BANCA D'ITALIA
EUROSISTEMA

GUIDA OPERATIVA DEI CONTROLLI
Allegato del Provvedimento della Banca d'Italia del 9 novembre 2021

BANCA D'ITALIA
EUROSISTEMA

INDICE

Introduzione e articolazione della Guida

La presente guida è adottata dalla Banca d'Italia in attuazione del Provvedimento della Banca d'Italia del 9 novembre 2021, recante "Disposizioni in materia di sorveglianza sui sistemi di pagamento e sulle infrastrutture strumentali tecnologiche o di rete" (di seguito il "Provvedimento") [1]. La guida intende fornire indicazioni operative ai gestori di sistemi di pagamento e ai fornitori che gestiscono infrastrutture strumentali tecnologiche o di rete (di seguito "fornitori di infrastrutture o servizi tecnici") sottoposti alla sorveglianza della Banca d'Italia.

In merito ai fornitori di infrastrutture o servizi tecnici:

- le previsioni circa la notifica di inizio e fine operatività si applicano a tutti i fornitori che svolgono una o più attività, secondo quanto indicato nell'art. 19 del Provvedimento[2];
- specifici requisiti di sorveglianza sono applicati a quelli considerati critici (di seguito "fornitori critici"), secondo i criteri di cui all'art. 20 del Provvedimento[3], in esito al procedimento di cui al par. 2 della presente guida.

La presente guida:

- disciplina le modalità con le quali i gestori di sistemi di pagamento e i fornitori di infrastrutture o servizi tecnici notificano alla Banca d'Italia l'avvio o la cessazione dell'attività (paragrafo 1);
- descrive il processo con il quale la Banca d'Italia individua nominativamente i fornitori critici e le modalità di comunicazione dell'assoggettamento a sorveglianza (paragrafo 2);
- definisce le modalità con cui i gestori di sistemi di pagamento e i fornitori critici sono tenuti a comunicare le informazioni previste dal Provvedimento (paragrafo 3);
- descrive le procedure e le tempistiche adottate nello svolgimento delle attività di sorveglianza della Banca d'Italia nei confronti di gestori di sistemi di pagamento (inclusi i sistemi di pagamento al dettaglio gestiti dalla Banca d'Italia) e dei fornitori critici (paragrafi da 4 a 6).

La Banca d'Italia elenca sul proprio sito internet i sistemi di pagamento al dettaglio e all'ingrosso[4] e i fornitori critici assoggettati a sorveglianza.

---

[1] Per i termini usati nella presente guida, si rimanda alle definizioni di cui all'art. 1 del Provvedimento.

[2] L'art. 19 prevede che tra i servizi standardizzati o infrastrutture tecnologiche o di rete rientrano "a titolo di esempio: a. servizi di messaggistica e di rete; b. servizi e/o applicazioni di business strumentali a trattamento e scambio di flussi finanziari e informativi, compensazione e/o regolamento di operazioni di pagamento tra prestatori di servizi di pagamento e/o tra prestatori di servizi di pagamento e clienti; c. servizi di conservazione e trattamento di dati sensibili relativi ai pagamenti, incluse le credenziali di sicurezza degli utenti e i dati per l'indirizzamento dei pagamenti; d. servizi per il trattamento delle operazioni di pagamento di cui all'art. 2, comma 1, numero 28 del Regolamento (UE) n. 2015/751 relativo alle commissioni interbancarie sulle operazioni di pagamento basate su carta; e. servizi tecnologici di interfaccia multi-operatore per l'accesso di terze parti ai conti ai sensi del Regolamento delegato (UE) n. 2018/389 della Commissione del 27 novembre 2017 che integra la Direttiva (UE) 2015/2366 del Parlamento europeo e del Consiglio per quanto riguarda le norme tecniche di regolamentazione per l'autenticazione forte del cliente e gli standard aperti di comunicazione comuni e sicuri."

[3] L'art. 20 prevede che "sulla base delle notifiche ricevute ai sensi dell'art. 19 e più in generale delle informazioni altrimenti acquisite, la Banca d'Italia individua nominativamente i fornitori di cui all'art. 19 considerati critici per l'ordinato funzionamento del sistema dei pagamenti italiano, dandone comunicazione secondo le modalità di cui alla [presente] guida operativa. Ai fini del giudizio sulla criticità dei soggetti in discorso, la Banca considera prioritariamente i seguenti criteri: i) erogazione di infrastruttura o servizi tecnici essenziali per la confidenzialità, l'integrità e la disponibilità dei dati processati per una quota significativa del mercato italiano; ii) importanza dei sistemi di pagamento serviti per il mercato italiano; e/o iii) assenza di fornitori alternativi per l'utenza servita".

