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 della direttiva 2015/2366/UE del Parlamento europeo e del Consiglio del 25 novembre 2015, relativa ai servizi di pagamento nel mercato interno (PSD2);

Tenuto conto della direttiva 2009/110/CE del Parlamento Europeo e del Consiglio, del 16 settembre 2009, concernente l'avvio, l'esercizio e la vigilanza prudenziale dell'attività degli istituti di moneta elettronica;

Tenuto conto degli Orientamenti emanati dall'Autorità bancaria europea ("ABE") in materia di:

- gestione dei rischi relativi alle tecnologie dell'informazione (*Information and Communication Technology*, ICT) e di sicurezza (EBA/GL/2019/04), del 28 novembre 2019;
- segnalazione dei gravi incidenti ai sensi della PSD2 (EBA/GL/2021/03), del 10 giugno 2021;

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 attuare gli Orientamenti dell'ABE sulla gestione dei rischi relativi alle tecnologie dell'informazione (ICT) e di sicurezza (EBA/GL/2019/04), nonché per coordinare le nuove previsioni con la normativa vigente.

Le modifiche, ivi incluse quelle relative a interventi di raccordo, riguardano: il Capitolo I, Sezioni I (fonti normative) e II (definizioni); il Capitolo VI, Sezione I e Allegati A, C, D, E; il Capitolo VIII, Sezioni I e II; il Capitolo XII, Sez. I, par. 2.

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

Gli istituti si adeguano al contenuto delle presenti disposizioni entro il 30 giugno 2023. Entro il 1° settembre 2023, trasmettono alla Banca d'Italia una relazione che descrive gli interventi effettuati per assicurare il rispetto delle stesse.

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

Il Governatore

Firmato digitalmente da
IGNAZIO VISCO

delibera 415/2022

ALLEGATO

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;
- 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. 161/1998, recante norme per l'individuazione dei requisiti di onorabilità e professionalità

degli esponenti aziendali delle banche e delle cause di sospensione, 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;

- 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 aggiornati in materia di segnalazione dei gravi incidenti ai sensi della PSD2 (EBA/GL/2021/03), emanati dall'EBA il 10 giugno 2021;
- 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;
- 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.

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.

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;
- *"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;
- "*incidente operativo o di sicurezza"*: ogni evento, o serie di eventi collegati, non pianificati dagli istituti che ha, o probabilmente avrà, un impatto negativo sull'integrità, la disponibilità, la riservatezza, e/o l'autenticità dei servizi;
- *"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;

- "*progetti* ICT": qualsiasi progetto, o parte di esso, in cui i sistemi e i servizi ICT sono modificati, sostituiti, dismessi o implementati. I progetti ICT possono far parte di più ampi programmi ICT o di trasformazione aziendale;
- "*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;
- "*rischio ICT e di sicurezza*": il rischio di incorrere in perdite economiche, di reputazione e di quote di mercato in relazione all'utilizzo di tecnologia dell'informazione e della comunicazione (*Information and Communication Technology* – ICT) dovuto a violazione della riservatezza, carente integrità dei sistemi e dei dati, inadeguatezza o indisponibilità dei sistemi e dei dati o incapacità di sostituire la tecnologia dell'informazione (ICT) entro ragionevoli limiti di tempo e costi in caso di modifica dei requisiti del contesto esterno o dell'attività (*agility*), nonché i rischi di sicurezza derivanti da processi interni inadeguati o errati o da eventi esterni, inclusi gli attacchi informatici o un livello di sicurezza fisica inadeguata;
- "*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;
- "*risorsa informativa"*: una raccolta di informazioni, tangibile o intangibile, che merita protezione;
- "*risorsa informatica* (*o* ICT)": qualsiasi *software* o *hardware* presente nel contesto aziendale;
- "*servizi* ICT": i servizi forniti dai sistemi ICT a uno o più utenti interni o esterni. Tali servizi comprendono, ad esempio: servizi di inserimento, archiviazione, elaborazione e comunicazione di dati, servizi di monitoraggio, di supporto alle attività e alle decisioni aziendali;
- "*sistemi* ICT": ICT adottato come parte di un meccanismo o di una rete di interconnessione a supporto delle operazioni dell'istituto;
- *"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);

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

- *"soggetto terzo"*: un soggetto o organizzazione che ha stretto rapporti commerciali o stipulato contratti con un istituto per la fornitura di un prodotto o un servizio;
- *"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*]

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.

