Commissione parlamentare di inchiesta
sul sistema bancario, finanziario e assicurativo

L'innovazione tecnologica e la resilienza operativa nel settore finanziario

Audizione del Capo del Dipartimento
Vigilanza bancaria e finanziaria della Banca d'Italia

Giuseppe Siani

Roma, 5 novembre 2026

Signor Presidente, Onorevoli Senatrici, Onorevoli Senatori,

ringrazio anzitutto la Commissione per l'invito. L'innovazione tecnologica e l'intelligenza artificiale (IA) sono oggi tra i principali fattori di trasformazione del settore finanziario e implicano sfide inedite per la solidità degli intermediari, la continuità dei servizi essenziali e la stabilità del sistema economico.

Nel mio intervento, illustrerò come l'evoluzione tecnologica stia modificando l'operatività degli intermediari, creando opportunità e nuove fonti di rischio. Richiamerò inoltre il quadro normativo europeo, le principali evidenze dell'attività di vigilanza e la collaborazione con le altre Autorità.

1. La trasformazione digitale del settore finanziario

La digitalizzazione trasforma strutturalmente l'economia e la finanza, incidendo sul funzionamento di mercati e intermediari. Processi digitali, ampia disponibilità di dati e crescenti capacità di calcolo ridefiniscono l'offerta dei servizi, gli assetti organizzativi, la gestione dei rischi e il rapporto con la clientela.

È cresciuto inoltre il ricorso a fornitori specializzati, in particolare da parte di intermediari di minori dimensioni, per accedere a competenze specialistiche ed economie di scala. Questa scelta offre vantaggi, ma aumenta le dipendenze operative e strategiche e amplifica i rischi esistenti, a causa anche dell'elevata concentrazione del settore. Le esternalizzazioni implicano inoltre complesse catene tecnologiche, con molti soggetti distribuiti su più livelli di subfornitura[1].

Investimenti adeguati e infrastrutture digitali avanzate sono divenuti essenziali per la competitività. Le nostre indagini[2] evidenziano una significativa accelerazione degli investimenti in tecnologie digitali, con rilevanti differenze tra intermediari per livello di sofisticazione delle soluzioni adottate e grado di integrazione nei processi aziendali. Gli investimenti si concentrano presso gli istituti di maggiori

---

1 Nei servizi di pagamento, una delle aree in cui l'innovazione si manifesta più rapidamente, la frammentazione delle attività tra intermediari, piattaforme e fornitori tecnologici può rendere più complessa l'attribuzione delle responsabilità operative e di quelle connesse con la prevenzione e la gestione delle frodi.

2 Si veda ad esempio: https://www.bancaditalia.it/pubblicazioni/indagine-fintech/2025-intermediari/index.html.

dimensioni, ma non mancano realtà più piccole particolarmente avanzate. La quasi totalità delle banche meno significative che hanno partecipato alla raccolta dati del 2026 dichiara di disporre di una strategia digitale[3] e, nei casi più virtuosi, di monitorarne attuazione e benefici.

Il rischio informatico non rappresenta quindi più un profilo meramente tecnico ma permea ormai l'intera operatività finanziaria e incide sulla sostenibilità del modello operativo. La solidità tecnologica ha pertanto assunto un rilievo pari a quello dell'equilibrio economico-patrimoniale.

In uno scenario di minacce mutevoli, interdipendenze crescenti e catene del valore sempre più complesse, gli intermediari mantengono la responsabilità primaria della gestione dei rischi e, a prescindere dalle esternalizzazioni realizzate, devono investire nella prevenzione, rafforzare il controllo delle proprie dipendenze tecnologiche, individuare tempestivamente le vulnerabilità e reagire rapidamente agli incidenti. Le difese adottate devono in ogni caso essere proporzionate alle caratteristiche di ciascun intermediario e coerenti con le strategie aziendali.

Al cambiamento contribuisce anche la rapida diffusione dei modelli di IA, che possono aumentare l'efficienza operativa, migliorare l'elaborazione delle informazioni e favorire lo sviluppo di nuovi servizi. Possono tuttavia rafforzare le capacità degli attori malevoli nell'individuare vulnerabilità, nel ridurre il tempo necessario per compromettere sistemi e servizi, nell'aumentare la sofisticazione delle frodi digitali[4].

La complessità dei modelli IA rende in ogni caso più difficile prevederne i comportamenti, rilevare anomalie e mantenere un controllo efficace dei processi; tendono ad amplificare rischi già esistenti, aumentandone velocità di propagazione e impatto.

2. La normativa europea

La crescente attenzione ai rischi informatici e alle interdipendenze tecnologiche ha modificato radicalmente la logica tradizionale della normativa europea, che non richiede unicamente l'adeguata gestione del rischio per la prevenzione degli

---

[3] Per "strategia digitale" si intende l'insieme delle iniziative degli intermediari per adottare soluzioni tecnologiche volte a offrire prodotti e servizi finanziari digitali, innovare i processi operativi e supportare la conduzione delle attività aziendali.

[4] A livello europeo, i dati evidenziano che il valore delle frodi nei pagamenti è aumentato negli ultimi anni, soprattutto per i bonifici e le carte. Le frodi, sia per valore sia per numero di operazioni, si concentrano nei pagamenti disposti a distanza. (EBA and ECB 2025 Report on Payment Fraud.pdf). Dinamiche analoghe emergono in Italia (Rapporto-operazioni-fraudolente-II-semestre-2025.pdf), dove rilevano le frodi basate sulla manipolazione del pagatore, in particolare nel pagamento dei bonifici.

eventi avversi, ma promuove il rafforzamento della resilienza operativa, ovvero la capacità di preservare le attività fondamentali per la clientela, il mercato e la stabilità finanziaria.