[4] Nell'elenco si dà conto dei collegamenti stabiliti dai sistemi al dettaglio individuati e comunicati all'autorità di sorveglianza.

1. Notifica di inizio e fine operatività

1.1 Gestori di sistemi di pagamento

Ai sensi dell'art. 3 del Provvedimento, in occasione dell'inizio e della fine dell'operatività i gestori di sistemi di pagamento trasmettono alla Banca d'Italia le informazioni seguenti:

- con un preavviso non inferiore ai 3 mesi prima dell'inizio dell'operatività: data, denominazione della società e del sistema gestito, forma giuridica, indirizzo della sede legale nonché, ove diverso, anche della sede operativa, indirizzo email e PEC, soggetti portatori di interesse (soci, partecipanti attuali e categorie di partecipanti potenzialmente ammessi), comparto servito (dettaglio/ingrosso), servizi offerti (in particolare, strumenti di pagamento trattati), referenti (contatto principale e alternativo, posizioni ricoperte, email e numeri di telefono), eventuali collegamenti con altri sistemi, documentazione contrattuale disponibile (ad es. contratti standard di adesione al sistema);
- con un preavviso non inferiore ai 6 mesi prima della fine dell'operatività, ove programmata: data di cessazione, strategia di uscita e implicazioni sui sistemi/servizi gestiti (in particolare, se la cessazione riguarda la totalità o parte dell'attività, quali comunicazioni saranno indirizzate ai partecipanti e quali azioni saranno intraprese nel periodo transitorio per garantire un'ordinata uscita dal mercato/disattivazione del servizio), e, laddove rilevante, operazione societaria straordinaria nel cui contesto si inquadra la cessazione.

1.2 Fornitori di infrastrutture o servizi tecnici

Ai sensi dell'art. 19 del Provvedimento, in occasione dell'inizio, della fine dell'operatività e di modifiche significative della stessa, i fornitori di infrastrutture o servizi tecnici trasmettono alla Banca d'Italia[5] le informazioni seguenti:

- con un preavviso non inferiore ai 3 mesi prima dell'inizio dell'operatività: data, denominazione della società e indicazione dei servizi o delle infrastrutture offerti, forma giuridica, indirizzo della sede legale nonché, ove diverso, anche della sede operativa, indirizzo email e PEC, soggetti portatori di interesse (soci, sistemi di pagamento e/o prestatori di servizi di pagamento serviti), comparto servito (dettaglio/ingrosso), servizi offerti e relativa descrizione, referenti (contatto principale e alternativo, posizioni ricoperte, email e numeri di telefono), documentazione contrattuale disponibile (es. contratti standard di adesione al servizio);
- con un congruo preavviso prima dell'implementazione di modifiche significative dell'operatività: data di implementazione delle modifiche e implicazioni sui servizi forniti (incluse le comunicazioni che saranno indirizzate agli utilizzatori e le azioni che saranno intraprese nel periodo transitorio);

[5] Anche in assenza della notifica, resta ferma la possibilità per la Banca di richiedere informazioni agli operatori i cui servizi potrebbero rientrare nell'ambito applicativo del Provvedimento.

- con un preavviso non inferiore ai 6 mesi prima della fine dell'operatività: data di cessazione delle attività e, solo per i fornitori critici, strategia di uscita e implicazioni sui servizi forniti (in particolare, se la cessazione riguarda la totalità o parte dell'attività, quali comunicazioni saranno indirizzate agli utilizzatori e quali azioni saranno intraprese nel periodo transitorio), nonché, laddove rilevante, operazione societaria straordinaria nel cui contesto si inquadra la cessazione.

Ai fini della notifica di cui sopra, per inizio e fine dell'operatività si intende l'avvio/la cessazione di un'offerta di servizi nel comparto dei pagamenti secondo le modalità e in presenza delle condizioni indicate dal Provvedimento (indipendentemente dai comparti - al dettaglio o all'ingrosso - serviti).

La notifica è trasmessa in formato elettronico all'indirizzo di posta elettronica certificata notifica.sorveglianza@pec.bancaditalia.it.