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, dei controlli interni e i sistemi informativi di gestione dei rischi operativi, inclusi i rischi ICT 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.

[*Omissis*]

([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.

Allegato A

Ruolo degli organi aziendali e sistema dei controlli interni

[*Omissis*]

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, inclusi i rischi ICT 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, inclusi quelli sul sistema informativo (*ITC audit*), 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, inclusi quelli ICT e di sicurezza e il 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, inclusi quelli ICT e di sicurezza, in relazione alle specifiche caratteristiche organizzative ed operative;
- valutano i rischi operativi, inclusi quelli ICT 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;

([1]) Tra le funzioni aziendali di controllo di secondo livello rientra la funzione di controllo dei rischi ICT e di sicurezza disciplinata dagli 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 recepiti nell'Allegato C. Resta ferma la possibilità per gli istituti di assegnare i compiti della funzione di controllo dei rischi ICT e di sicurezza alle funzioni aziendali di controllo dei rischi e di conformità alle norme, in coerenza con il ruolo, le responsabilità e le competenze proprie di ciascuna.

([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.

– 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 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

---

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

([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.

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.

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;

([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 dei rischi ICT e di sicurezza, cfr. par.11 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), recepiti nell'Allegato C. Resta ferma la possibilità per gli istituti di assegnare i compiti della funzione di controllo dei rischi ICT e di sicurezza alle funzioni aziendali di controllo dei rischi e di conformità alle norme, in coerenza con il ruolo, le responsabilità e le competenze proprie di ciascuna.

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;

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;

([7]) Per la funzione di controllo dei rischi ICT e di sicurezza resta fermo quanto previsto dal par. 11 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 recepito nell'Allegato C. Resta ferma la possibilità per gli istituti di assegnare i compiti della funzione di controllo dei rischi ICT e di sicurezza alle funzioni aziendali di controllo dei rischi e di conformità alle norme, in coerenza con il ruolo, le responsabilità e le competenze proprie di ciascuna.

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 *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.

[*Omissis*]

Allegato C

Sistemi informativi e gestione dei rischi operativi, inclusi i rischi ICT 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 informativo-contabili sono adeguati al contesto operativo e ai rischi ai quali l'istituto è esposto.

Essi 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 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.

Gli istituti si dotano di sistemi e misure di mitigazione e di meccanismi di controllo adeguati per gestire i rischi operativi, inclusi i rischi ICT 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) adottano misure per prevenire e gestire gli incidenti operativi o di sicurezza e individuano i soggetti responsabili dell'assistenza ai clienti in relazione ai reclami concernenti la sicurezza dei servizi di pagamento prestati. I gravi incidenti operativi o di sicurezza che interessano direttamente o indirettamente gli istituti sono comunicati senza indugio alla Banca d'Italia con le modalità e nei termini da essa stabiliti, conformemente agli Orientamenti aggiornati dell'EBA in materia di segnalazione dei gravi incidenti ai sensi della PSD2 (EBA/GL/2021/03) ([1]). Gli istituti utilizzano il modulo disponibile sul sito *internet* dell'Istituto ([2]). Se l'incidente incide o potrebbe incidere sugli interessi finanziari dei propri utenti di servizi di pagamento, gli istituti informano altresì quest'ultimi senza indugio dell'incidente e di tutte le misure a disposizione che possono adottare per attenuarne gli effetti negativi ([3]);

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

([2]) https://www.bancaditalia.it/compiti/vigilanza/incidenti-operativi/index.html.

