurezza tecnici adottati per assicurare l'affidabilità e la disponibilità del servizio.

Descrizione delle procedure di integrazione con i meccanismi di autenticazione forniti dal prestatore di servizi di pagamento di radicamento del conto.

Modalità di acquisizione del consenso dell'utente e relativi presidi di sicurezza tecnici adottati.

PARTE II

1 - Gestione e controllo frodi

Misure dirette alla prevenzione e alla rilevazione di comportamenti anomali, di tentativi di manipolazione o di utilizzi fraudolenti.

2 - Gestione reclami

Procedure per la gestione dei reclami degli utenti in materia di sicurezza a seguito di disservizi, malfunzionamenti o frodi inerenti al servizio di pagamento prestato.

B.4. Servizio di pagamento di cui all'art. 1, comma 2, lett. h-septies.1) n. 8, del TUB (Servizio di informazione sui conti) B.4. Servizio di pagamento di cui all'art. 1, comma 2, lett. h-septies.1) n. 8, del TUB (Servizio di informazione sui conti)

PARTE I

1 - Contrattualizzazione

Caratteristiche del servizio offerto all'utenza, incluse le modalità di registrazione delle operazioni di sottoscrizione e estinzione del rapporto con l'utente e le relazioni contrattuali con le altre parti eventualmente coinvolte.

Caratteristiche dei conti di pagamento cui il prestatore accede.

2 – Accesso ai conti di pagamento

Descrizione delle modalità e delle procedure di accesso ai conti di pagamento.

Descrizione delle procedure interne per la richiesta di rilascio, gestione, revoca e aggiornamento dei certificati con cui il prestatore di servizi di informazione sui conti si identifica presso il prestatore di servizi di pagamento di radicamento del conto.

Descrizione delle misure di sicurezza delle TIC adottate, in particolare modalità di identificazione/autenticazione degli utenti e di gestione di eventuali sistemi di crittografia, misure dirette a preservare l'integrità e la riservatezza dei dati e ad assicurare la protezione dei dispositivi fisici.

3 – Autenticazione e consenso

Descrizione delle caratteristiche dei dispositivi personalizzati e/o delle procedure eventualmente concordate tra il prestatore di servizi di informazione sui conti e l'utente, anche in aggiunta a quelle fornite dal prestatore di servizi di pagamento di radicamento del conto.

Presidi di sicurezza tecnici adottati per assicurare l'affidabilità e la disponibilità del servizio.

Descrizione delle procedure di integrazione con i meccanismi di autenticazione forniti dal prestatore di servizi di pagamento di radicamento del conto. Modalità di acquisizione del consenso dell'utente e presidi di sicurezza tecnici adottati, inclusi i meccanismi con cui si assicura l'accesso esclusivamente alle informazioni sui conti di pagamento designati e sulle operazioni di pagamento a questi associati.

PARTE II

1 - Gestione e controllo frodi

Misure dirette alla prevenzione e alla rilevazione di comportamenti anomali, di tentativi di manipolazione o di utilizzi fraudolenti.

2 - Gestione reclami

Procedure per la gestione dei reclami degli utenti in materia di sicurezza a seguito di disservizi, malfunzionamenti o frodi inerenti al servizio di pagamento prestato.

Sezione C – Moneta elettronica

Gli istituti di moneta elettronica forniscono le informazioni di cui alla Sezione B.1 con riferimento all'attività di emissione di moneta elettronica. Essi descrivono inoltre i seguenti aspetti:

a) caratteristiche tecniche e di funzionamento dello strumento di pagamento (esempio: carte fisiche ovvero dispositivi virtuali; nominativi o anonimi; ricaricabili o meno; eventuale possibilità di effettuare trasferimenti di moneta elettronica da un dispositivo ad un altro);

b) modalità di avvaloramento iniziale e, ove previsti, di avvaloramento successivo;

c) modalità di rimborso della moneta elettronica e caratteristiche essenziali del rapporto contrattuale con il detentore di moneta elettronica (es. valore monetario iniziale, importi massimi di avvaloramento, importo massimo delle singole ricariche, condizioni e modalità di utilizzo, commissioni applicate);

d) meccanismi di registrazione delle operazioni di avvaloramento, utilizzo, ricarica, rimborso e, ove previsti, dei trasferimenti da un dispositivo ad un altro.

[*omissis*]