2. Valutazione di criticità dei fornitori di infrastrutture strumentali tecnologiche o di rete

Sulla base di quanto previsto dall'art. 20 del Provvedimento, i fornitori di infrastrutture o servizi tecnici considerati critici dalla Banca d'Italia sono assoggettati ai requisiti di sorveglianza.

A tal fine la Banca d'Italia esamina le informazioni contenute nelle notifiche di inizio operatività o di modifiche significative della stessa, nonché ogni altra informazione in suo possesso per valutare la criticità dei fornitori di infrastrutture o servizi tecnici ai sensi dell'art. 20 del Provvedimento.

La Banca d'Italia pubblica sul proprio sito web l'elenco dei fornitori ritenuti critici ai sensi dell'art. 20 del Provvedimento.

2.1 Procedimento amministrativo per la valutazione della criticità di un fornitore

Un fornitore è qualificato come critico con un provvedimento della Banca d'Italia, adottato all'esito di un procedimento amministrativo d'ufficio. Si applicano, in quanto compatibili, le disposizioni del Regolamento generale sui procedimenti amministrativi della Banca d'Italia.

L'unità organizzativa responsabile del procedimento è il Servizio Supervisione mercati e sistemi di pagamento, ad eccezione dei procedimenti amministrativi relativi ai fornitori che gestiscono interfacce multi-operatore (come definite all'art. 19, comma 1, lett. e) del Provvedimento) per i quali l'unità organizzativa responsabile è il Servizio Strumenti e servizi di pagamento al dettaglio. Il Responsabile del procedimento è il Capo del Servizio competente o, in caso di assenza o impedimento, il suo Vice.

Comunicazioni relative al procedimento

Le comunicazioni relative al procedimento avvengono via PEC, salvo i casi di oggettiva impossibilità.

Primo atto d'impulso e termine del procedimento

La Banca d'Italia avvia il procedimento quando, all'esito di un preliminare accertamento delle informazioni in suo possesso, ricevute attraverso la notifica di inizio attività o di modifiche significative della stessa effettuata dal fornitore ai sensi dell'art. 19 o apprese diversamente, ritiene che possano sussistere i presupposti per la qualificazione di un fornitore come critico.

Fatte salve le cause di sospensione o interruzione, il procedimento si conclude nel termine di 90 giorni dall'avvio, con un provvedimento di qualificazione del fornitore come critico o con un provvedimento di archiviazione.

In seguito all'adozione del provvedimento di qualificazione del fornitore come critico la Banca d'Italia aggiorna l'elenco dei fornitori critici disponibile sul proprio sito web.

2.2 Rivalutazione della criticità di un fornitore

La Banca d'Italia monitora nel continuo l'evoluzione del mercato dei servizi tecnici a supporto del sistema dei pagamenti italiano. Sulla base delle informazioni acquisite, essa può rivalutare la criticità dei fornitori[6].

A tal fine, la Banca d'Italia avvia un procedimento che si svolge secondo le disposizioni sopra richiamate[7] e, laddove necessario, aggiorna l'elenco dei fornitori critici disponibile sul proprio sito web.

3. Obblighi informativi

3.1 Disposizioni di carattere generale

In aggiunta alle informazioni di cui al par. 1 il Provvedimento prevede specifici obblighi informativi in capo ai gestori di sistemi di pagamento e ai fornitori critici individuati dalla Banca d'Italia ai sensi rispettivamente degli art. 13 e 22.

Le informazioni devono essere fornite dai gestori in occasione dell'inizio dell'operatività e dai fornitori a seguire la loro qualificazione come critici, secondo le tempistiche di volta in volta definite dalla Banca d'Italia sulla base di un confronto con i soggetti sorvegliati. Le informazioni devono essere aggiornate annualmente, entro il mese di aprile per i gestori e per i fornitori critici, nonché in occasione di modifiche rilevanti dei profili architetturali, funzionali, tecnico-operativi, economici e giuridici dell'operatività. La documentazione da fornire in tema di resilienza cibernetica è descritta in modo dettagliato nell'appendice alla presente guida sulla base dei contenuti minimi richiesti dal Provvedimento ai gestori di sistemi di pagamento, ai sensi degli artt. 5, comma 1, e 13, comma 1, lett. i), e ai fornitori critici, ai sensi dell'art. 22, comma 1, lett. g).