([3]) Cfr., Articolo 96, paragrafo 1, comma 2, della PSD2.

iii) 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 ([4]). Una relazione contenente le risultanze di tale valutazione è trasmessa alla Banca d'Italia entro il 30 aprile di ogni anno ([5]).

iv) in materia di continuità operativa, individuano le operazioni critiche, si dotano di piani di emergenza efficaci e di una procedura per testare periodicamente tali piani e riesaminarne l'adeguatezza e l'efficacia;

v) 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.

Gli istituti applicano gli Orientamenti dell'EBA sulla gestione dei rischi relativi alle tecnologie dell'informazione (*Information and Communication Technology*, ICT) e di sicurezza (EBA/GL/2019/04). In linea con l'impostazione generale della disciplina in materia di controlli interni e gestione dei rischi, gli istituti applicano le disposizioni contenute negli Orientamenti secondo il principio di proporzionalità, cioè tenuto conto della dimensione e complessità operative, della natura dell'attività svolta, della tipologia dei servizi prestati.

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.

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

([5]) 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 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

[*Omissis*]

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. Specifici riferimenti dovranno essere prodotti in merito alle procedure poste in essere nel caso di utilizzo di reti distributive informatiche (es. Internet) ([1]).

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 di sicurezza 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 ICT e la riservatezza dei dati (individuazione dei soggetti abilitati, gestione di *userid* e *password*, sistemi di *back-up* e

([1]) Gli istituti applicano i già citati "Orientamenti finali in materi di sicurezza dei pagamenti tramite internet" emanati dall'EBA.

di *recovery*, ecc.). Con particolare riferimento ai dati sensibili relativi ai pagamenti:

   i. descrivere la *policy* in materia di diritto di accesso 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. Individuare il responsabile ICT e le funzioni ad esso attribuite.

5. Descrivere il piano di emergenza e di continuità operativa stabilito per assicurare la propria capacità di operare su base continuativa e di limitare le perdite operative in caso di gravi interruzioni dell'operatività; 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.

6. Descrivere il sistema di gestione dei rischi operativi e di sicurezza ([2]).

([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

[*Omissis*]

Sezione B – Caratteristiche dei servizi di pagamento

[*Omissis*]

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.

[*Omissis*]

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 informatica 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.

[*Omissis*]

CAPITOLO VIII
OPERATIVITÀ IN ITALIA DEGLI ISTITUTI

SEZIONE I
OPERATIVITÀ DEGLI ISTITUTI DELL'UNIONE EUROPEA ([1])

1. Ambito di applicazione

Le presenti disposizioni si applicano:

- agli istituti dell'Unione europea che intendono prestare in Italia servizi di pagamento attraverso l'esercizio del diritto di stabilimento o in regime di libera prestazione di servizi, anche mediante l'impiego di agenti;
- agli istituti di moneta elettronica dell'Unione europea che intendono prestare in Italia l'attività di emissione di moneta elettronica attraverso l'esercizio del diritto di stabilimento o in regime di libera prestazione di servizi, anche mediante l'impiego di soggetti convenzionati per la distribuzione e il rimborso della moneta elettronica.

2. Stabilimento di succursali: primo insediamento ([2])

L'istituto dell'Unione europea che intende per la prima volta operare in Italia tramite l'insediamento di una succursale notifica questo intendimento all'autorità competente dello Stato d'origine.

L'inizio dell'operatività della succursale è subordinato alla ricezione da parte della Banca d'Italia della comunicazione inviata dall'autorità competente dello Stato d'origine dell'istituto.

Entro 30 giorni dalla ricezione della notifica, la Banca d'Italia comunica all'autorità competente dello Stato di origine se sussistono ragionevoli motivi per sospettare che, relativamente all'insediamento della succursale, siano in corso o siano state compiute o tentate operazioni di riciclaggio o di finanziamento del terrorismo ovvero che possa aumentare il rischio di riciclaggio o di finanziamento al terrorismo.

