BANCA D'ITALIA
EUROSISTEMA

Servizi di pagamento: risultanze dell'analisi dei rischi operativi e di sicurezza

Codice ABI intermediario/gruppo (*su quattro o cinque cifre*)

Denominazione intermediario/gruppo

Nome e cognome del referente

E-mail referente

Recapito telefonico referente

Ver. 2.0

La circolare 285 “Disposizioni di vigilanza per le banche” e le “Disposizioni di vigilanza per gli istituti di pagamento e gli istituti di moneta elettronica” richiedono che i prestatori di servizi di pagamento (PSP) redigano annualmente una relazione sulle risultanze dell’analisi dei rischi operativi e di sicurezza relativi ai servizi di pagamento.

Il presente modulo, debitamente compilato (in lingua italiana oppure in inglese), consente di rappresentare in forma sintetica e standardizzata le suddette risultanze alla Banca d’Italia.

Il modulo va compilato dalle capogruppo dei gruppi bancari e dalle banche individuali, dagli istituti di pagamento e di moneta elettronica non appartenenti a gruppi, dalle succursali di banche, istituti di pagamento e di moneta elettronica extracomunitari. I gruppi bancari possono fornire un singolo modulo o più moduli a seconda che le soluzioni siano omogenee all’interno del gruppo o specifiche per ciascuna entità.

Ove applicabile, il presente modulo va accompagnato (una tantum) dal modulo di "Esenzione dall’autenticazione forte del cliente per i pagamenti corporate ai sensi dell’art. 17 del Regolamento (eu) 2018/389, disponibile sul sito internet della Banca d'italia.

Il modulo, firmato elettronicamente dal legale rappresentante o accompagnato da una lettera firmata dal legale rappresentante, va inviato alla casella PEC RIV@pec.bancaditalia.it, recando nell’oggetto il codice ABI dell'intermediario e la dicitura “Relazione analisi rischi operativi e di sicurezza servizi di pagamento”. Si raccomanda di compilare il modulo utilizzando Acrobat Reader e di non modificarne il formato prima dell'invio.

Richieste relative a chiarimenti sulla procedura e sulle modalità di compilazione del presente modulo possono essere inoltrate alla casella di email VIG_PSD2@bancaditalia.it

Sezione 1 (Riservata ai gruppi bancari)

Elenco dei prestatori di servizi di pagamento (PSP) appartenenti al gruppo per cui si applicano le risposte al presente questionario

ABI PSP	DENOMINAZIONE PSP

Note (da utilizzare anche per inserire ulteriori PSP nel caso i campi nella tabella non siano sufficienti)

Sezione 2 - Valutazione dei rischi operativi e di sicurezza relativi ai servizi di pagamento offerti

[Nel resto del documento per valutazione dei rischi si intenderà "Valutazione dei rischi operativi e di sicurezza relativi ai servizi di pagamento"]

1. Indicare i servizi di pagamento offerti[1] e i relativi canali di fruizione utilizzati dai clienti:

	Filiali / sede propria	Esercizi conven-zionati	Rete di agenti	Phone banking	POS	Internet (Web)	Mobile (APP)	Online merch-ant	ATM	Note
1.Servizi che permettono di depositare il contante su un conto di pagamento nonché tutte le operazioni richieste per la gestione di un conto di pagamento.[2]										
2.Servizi che permettono prelievi in contante da un conto di pagamento nonché tutte le operazioni richieste per la gestione di un conto di pagamento.										
3.Esecuzione di operazioni di pagamento, incluso il trasferimento di fondi, su un conto di pagamento presso il PSP dell'utente o presso un altro PSP.										
4. Esecuzione di operazioni di pagamento quando i fondi rientrano in una linea di credito accordata ad un utente di servizi di pagamento.										
5.Emissione di strumenti di pagamento e/o convenzionamento di operazioni di pagamento.										
6.Rimessa di denaro (money transfer).										
7.Servizi di disposizione di ordine di pagamento (PIS).*										
8.Servizi di informazione sui conti (AIS).*										

*** Per servizi PIS e AIS si intendono quelli svolti con ruolo attivo di terza parte per l'accesso ai conti dei clienti detenuti presso altri PSP. Compilare le righe relative solo nel caso il PSP svolga tale ruolo.**

[1] Per la classificazione dei servizi di pagamento si fa riferimento all'Allegato 1 della PSD2.

[2] In tali servizi sono ricompresi i servizi di cassa tradizionali, riconducibili ai servizi di filiale.

2. È stata formalizzata una metodologia per la valutazione dei rischi?