I gestori e i fornitori critici trasmettono alla Banca d'Italia la documentazione concernente solamente le attività che ricadono nell'ambito della sorveglianza, e non i documenti e le informazioni già inviati alla Banca d'Italia in adempimento di obblighi informativi previsti da altra normativa vigente. In tale ultimo caso dovrà essere fornita idonea evidenza dell'invio avvenuto in precedenza. La Banca d'Italia, nell'esercizio dei poteri di sorveglianza e anche nell'ambito della cooperazione con l'Eurosistema, può richiedere ai soggetti sorvegliati ogni altra informazione e documenti ritenuti utili.

Tutta la documentazione e le informazioni sopra indicate sono trasmesse esclusivamente in formato

[6] La Banca d'Italia si avvale, tra l'altro, dello scambio informativo con ciascun fornitore e delle informazioni apprese attraverso le attività di sorveglianza sul singolo fornitore critico.

[7] Il procedimento si conclude a seconda dei casi con un provvedimento di qualificazione del fornitore come critico, di cancellazione dall'elenco dei fornitori critici o di archiviazione laddove vengano confermate le valutazioni precedentemente svolte.

elettronico agli indirizzi di posta elettronica certificata comunicati dalla Banca d'Italia.

3.2 Malfunzionamenti / *Incident Reporting*

I gestori di sistemi di pagamento e i fornitori critici assicurano la gestione di malfunzionamenti e la connessa reportistica (ai sensi, rispettivamente, degli artt. 5 comma 2 e 13 comma 1, lett. h), e dell'art. 22 comma 1 lett. f) del Provvedimento).

Per malfunzionamento, ai sensi dell'art. 1 del Provvedimento, si intende l'arresto dell'operatività del sistema, gli errori procedurali, il peggioramento dei tempi di elaborazione delle operazioni di pagamento, la perdita di riservatezza e l'alterazione non autorizzata dei dati trattati. Tale definizione include gli incidenti come definiti dall'Autorità bancaria europea (ABE)[8].

In caso di malfunzionamenti, i gestori di sistemi di pagamento e i fornitori critici:

a) assicurano la tempestiva individuazione degli eventi di rischio, in linea con le migliori prassi a livello internazionale;
b) classificano gli eventi secondo i criteri comunicati dalla Banca d'Italia;
c) notificano singolarmente gli incidenti gravi, secondo gli schemi di reportistica e i tempi comunicati dalla Banca d'Italia;
d) ne analizzano e rimuovono le cause, provvedendo al ripristino della regolare operatività; in linea con le migliori prassi a livello internazionale, adottano misure per evitare il ripetersi degli eventi e, laddove opportuno, comunicano ai clienti o al pubblico specifiche informazioni sull'evento occorso.

La classificazione di gravità dell'incidente per i gestori di sistemi di pagamento e i fornitori critici va effettuata in base a criteri - che saranno resi noti in dettaglio ai soggetti sorvegliati con apposita comunicazione - basati sui seguenti fattori: i) numero di transazioni interessate, ii) numero di partecipanti interessati, iii) tempi di interruzione del servizio, iv) ritardo in eventuali tempi di *cut-off*, v) coinvolgimento, anche solo probabile, del *Chief Information Officer* (o ruolo analogo) nella risoluzione dell'incidente, vi) impatti su altre infrastrutture del mercato finanziario/sistemi di pagamento e vii) impatto reputazionale sull'operatore.

Il processo segnaletico degli incidenti classificati "gravi" si articola in tre distinti momenti: i) il report iniziale, contenente informazioni preliminari, da inviare entro 3 ore dal momento in cui l'incidente è stato rilevato[9]; ii) il report intermedio, che include informazioni di maggior dettaglio sul malfunzionamento, da trasmettere entro 3 giorni lavorativi dall'invio del primo report; iii) il report finale da inviare entro massimo 2 settimane dalla ripresa della normale operatività.

[8] In tale contesto si fa riferimento agli "incidenti operativi o di sicurezza" così come definiti dagli Orientamenti aggiornati dell'ABE "in materia di segnalazione dei gravi incidenti ai sensi della PSD2" (EBA/GL/2021/03), vale a dire: "Singolo evento o serie di eventi collegati non pianificati dal prestatore di servizi di pagamento che ha o probabilmente avrà un impatto negativo su integrità, disponibilità, riservatezza, e/o autenticità dei servizi connessi ai pagamenti.".

[9] In caso il malfunzionamento non sia immediatamente classificato come grave secondo i citati criteri, le tempistiche del processo di notifica decorrono dal momento in cui il malfunzionamento è classificato come grave.