([1]) Le comunicazioni di cui alla presente Sezione vanno inviate alla Banca d'Italia - Amministrazione Centrale - Servizio Regolamentazione e analisi macroprudenziale.

([2]) Cfr. Regolamento delegato (UE) 2017/2055 della Commissione del 23 giugno 2017 che integra la Direttiva 2015/2366/UE del Parlamento europeo e del Consiglio per quanto riguarda le norme tecniche di regolamentazione per la cooperazione e lo scambio di informazioni tra autorità competenti in relazione all'esercizio del diritto di stabilimento e della libera prestazione dei servizi degli istituti di pagamento

3. Impiego di agenti o di soggetti convenzionati insediati in Italia ([3])

3.1. Diritto di stabilimento

In conformità a quanto previsto dall'articolo 128-*decies*, comma 2-*bis,* del TUB, l'istituto dell'Unione europea che intende prestare in Italia, in regime di diritto di stabilimento senza succursale, servizi di pagamento per il tramite di agenti designa in Italia un punto di contatto centrale, nel rispetto di quanto previsto dal Regolamento delegato della Commissione sul punto di contatto centrale ai sensi della direttiva 2015/2366/UE ([4]). Quando è costituito in Italia il punto di contatto centrale ai sensi delle disposizioni di cui al Titolo II, Capo V, del decreto legislativo 21 novembre 2007, n. 231, e successive modificazioni, l'istituto designa questo punto di contatto centrale anche per le finalità di cui alle presenti Disposizioni e per lo svolgimento delle funzioni previste dal Regolamento citato nel presente capoverso.

L'istituto dell'Unione europea che intende prestare servizi di pagamento in Italia attraverso agenti insediati in Italia notifica tale intendimento all'autorità competente dello Stato d'origine, indicando, tra l'altro, nome del responsabile, indirizzo e recapiti del punto di contatto centrale.

L'istituto di moneta elettronica dell'Unione europea che intende distribuire e rimborsare moneta elettronica in Italia attraverso soggetti convenzionati notifica tale intendimento all'autorità competente dello Stato d'origine, indicando la qualificazione motivata dell'attività quale esercizio della libertà di stabilimento.

L'inizio dell'operatività dell'agente o del soggetto convenzionato è subordinato alla ricezione da parte della Banca d'Italia della comunicazione inviata dall'autorità competente dello Stato d'origine dell'istituto. La Banca d'Italia comunica all'autorità competente dello Stato di origine se sussistono ragionevoli motivi per sospettare che, relativamente all'utilizzo dell'agente o del soggetto convenzionato, siano in corso o siano state compiute o tentate operazioni di riciclaggio o di finanziamento del terrorismo ovvero che l'impiego dell'agente o del soggetto convenzionato possa aumentare il rischio di riciclaggio o di finanziamento al terrorismo.

3.2 Libera prestazione di servizi

L'istituto che intende prestare servizi di pagamento in Italia in regime di libera prestazione di servizi attraverso agenti notifica tale intendimento all'autorità competente dello Stato d'origine, indicando la qualificazione motivata dell'attività quale libera prestazione di servizi.

L'agente può iniziare l'attività dopo che la Banca d'Italia ha ricevuto la notifica da parte della autorità competente dello Stato d'origine.

L'istituto di moneta elettronica che intende avvalersi di soggetti convenzionati per la distribuzione e il rimborso in Italia della moneta elettronica in regime di libera prestazione di servizi notifica tale

([3]) Restano fermi gli altri obblighi di comunicazione imposti agli istituti dell'Unione europea ai sensi dall'art. 128-*quater* comma 7-*bis* del TUB.