◯ **SI** **dal** _____ **Indicare la data dell'ultima revisione** _____

◯ **NO**

Note [indicare, tra l'altro, se la metodologia è generale o specifica per i servizi di pagamento]

_____

3. Figure aziendali coinvolte nel processo di valutazione dei rischi, specificando il ruolo RACI* assunto nel processo di valutazione dei rischi:

Funzione aziendale	**Addetto/Esecutore (*Responsible*)**	**Responsabile (*Accountable*)**	**Consultato (*Consulted*)**	**Informato (*Informed*)**
Funzioni di business	◯	◯	◯	◯
Funzione ICT	◯	◯	◯	◯
Sicurezza informatica	◯	◯	◯	◯
Risk management	◯	◯	◯	◯
Revisione interna	◯	◯	◯	◯

* La matrice RACI prende la propria denominazione dalle iniziali dei ruoli previsti in lingua inglese per l'esecuzione delle attività dei processi aziendali. I ruoli previsti dalla matrice sono:
Responsible (R) : Addetto/Esecutore, è colui che esegue e assegna l'attività.
Accountable (A) : Responsabile, è colui che ha la responsabilità sul risultato dell'attività. A differenza degli altri 3 ruoli, per ciascuna attività deve essere univocamente assegnato.
Consulted (C) : Consultato, è la persona che aiuta e collabora con il Responsible per l'esecuzione dell'attività.
Informed (I) : Informato, è colui che deve essere informato al momento dell'esecuzione dell'attività.

Note (indicare di seguito, tra l'altro, altre funzioni se necessario)

_____

4. Metodo adottato per la valutazione dei rischi:

◯ **Metodo quantitativo**

◯ **Metodo qualitativo**

◯ **Metodo quali-quantitativo**

Note

5. **Frequenza di aggiornamento della valutazione dei rischi:**

- ◯ **Annuale**
- ◯ **Semestrale**
- ◯ **Trimestrale**
- ◯ **Altro, specificare**

Note

6. **Fattori che determinano una valutazione dei rischi ulteriore rispetto all'aggiornamento periodico:**

- ☐ **Cambiamenti (ICT - inclusi di sicurezza, organizzativi)**
- ☐ **Incidenti operativi o di sicurezza**
- ☐ **Evidenza di nuove minacce**
- ☐ **Altro, specificare**

Note

7. **Indicare la data di riferimento dell'ultima valutazione dei rischi svolta:**

Note

8. **La valutazione dei rischi ha dato luogo ad un report portato all'attenzione degli organi con funzione di gestione o di supervisione strategica?**

◯ **SI** ◯ **NO**

Note [*nel caso in cui la valutazione dei rischi abbia dato luogo ad apposita reportistica, si chiede di fornire indicazione circa il raccordo, se presente, con altri documenti aziendali relativi alle politiche di gestione dei rischi (ad es, ICAAP, RAF, Relazioni funzioni di controllo, ecc.)*]

9. **Esiste un inventario aggiornato:**

- ☐ delle funzioni aziendali
- ☐ dei processi
- ☐ delle risorse informatiche di supporto

Data ultimo aggiornamento

Frequenza di aggiornamento

Note

10. **L'intermediario ha classificato sotto il profilo della criticità (Riservatezza, Integrità, Disponibilità):**

- ☐ **le funzioni aziendali**
- ☐ **i processi**
- ☐ **le risorse informatiche di supporto**

Note

11. Indicare eventuali servizi di pagamento, processi o risorse informatiche che li supportano esclusi dalla valutazione dei rischi; descrivere i motivi alla base dell'esclusione.

12. Indicare l'ammontare in euro delle perdite operative associate ai servizi di pagamento osservate nell'anno precedente[3]

Note

13. Informazioni integrative [*utilizzare questo spazio per fornire informazioni che non è stato possibile dare nel resto del questionario***]**

[3] Per perdite operative si intendono quelle derivanti "da processi interni, persone e sistemi inadeguati o falliti o da eventi esterni. Questa definizione include il rischio legale, ma esclude il rischio strategico e reputazionale". La stima, laddove necessario, può essere effettuata "on a best-effort basis" e può includere la perdita contabilizzata su base annuale o, se maggiore e in via prudenziale, una stima judgmental (possono essere utili a tal fine eventuali valutazioni effettuate in sede ICAAP per la quantificazione del capitale interno in condizioni ordinarie e stressate). Il campo note di seguito è a disposizione per esplicitare: i) la ragione alla base dell'impossibilità di quantificare il suddetto ammontare; ii) il criterio adottato per la quantificazione (contabile/judgmental); iii) altre informazioni utili alla Vigilanza per una maggiore comprensione del dato riportato.