La segnalazione alla Banca d'Italia deve essere trasmessa secondo le istruzioni e gli schemi di segnalazione (report iniziale, intermedio, finale) resi disponibili dalla Banca d'Italia con apposita comunicazione ai soggetti sorvegliati, che include anche la specifica dei citati criteri e delle soglie per la classificazione di gravità[10], nonché la casella PEC dedicata.

I soggetti sorvegliati trasmettono le segnalazioni sugli incidenti gravi alla casella PEC dedicata specificando nell'oggetto del messaggio: i) il tipo di report (iniziale, intermedio, finale); ii) il tipo di incidente e iii) l'ente segnalante.

In aggiunta alle segnalazioni sugli incidenti gravi, i gestori di sistemi di pagamento e i fornitori critici redigono una relazione annuale su tutti i malfunzionamenti occorsi durante l'anno, a prescindere dalla loro gravità, che dovrà contenere, tra l'altro, un'analisi delle caratteristiche degli eventi, della relativa classificazione e della loro frequenza, nonché descrivere le misure di rimedio adottate. La relazione viene trasmessa alla Banca d'Italia annualmente, entro fine aprile, agli indirizzi di posta comunicati.

3.3 Dati statistici

I soggetti sorvegliati trasmettono i dati statistici ai sensi degli artt. 13 lett. h) e 22 lett. f) del Provvedimento sulla base degli schemi segnaletici e secondo le modalità e i tempi di invio che saranno individualmente comunicati dalla Banca d'Italia, al fine di tener conto della specifica attività svolta dall'operatore. Gli schemi segnaletici sono aggiornati periodicamente tenendo conto dell'evoluzione del mercato e del quadro normativo.

Le segnalazioni hanno ad oggetto, in generale, le operazioni gestite e i relativi dettagli, quali ad esempio: tipo di strumento trattato o procedura utilizzata e attori coinvolti nella transazione (PSP[11] ed eventuali altre infrastrutture). Per i gestori di sistemi di pagamento, le transazioni sono aggregate a livello giornaliero e mensile, nonché ripartite tra inviate e ricevute per ciascun partecipante.

Per i gestori di sistemi di clearing di cui alla Guida per gli operatori del sistema di compensazione BI-COMP, l'obbligo informativo di cui all'art. 13 lettera h si intende assolto con l'invio alla Banca d'Italia dei dati statistici previsti dall'allegato C4 della Guida citata.

I fornitori critici che gestiscono interfacce multi-operatore inviano le informazioni statistiche sulla base degli schemi forniti dalla Banca d'Italia e secondo le seguenti modalità:

- su base semestrale, sono inviati i dati sulla partecipazione e sull'attività delle piattaforme, con dettagli su adesione dei PSP di 'radicamento' del conto, numero delle "terze parti"[12] che hanno avuto accesso ai conti, volumi di operatività, numero delle chiamate alle interfacce API, tempi di risposta,

[10] Per quanto riguarda i fornitori critici, laddove necessario, la Banca d'Italia definisce, sulla base di interlocuzioni bilaterali, gli eventuali adattamenti allo schema di segnalazione.

[11] Avendo riguardo alla modalità di partecipazione diretta o indiretta o alla loro raggiungibilità attraverso il sistema.

[12] Confronta art. 1 comma 1 lett. (o) del Provvedimento; oltre a quelle sui prestatori di servizi di informazione sui conti e di disposizione di ordini di pagamento potranno essere richieste le informazioni relative ai prestatori di servizi di emissione carte senza diretta visibilità del conto del cliente (servizio che consente all'emittente carta, tramite interrogazione on-line con esito OK/KO, di verificare se un dato pagamento ha capienza sul conto del cliente).

disponibilità del servizio, dispute. Laddove è possibile, le rilevazioni sono distinte per tipologia di servizio (servizi di informazione sui conti e di disposizione di ordini di pagamento), per tipologia di PSP (banca, IP o IMEL);

- su base mensile, le informazioni relative alle richieste di supporto (ticket) ricevute sia dai PSP di 'radicamento' del conto sia dalle terze parti, con indicazione della competenza del ticket e dei tempi di gestione[13].

4. Attività di sorveglianza

La Banca d'Italia svolge la sorveglianza secondo un principio di proporzionalità, avuto riguardo alla dimensione, alla complessità operativa, al profilo di rischio, alla natura dell'attività svolta e alla tipologia dei servizi prestati dal soggetto sorvegliato.