([4]) Restano ferme le disposizioni dettate per finalità di prevenzione del riciclaggio e di finanziamento del terrorismo dall'articolo 43, commi 3 e 4 e dall'articolo 45 del decreto legislativo 21 novembre 2007, n. 231 e successive modificazioni

intendimento all'autorità competente dello Stato d'origine, indicando la qualificazione motivata dell'attività quale libera prestazione di servizi.

Il soggetto convenzionato può iniziare l'attività dopo che la Banca d'Italia ha ricevuto la notifica da parte della autorità competente dello Stato d'origine.

4. Prestazione di servizi di pagamento in regime di libera prestazione di servizi

Fermo restando quanto previsto al paragrafo 3.1, l'istituto di pagamento dell'Unione europea che intende prestare in Italia per la prima volta servizi di pagamento in regime di libera prestazione di servizi può iniziare l'attività dopo che la Banca d'Italia ha ricevuto la notifica da parte dell'autorità competente dello Stato d'origine.

L'istituto di moneta elettronica dell'Unione europea che intende prestare in Italia per la prima volta attività di emissione di moneta elettronica o prestare servizi di pagamento in regime di libera prestazione di servizi può iniziare l'attività dopo che la Banca d'Italia ha ricevuto la notifica da parte dell'autorità competente dello Stato d'origine.

5. Controlli della Banca d'Italia e collaborazione con le autorità estere

La Banca d'Italia esercita sugli istituti dell'Unione europea operanti in Italia i controlli, anche ispettivi, di competenza previsti dalla legislazione vigente.

Ai sensi dell'articolo 114-*quinquiesdecies,* comma 1, lett. *b)*, del TUB, la Banca d'Italia scambia informazioni con le altre autorità competenti ai sensi delle disposizioni dell'Unione europea applicabili ai prestatori di servizi di pagamento ([5]).

([5]) Cfr. Regolamento delegato della Commissione sulla cooperazione tra le autorità competenti dello stato di origine e dello stato ospitante per la supervisione degli istituti di pagamento che operano su base transfrontaliera ai sensi dell'art. 29(6) della PSD2.

SEZIONE II
CONDIZIONI PER L'ESERCIZIO IN ITALIA DELL'ATTIVITA' DI CONCESSIONE DI CREDITO DA PARTE DI ISTITUTI DI PAGAMENTO DELL'UNIONE EUROPEA

1. Ambito di applicazione

Le presenti disposizioni si applicano agli istituti di pagamento dell'Unione europea, che prestano servizi di pagamento in Italia ai sensi dell'art. 114-*decies*, commi 2 e 4, del TUB.

2. Condizioni per la concessione del credito

Gli istituti di pagamento dell'Unione europea che prestano servizi di pagamento in Italia, possono concedere credito di durata superiore ai 12 mesi collegato all'emissione o alla gestione di carte di credito qualora siano rispettate le seguenti condizioni:

a) istituiscono una succursale ai sensi della Sezione I, par. 2;

b) l'attività di concessione del credito è svolta con modalità analoghe nel paese d'origine ed è sottoposta a vigilanza;

c) l'attività di concessione del credito nel territorio italiano è esercitata nel rispetto delle disposizioni vigenti nel paese d'origine;

d) la succursale rispetta la disciplina italiana in materia di trasparenza e correttezza delle relazioni tra intermediari e clienti, contrasto dell'usura, del riciclaggio e del finanziamento al terrorismo;

e) l'autorità competente per la vigilanza nel paese di origine assume la responsabilità del controllo sulle attività di concessione del credito, sui rischi rilevanti ad essa connessi, sugli assetti organizzativi e sul sistema di controlli interni della succursale;

f) l'autorità del paese d'origine comunica tempestivamente alla Banca d'Italia tutte le informazioni rilevanti, in particolare nel caso di violazioni, ancorché non accertate in via definitiva, da parte di una succursale della normativa ad essa applicabile.