14. Descrivere in sintesi le risultanze dell'analisi dei rischi operativi e di sicurezza relativi ai servizi di pagamento; esprimere una valutazione dell'adeguatezza delle misure di riduzione del rischio e dei meccanismi di controllo realizzati in risposta ai rischi identificati (max 5000 caratteri)[4].

[4] La trattazione deve essere coerente, in termini di identificazione dei rischi e dei presidi di mitigazione, con quanto riportato in maniera analitica nelle risposte al quesito 15. Deve inoltre, nei limiti dello spazio disponibile, fornire un'illustrazione della metodologia adottata. Evidenziare, laddove possibile, le principali differenze con la valutazione fornita alla Banca d'Italia nel questionario dell'anno precedente.

15. Indicare, al più, i primi 10 rischi operativi e di sicurezza "potenziali" valutati come più rilevanti. Riportare i rischi in ordine di rilevanza (dal più rilevante al meno).

Nel sottolineare che la classificazione dei rischi è nella responsabilità dell'intermediario, è utile specificare che l'intento del questionario è raccogliere informazioni su quali eventi l'intermediario valuta più rilevanti tra quelli che potrebbero verificarsi e produrre impatti negativi sui servizi di pagamento offerti (a titolo di esempio, accessi non autorizzati a dati sensibili, eventi legati a virus informatici, phishing, disastri naturali, malfunzionamenti hardware o software, ecc.). Per quanto riguarda le misure di sicurezza si faccia anche riferimento a quelle indicate negli Orientamenti EBA "Guidelines on security measures for operational and security risks under the PSD2".

Rischio #1 (Più rilevante)

Denominazione e descrizione del rischio

Servizio/i di pagamento interessato/i (cfr. quesito 1 per tassonomia)

- ☐ **1** - Deposito di contante su conto
- ☐ **2** - Prelievi di contante su conto
- ☐ **3** - Esecuzione di operazioni di pagamento su conto
- ☐ **4** - Esecuzione di pagamenti su linee di credito
- ☐ **5** - Issuing e Acquiring carte
- ☐ **6** - Rimessa di denaro
- ☐ **7** - PIS
- ☐ **8** - AIS

Canale/i di fruizione interessato/i (cfr. quesito 1 per tassonomia)

- ☐ Filiali/Sede propria
- ☐ Esercizi convenzionati
- ☐ Rete di agenti
- ☐ Phone banking
- ☐ POS
- ☐ Internet (WEB)
- ☐ Mobile (App)
- ☐ On-line Merchant
- ☐ ATM

[Per i gruppi bancari] Intermediario/i interessato/i

Principali misure di sicurezza adottate prima dell'ultima valutazione dei rischi

Principali aree di miglioramento identificate in fase di ultima valutazione dei rischi

Piano di rimedio (attività già implementate e in corso di realizzazione, tempistiche)

Rischio #2

Denominazione e descrizione del rischio

Servizio/i di pagamento interessato/i (cfr. quesito 1 per tassonomia)

- ☐ **1** - Deposito di contante su conto
- ☐ **2** - Prelievi di contante su conto
- ☐ **3** - Esecuzione di operazioni di pagamento su conto
- ☐ **4** - Esecuzione di pagamenti su linee di credito
- ☐ **5** - Issuing e Acquiring carte
- ☐ **6** - Rimessa di denaro
- ☐ **7** - PIS
- ☐ **8** - AIS

Canale/i di fruizione interessato/i (cfr. quesito 1 per tassonomia)

- ☐ Filiali/Sede propria
- ☐ Esercizi convenzionati
- ☐ Rete di agenti
- ☐ Phone banking
- ☐ POS
- ☐ Internet (WEB)
- ☐ Mobile (App)
- ☐ On-line Merchant
- ☐ ATM

[Per i gruppi bancari] Intermediario/i interessato/i

Principali misure di sicurezza adottate prima dell'ultima valutazione dei rischi

Principali aree di miglioramento identificate in fase di ultima valutazione dei rischi

Piano di rimedio (attività già implementate e in corso di realizzazione, tempistiche)

Rischio #3

Denominazione e descrizione del rischio

Servizio/i di pagamento interessato/i (cfr. quesito 1 per tassonomia)

- ☐ **1** - Deposito di contante su conto
- ☐ **2** - Prelievi di contante su conto
- ☐ **3** - Esecuzione di operazioni di pagamento su conto
- ☐ **4** - Esecuzione di pagamenti su linee di credito
- ☐ **5** - Issuing e Acquiring carte
- ☐ **6** - Rimessa di denaro
- ☐ **7** - PIS
- ☐ **8** - AIS