La Banca d'Italia definisce le attività di sorveglianza nei confronti dei gestori e dei fornitori critici nell'ambito della più ampia cornice di sorveglianza prevista dall'Eurosistema, da cui promanano le linee di indirizzo, l'approccio basato sul rischio, nonché gli strumenti adottati.

Le attività di sorveglianza sono avviate dalla Banca d'Italia nei confronti dei gestori a partire dalla ricezione della notifica di inizio attività, per i fornitori critici all'esito della valutazione di criticità di cui al paragrafo 2. Esse consentono di verificare la conformità dei gestori e dei fornitori critici alle disposizioni del Provvedimento, attraverso l'analisi cartolare e/o la richiesta di esercizi di autovalutazione. La Banca d'Italia analizza le informazioni ricevute dagli operatori (vedi paragrafo 3) o apprese diversamente, e, ove necessario, richiede documentazione integrativa.

Ove ritenuto opportuno, e in applicazione del principio di proporzionalità, la Banca d'Italia può elaborare programmi mirati di controllo per ciascun operatore soggetto a sorveglianza, finalizzati ad approfondire specifici profili di rischio identificati sulla base delle informazioni ricevute ai sensi degli artt. 13 e 22. L'operatore è informato dell'avvio di un programma mirato di sorveglianza mediante apposita comunicazione via PEC, contenente indicazioni sui relativi tempi e contenuti.

La Banca d'Italia prevede di norma un incontro all'anno con ciascun soggetto sorvegliato, nel corso del quale sono discusse le iniziative correnti e prospettiche degli operatori nonché presentate le eventuali valutazioni svolte della sorveglianza. La Banca d'Italia può richiedere incontri - a diversi livelli di rappresentatività e/o con specifiche funzioni aziendali - dedicati ad approfondimenti specifici su strategie, linee evolutive e aspetti tecnici di funzionamento del sistema/dei servizi offerti o su eventuali malfunzionamenti/incidenti occorsi.

Infine, la Banca d'Italia dispone degli ulteriori poteri previsti dall'art. 146 del TUB nei confronti dei soggetti sorvegliati, compreso quello di disporre ispezioni.

[13] Sono esclusi quelli relativi ad attività di mero *testing*.

4.1 Attività correnti

La Banca d'Italia, ai fini dello svolgimento della sorveglianza, esamina le informazioni raccolte in base agli obblighi informativi di cui agli art. 13 e 22 del Provvedimento (ad es. il piano strategico operativo, la relazione sui malfunzionamenti occorsi durante l'anno, i dati statistici, la strategia di resilienza cibernetica ed il relativo *framework*), nonché le ulteriori evidenze documentali richieste.

In tale ambito, la Banca d'Italia esamina le modifiche al sistema o ai servizi offerti (a titolo esemplificativo, nuove funzionalità di business, riprogettazione dell'architettura IT, modifiche alle regole del sistema, ecc.) comunicate dal soggetto sorvegliato al fine di verificarne la rispondenza ai requisiti di sorveglianza applicabili. Nel caso in cui il cambiamento fosse valutato rilevante, la Banca avvia un esercizio specifico di *assessment* (vedi paragrafo seguente).

4.2 Attività periodiche e mirate

Nell'ambito delle attività di sorveglianza, inclusi gli specifici programmi di sorveglianza comunicati di volta in volta, la Banca d'Italia può condurre esercizi di valutazione rispetto a: 1) tutti i requisiti del Provvedimento (cd. *assessment* completo) o 2) un sottoinsieme di questi (cd. *assessment* mirati). Di norma, un *assessment* mirato viene avviato in occasione della comunicazione da parte di un soggetto sorvegliato di modifiche rilevanti dei profili architetturali, funzionali, tecnico-operativi, economici o giuridici dei servizi offerti ed è volto a valutare eventuali impatti di tali modifiche sui requisiti di affidabilità ed efficienza. La Banca d'Italia può altresì decidere di condurre un *assessment* mirato su uno specifico profilo di rischio, considerato rilevante, con l'obiettivo di avere adeguata rassicurazione sui presidi in essere e, se necessario, indurre gli opportuni cambiamenti.

Al termine di ogni *assessment* la Banca d'Italia fornisce al soggetto sorvegliato un riscontro sull'esito delle valutazioni.