L'avvio da parte della succursale dell'attività di concessione del credito superiore ai 12 mesi collegato all'emissione o alla gestione di carte di credito è subordinata al raggiungimento di un accordo di collaborazione tra la Banca d'Italia e l'autorità competente del paese di origine, nel quale quest'ultima attesta il rispetto delle condizioni di cui ai punti da b) ad f) del presente paragrafo. L'accordo definisce in dettaglio le modalità e le condizioni per l'esercizio dei controlli di competenza da parte delle autorità coinvolte, eventuali forme di collaborazione e i relativi scambi di informazioni, fermo restando quando previsto dal successivo paragrafo 3.

3. Controlli della Banca d'Italia

La Banca d'Italia esercita sulle succursali in Italia degli istituti di pagamento dell'Unione europea insediate in Italia per le attività di cui alla presente Sezione ([1]) i controlli, anche ispettivi, di competenza..

Allo scopo di effettuare i controlli di propria competenza nonché di garantire la completezza delle informazioni che riguardano il mercato italiano, la Banca d'Italia si riserva la facoltà di chiedere alle succursali di istituti dell'Unione europea i medesimi dati e documenti previsti per gli intermediari finanziari di cui al Titolo V del TUB. In particolare, la Banca d'Italia può richiedere i dati e le informazioni utili ai fini della verifica del rispetto delle disposizioni in materia di trasparenza e correttezza dei comportamenti, contrasto all'usura, al riciclaggio e al finanziamento al terrorismo e diritti e obblighi delle parti.

La Banca d'Italia scambia con l'autorità competente del paese di origine dell'istituto di pagamento dell'Unione europea tutte le informazioni essenziali e/o pertinenti, in particolare nel caso di violazioni o presunte violazioni da parte di una succursale della normativa applicabile.

[*Omissis*]

([1]) Per la prestazione dell'attività di concessione di finanziamento con scadenza superiore ai 12 mesi tramite agenti, gli istituti di pagamento si avvalgono di agenti in attività finanziaria di cui all'art 128 – *quater* del TUB.

CAPITOLO XII
VIGILANZA ISPETTIVA

SEZIONE I
DISPOSIZIONI DI CARATTERE GENERALE

1. Premessa

La Banca d'Italia può effettuare accertamenti ispettivi presso gli istituti operanti in Italia.

Le ispezioni sono volte ad accertare che l'attività degli enti vigilati risponda a criteri di sana e prudente gestione, sia svolta in coerenza con le esigenze di regolare funzionamento del sistema dei pagamenti e sia espletata nell'osservanza delle disposizioni vigenti. In particolare, l'accertamento ispettivo è volto a valutare la complessiva situazione tecnica e organizzativa dell'ente, nonché a verificare l'attendibilità delle informazioni fornite alla Banca d'Italia.

Gli accertamenti possono riguardare la complessiva situazione aziendale ("a spettro esteso"), specifici comparti operativi e/o il rispetto di normative di settore ("mirati") nonché la rispondenza di eventuali azioni correttive poste in essere dall'istituto ("*follow up*").

Gli istituti ispezionati prestano la massima collaborazione all'espletamento degli accertamenti e, in particolare, forniscono con tempestività e completezza i documenti che gli incaricati ritengono necessario acquisire ([1]).

2. Ambito di applicazione

La vigilanza ispettiva è svolta presso:

- gli istituti italiani;
- le succursali in Italia di istituti di pagamento dell'Unione europea o di istituti di moneta elettronica dell'Unione europea, anche nel caso in cui le competenti autorità dello Stato membro d'origine lo richiedano;
- le succursali in Italia di istituti di moneta elettronica aventi sede in stati terzi.

[*Omissis*]

([1]) Cfr. Regolamento delegato della Commissione sulla cooperazione tra le autorità competenti dello stato di origine e dello stato ospitante per la supervisione degli istituti di pagamento che operano su base transfrontaliera ai sensi dell'art. 29(6) della PSD2.