Canale/i di fruizione interessato/i (cfr. quesito 1 per tassonomia)

- ☐ Filiali/Sede propria
- ☐ Esercizi convenzionati
- ☐ Rete di agenti
- ☐ Phone banking
- ☐ POS
- ☐ Internet (WEB)
- ☐ Mobile (App)
- ☐ On-line Merchant
- ☐ ATM

[Per i gruppi bancari] Intermediario/i interessato/i

Principali misure di sicurezza adottate prima dell'ultima valutazione dei rischi

Principali aree di miglioramento identificate in fase di ultima valutazione dei rischi

Piano di rimedio (attività già implementate e in corso di realizzazione, tempistiche)

Rischio #4

Denominazione e descrizione del rischio

Servizio/i di pagamento interessato/i (cfr. quesito 1 per tassonomia)

- ☐ **1** - Deposito di contante su conto
- ☐ **2** - Prelievi di contante su conto
- ☐ **3** - Esecuzione di operazioni di pagamento su conto
- ☐ **4** - Esecuzione di pagamenti su linee di credito
- ☐ **5** - Issuing e Acquiring carte
- ☐ **6** - Rimessa di denaro
- ☐ **7** - PIS
- ☐ **8** - AIS

Canale/i di fruizione interessato/i (cfr. quesito 1 per tassonomia)

- ☐ Filiali/Sede propria
- ☐ Esercizi convenzionati
- ☐ Rete di agenti
- ☐ Phone banking
- ☐ POS
- ☐ Internet (WEB)
- ☐ Mobile (App)
- ☐ On-line Merchant
- ☐ ATM

[Per i gruppi bancari] Intermediario/i interessato/i

Principali misure di sicurezza adottate prima dell'ultima valutazione dei rischi

Principali aree di miglioramento identificate in fase di ultima valutazione dei rischi

Piano di rimedio (attività già implementate e in corso di realizzazione, tempistiche)

Rischio #5

Denominazione e descrizione del rischio

Servizio/i di pagamento interessato/i (cfr. quesito 1 per tassonomia)

- ☐ **1** - Deposito di contante su conto
- ☐ **2** - Prelievi di contante su conto
- ☐ **3** - Esecuzione di operazioni di pagamento su conto
- ☐ **4** - Esecuzione di pagamenti su linee di credito
- ☐ **5** - Issuing e Acquiring carte
- ☐ **6** - Rimessa di denaro
- ☐ **7** - PIS
- ☐ **8** - AIS

Canale/i di fruizione interessato/i (cfr. quesito 1 per tassonomia)

- ☐ Filiali/Sede propria
- ☐ Esercizi convenzionati
- ☐ Rete di agenti
- ☐ Phone banking
- ☐ POS
- ☐ Internet (WEB)
- ☐ Mobile (App)
- ☐ On-line Merchant
- ☐ ATM

[Per i gruppi bancari] Intermediario/i interessato/i

Principali misure di sicurezza adottate prima dell'ultima valutazione dei rischi

Principali aree di miglioramento identificate in fase di ultima valutazione dei rischi

Piano di rimedio (attività già implementate e in corso di realizzazione, tempistiche)

Rischio #6

Denominazione e descrizione del rischio

Servizio/i di pagamento interessato/i (cfr. quesito 1 per tassonomia)

- ☐ **1** - Deposito di contante su conto
- ☐ **2** - Prelievi di contante su conto
- ☐ **3** - Esecuzione di operazioni di pagamento su conto
- ☐ **4** - Esecuzione di pagamenti su linee di credito
- ☐ **5** - Issuing e Acquiring carte
- ☐ **6** - Rimessa di denaro
- ☐ **7** - PIS
- ☐ **8** - AIS

Canale/i di fruizione interessato/i (cfr. quesito 1 per tassonomia)

- ☐ Filiali/Sede propria
- ☐ Esercizi convenzionati
- ☐ Rete di agenti
- ☐ Phone banking
- ☐ POS
- ☐ Internet (WEB)
- ☐ Mobile (App)
- ☐ On-line Merchant
- ☐ ATM

[Per i gruppi bancari] Intermediario/i interessato/i

Principali misure di sicurezza adottate prima dell'ultima valutazione dei rischi

Principali aree di miglioramento identificate in fase di ultima valutazione dei rischi

Piano di rimedio (attività già implementate e in corso di realizzazione, tempistiche)

Rischio #7

Denominazione e descrizione del rischio

Servizio/i di pagamento interessato/i (cfr. quesito 1 per tassonomia)