Infine, la Banca d'Italia può disporre *assessment* nell'ambito di esercizi coordinati nell'ambito dell'Eurosistema sulla base del *framework* di sorveglianza applicabile.

5. Strumentario utilizzato per la valutazione di conformità con il Provvedimento

La Banca d'Italia adotta le metodologie e le prassi di sorveglianza dell'Eurosistema, opportunamente integrate e adattate in linea con il quadro normativo nazionale e per tenere conto delle specificità del mercato di riferimento.

Tale impostazione mira ad assicurare parità di trattamento e confrontabilità dei risultati a livello europeo. Si fa riferimento, in particolare, ai seguenti strumenti e metodologie:

- *Assessment methodology* dell'Eurosistema per i sistemi di pagamento[14], integrata e adattata per i profili di: assetto organizzativo e dei controlli, esternalizzazione e rischio di impresa;
- *Assessment methodology* dell'*Annex F* dei PFMI[15] per i fornitori di servizi critici, integrata e adattata per i profili di: assetto organizzativo e dei controlli, esternalizzazione e rischio di impresa;

Con riferimento ai rischi cibernetici la Banca d'Italia adotta:

- la *Cyber Resilience Survey*[16].
- le *Cyber Resilience Oversight Expectations* (CROE)[17]. Il livello di aspettative (base, intermedio, avanzato) è stabilito dalla Banca d'Italia sulla base di un approccio armonizzato nell'ambito dell'Eurosistema, che tiene conto del principio di proporzionalità e della rischiosità, per il settore finanziario, del soggetto sottoposto a valutazione.

Con riferimento ai fornitori critici che gestiscono interfacce multi-operatore, la Banca d'Italia tiene anche conto del Regolamento delegato (UE) n. 2018/389 della Commissione del 27 novembre 2017, nonché di Linee guida, Pareri, Q&A e degli altri documenti pubblicati dall'Autorità bancaria europea (ABE).

6. Modalità di svolgimento degli *assessment* e del relativo *follow-up*

Nello svolgimento delle attività di cui al paragrafo 4.2, la Banca d'Italia può richiedere al gestore e al fornitore critico di effettuare esercizi di autovalutazione rispetto ai requisiti di sorveglianza, secondo le metodologie di cui al paragrafo 5. Dopo aver esaminato le eventuali autovalutazioni e la documentazione a supporto fornita dal soggetto sorvegliato, la Banca d'Italia redige un rapporto e ne condivide i risultati con il soggetto stesso.

Completate le fasi di analisi, anche tramite il dialogo con gli operatori, la Banca d'Italia formula un giudizio sulla conformità del soggetto ai requisiti di sorveglianza.

A fronte di non conformità, ferma restando la possibilità, nei casi più gravi, di esercitare i poteri di cui all'art. 146, comma 2, lettera d) del TUB, la Banca d'Italia formula raccomandazioni al soggetto sorvegliato affinché ponga in essere le misure correttive necessarie. In particolare, viene chiesto al soggetto di definire un piano di azione con le misure che esso intende adottare e i tempi previsti per la loro implementazione. Il piano

[14] Tale metodologia prende a riferimento l'*assessment methodology* sviluppata dal CPMI-IOSCO in relazione ai PFMI, tenendo conto delle prassi già adottate dall'Eurosistema per la sorveglianza dei sistemi di pagamento, e include il riferimento alle CROE per i profili di sicurezza cibernetica. La metodologia copre i principali profili di rischio a cui può essere esposta un'infrastruttura di mercato. https://www.ecb.europa.eu/pub/pdf/other/ecb.revisedassessmentmethodologyforpaymentsystems.pdf.

[15] Tale metodologia consente di valutare l'affidabilità di un fornitore critico di servizi che supporta l'operatività di una infrastruttura di mercato. Essa si articola in una serie di previsioni sul rischio operativo rivolte a un fornitore critico di servizi. Assessment methodology for the oversight expectetions applicable to critical service providers https://www.iosco.org/library/pubdocs/pdf/IOSCOPD468.pdf.

[16] È uno strumento di prima diagnosi, sviluppato dall'Eurosistema, nella forma di un questionario relativo alla gestione, ai processi e alle procedure di resilienza cibernetica poste in essere dai soggetti sottoposti a sorveglianza.