- ☐ **1** - Deposito di contante su conto
- ☐ **2** - Prelievi di contante su conto
- ☐ **3** - Esecuzione di operazioni di pagamento su conto
- ☐ **4** - Esecuzione di pagamenti su linee di credito
- ☐ **5** - Issuing e Acquiring carte
- ☐ **6** - Rimessa di denaro
- ☐ **7** - PIS
- ☐ **8** - AIS

Canale/i di fruizione interessato/i (cfr. quesito 1 per tassonomia)

- ☐ Filiali/Sede propria
- ☐ Esercizi convenzionati
- ☐ Rete di agenti
- ☐ Phone banking
- ☐ POS
- ☐ Internet (WEB)
- ☐ Mobile (App)
- ☐ On-line Merchant
- ☐ ATM

[Per i gruppi bancari] Intermediario/i interessato/i

Principali misure di sicurezza adottate prima dell'ultima valutazione dei rischi

Principali aree di miglioramento identificate in fase di ultima valutazione dei rischi

Piano di rimedio (attività già implementate e in corso di realizzazione, tempistiche)

Rischio #8

Denominazione e descrizione del rischio

Servizio/i di pagamento interessato/i (cfr. quesito 1 per tassonomia)

- ☐ **1** - Deposito di contante su conto
- ☐ **2** - Prelievi di contante su conto
- ☐ **3** - Esecuzione di operazioni di pagamento su conto
- ☐ **4** - Esecuzione di pagamenti su linee di credito
- ☐ **5** - Issuing e Acquiring carte
- ☐ **6** - Rimessa di denaro
- ☐ **7** - PIS
- ☐ **8** - AIS

Canale/i di fruizione interessato/i (cfr. quesito 1 per tassonomia)

- ☐ Filiali/Sede propria
- ☐ Esercizi convenzionati
- ☐ Rete di agenti
- ☐ Phone banking
- ☐ POS
- ☐ Internet (WEB)
- ☐ Mobile (App)
- ☐ On-line Merchant
- ☐ ATM

[Per i gruppi bancari] Intermediario/i interessato/i

Principali misure di sicurezza adottate prima dell'ultima valutazione dei rischi

Principali aree di miglioramento identificate in fase di ultima valutazione dei rischi

Piano di rimedio (attività già implementate e in corso di realizzazione, tempistiche)

Rischio #9

Denominazione e descrizione del rischio

Servizio/i di pagamento interessato/i (cfr. quesito 1 per tassonomia)

- ☐ **1** - Deposito di contante su conto
- ☐ **2** - Prelievi di contante su conto
- ☐ **3** - Esecuzione di operazioni di pagamento su conto
- ☐ **4** - Esecuzione di pagamenti su linee di credito
- ☐ **5** - Issuing e Acquiring carte
- ☐ **6** - Rimessa di denaro
- ☐ **7** - PIS
- ☐ **8** - AIS

Canale/i di fruizione interessato/i (cfr. quesito 1 per tassonomia)

- ☐ Filiali/Sede propria
- ☐ Esercizi convenzionati
- ☐ Rete di agenti
- ☐ Phone banking
- ☐ POS
- ☐ Internet (WEB)
- ☐ Mobile (App)
- ☐ On-line Merchant
- ☐ ATM

[Per i gruppi bancari] Intermediario/i interessato/i

Principali misure di sicurezza adottate prima dell'ultima valutazione dei rischi

Principali aree di miglioramento identificate in fase di ultima valutazione dei rischi

Piano di rimedio (attività già implementate e in corso di realizzazione, tempistiche)

Rischio #10

Denominazione e descrizione del rischio

Servizio/i di pagamento interessato/i (cfr. quesito 1 per tassonomia)

- ☐ **1** - Deposito di contante su conto
- ☐ **2** - Prelievi di contante su conto
- ☐ **3** - Esecuzione di operazioni di pagamento su conto
- ☐ **4** - Esecuzione di pagamenti su linee di credito
- ☐ **5** - Issuing e Acquiring carte
- ☐ **6** - Rimessa di denaro
- ☐ **7** - PIS
- ☐ **8** - AIS

Canale/i di fruizione interessato/i (cfr. quesito 1 per tassonomia)

- ☐ Filiali/Sede propria
- ☐ Esercizi convenzionati
- ☐ Rete di agenti
- ☐ Phone banking
- ☐ POS
- ☐ Internet (WEB)
- ☐ Mobile (App)
- ☐ On-line Merchant
- ☐ ATM

[Per i gruppi bancari] Intermediario/i interessato/i

Principali misure di sicurezza adottate prima dell'ultima valutazione dei rischi

Principali aree di miglioramento identificate in fase di ultima valutazione dei rischi

Piano di rimedio (attività già implementate e in corso di realizzazione, tempistiche)