[17] Sono uno strumento di valutazione approfondita della postura di resilienza cibernetica del soggetto sorvegliato. Il loro utilizzo presuppone la comunicazione della Banca d'Italia al soggetto sorvegliato del livello di aspettative atteso: i) *evolving* (base), ii) *advancing* (intermedio), iii) *innovating* (avanzato). https://www.ecb.europa.eu/paym/pdf/cons/cyberresilience/Cyber_resilience_oversight_expectations_for_financial_market_infrastructures.pdf.

forma oggetto di confronto con la funzione di sorveglianza che ne monitora l'attuazione nell'ambito delle attività correnti.

Anche in caso di conformità, la Banca d'Italia si riserva la facoltà di formulare raccomandazioni volte a potenziare l'affidabilità e l'efficienza del soggetto sorvegliato.

APPENDICE

Documentazione in tema di resilienza cibernetica

I gestori di sistemi di pagamento (ai sensi degli artt. 5 comma 1 e 13 comma 1 lett. i)) e i fornitori critici (ai sensi dell'art. 22 comma 1 lett. g)) devono trasmettere alla Banca d'Italia la strategia di resilienza cibernetica, con connesse procedure di implementazione.

Per strategia di resilienza cibernetica si intende un documento in cui sono individuati gli obiettivi di resilienza cibernetica dell'operatore i princìpi e i piani a medio termine per raggiungere detti obiettivi e gestire il rischio cibernetico[18]. Le connesse procedure di implementazione sono articolate in un quadro di riferimento di resilienza cibernetica (*framework*) e possono assumere una forma e un contenuto diversi in funzione dei servizi forniti e dell'impianto organizzativo e regolamentare adottato dal singolo soggetto[19]. Tale quadro di riferimento deve includere:

a. una chiara allocazione di ruoli e responsabilità, secondo le tre linee di difesa (operativa, di gestione dei rischi e di audit);
b. un processo di valutazione del rischio cibernetico, integrato nel più generale processo di gestione del rischio aziendale;
c. un processo di identificazione delle funzioni critiche;
d. politiche e procedure sulla gestione della sicurezza cibernetica;
e. un processo di gestione delle utenze, dei ruoli e dei diritti di accesso, basato sui princìpi del "*need to know*" e "*least privilege*";
f. un processo di gestione dei cambiamenti;
g. politiche e procedure in tema di gestione degli incidenti e connessi piani di risposta.

Inoltre, nell'ambito della documentazione richiesta ai sensi degli artt. 13 comma 1 lett. r) e 22 comma 1 lett. i), riguardante la gestione dei rischi operativi, i gestori e i fornitori critici inviano:

h. un programma completo di verifiche e relativi esiti, che può includere diverse metodologie di *testing*[20] e scenari di rischio cibernetico;
i. l'elenco dei processi individuati come critici e i relativi obiettivi in termini di disponibilità, affidabilità, tempo di ripristino e punto di ripristino;
j. l'esito dell'esercizio di autovalutazione del sistema di gestione dei rischi operativi, con particolare focus sulla resilienza cibernetica;

[18] Cfr. Committee on Payments and Market Infrastructures - Board of the International Organization of Securities Commissions (CPMI-IOSCO), "*Guidance on cyber resilience for financial market infrastructures*" (anche *Cyber Guidance*), 2016.

[19] Ad esempio, le procedure di implementazione possono essere formalizzate in uno o più documenti con diverso grado di dettaglio. In particolare, si fa riferimento a politiche, linee guida, prassi e controlli posti in essere dai soggetti per rilevare, identificare, proteggere, rispondere e ripristinare l'attività a fronte del rischio cibernetico.

[20] Ogni soggetto, in base ai rischi identificati e al principio di proporzionalità, può includere diversi strumenti di *testing* e scenari di rischio, quali ad esempio: scansioni di vulnerabilità periodiche e su perimetri più o meno ampi, *penetration tests*, test di sicurezza avanzati (*Threat-Led Penetration Tests*), test di continuità operativa, esercitazioni di tipo *table-top*, etc.

k. i risultati dei test di continuità operativa, con particolare riferimento agli scenari relativi alla resilienza cibernetica, ed eventuali aggiornamenti del piano di continuità operativa e di *disaster recovery*.

Per ulteriori dettagli relativi ai contenuti della documentazione richiesta nella presente appendice e alle eventuali ulteriori informazioni che la Banca d'Italia può richiedere, i gestori e i fornitori critici possono fare riferimento alle citate "CROE"[21].

[21] Cfr. paragrafo 5.