La strategia legislativa europea comprende in primo luogo la direttiva NIS2[5] volta al rafforzamento della sicurezza cibernetica dei settori essenziali e importanti. Per il settore finanziario, il riferimento centrale è invece il *Digital Operational Resilience Act* (DORA)[6], che introduce requisiti più dettagliati e specificamente rivolti alla continuità dei servizi per tutte le società finanziarie dell'Unione.

Il DORA introduce per la prima volta una visione integrata della resilienza operativa, basata su cinque "pilastri": (i) governo e gestione dei rischi relativi alle tecnologie dell'informazione e della comunicazione (*Information and Communication Technology*, ICT), (ii) classificazione e segnalazione degli incidenti, (iii) test di resilienza operativa, inclusi i Threat-Led Penetration Test ('TLPT')[7], (iv) gestione del rischio di terza parte e sorveglianza europea dei fornitori tecnologici critici, (v) scambio di informazioni sulle minacce cibernetiche.

Il Regolamento segue il principio di neutralità tecnologica: non prescrive specifiche soluzioni tecniche, ma definisce obiettivi e requisiti di resilienza indipendenti dagli strumenti utilizzati; richiede in ogni caso di valutare benefici e rischi connessi con l'opzione concreta adottata dagli intermediari. Tale impostazione favorisce l'innovazione e preserva l'efficacia del quadro normativo anche in un contesto di rapida evoluzione e richiede a intermediari e Autorità di prestare costante attenzione all'origine dei rischi, a come questi sono gestiti, ai soggetti che ne sopportano le conseguenze e ai possibili canali di contagio.

Il quadro europeo è stato poi integrato da nuovi interventi normativi destinati a incidere sul settore finanziario e sui compiti delle Autorità di settore. L'AI Act disciplina lo sviluppo e l'utilizzo dei sistemi di IA, particolarmente rilevante per gli utilizzi ad alto rischio, come la valutazione del merito creditizio delle persone

---

5 La Direttiva (UE) 2022/2555 (NIS2) e la Direttiva (UE) 2022/2557 (CER), concernente la resilienza delle entità critiche rispetto ai rischi fisici e ibridi, sono applicate a tutti i settori vitali dell'economia, inclusi il credito e le infrastrutture dei servizi finanziari.

6 Il Regolamento DORA rappresenta l'elemento principale del *Digital Finance Package* presentato dalla Commissione europea nel 2020, che comprende anche la Direttiva (UE) 2022/2556 (di allineamento ai nuovi obblighi introdotti direttamente dal DORA), il Regolamento MiCA sui mercati delle cripto-attività e il regime pilota per le infrastrutture di mercato basate sulla tecnologia a registro distribuito (DLT).

7 Diversamente dai tradizionali test di sicurezza, i *Threat-Led Penetration Test* (TLPT) simulano attacchi condotti con le stesse tecniche utilizzate da aggressori reali e consentono di valutare la capacità dell'intermediario di prevenire, rilevare, contenere e superare incidenti che interessano funzioni e servizi critici. I TLPT sono resi obbligatori dal DORA e integrano il quadro informativo a disposizione della supervisione.

fisiche[8]. Il Cyber Resilience Act (CRA) introduce requisiti armonizzati di sicurezza cibernetica per i prodotti digitali.

AI Act, CRA e DORA perseguono finalità complementari e si applicano in modo integrato: l'AI Act disciplina l'impiego dei sistemi di IA in funzione dei rischi per i diritti fondamentali delle persone; il CRA rafforza la sicurezza dei prodotti *hardware* e *software*, responsabilizzando i fornitori; il DORA rafforza la resilienza operativa degli intermediari finanziari che utilizzano prodotti digitali o sistemi di IA e dei loro fornitori.

Integrano il quadro normativo le proposte in materia di servizi di pagamento, che rafforzano il contrasto alle frodi e la tutela dei consumatori[9]. Ulteriori iniziative legislative riguardano i rischi connessi con il *cloud computing* e la transizione alla crittografia post-quantistica, oggetto di iniziative anche a livello nazionale.

3. L'attività di vigilanza

La Banca d'Italia contribuisce all'attuazione del quadro delle regole europee nell'ambito del Meccanismo di Vigilanza Unico (MVU)[10] e a livello nazionale con le altre Autorità, in particolare con l'Agenzia per la cybersicurezza nazionale (ACN).

L'innovazione tecnologica procede a ritmi senza precedenti e spesso anticipa l'adeguamento delle regole, delle metodologie e degli strumenti di controllo. La sfida per la supervisione non è soltanto verificare il rispetto delle regole, ma preservare e adattare i metodi e gli strumenti di vigilanza alle trasformazioni dell'ecosistema digitale.

La Vigilanza conduce tre principali tipologie di attività: i) la supervisione ordinaria, a distanza e ispettiva, sui singoli soggetti vigilati; ii) le analisi 'orizzontali' sul sistema per rilevare possibili fragilità comuni, concentrazioni di rischio ed

---

8 La Banca d'Italia è stata designata Autorità nazionale di vigilanza del mercato per i sistemi di IA ad alto rischio utilizzati nell'erogazione di finanziamenti o altri servizi finanziari disciplinati dal Testo Unico Bancario. I relativi requisiti e poteri si applicheranno dal 2 dicembre 2027.

9 La direttiva PSD3 (*Payment Services Directive 3*) e il regolamento PSR (*Payment Services Regulation*) introducono la verifica della corrispondenza tra beneficiario e IBAN, rafforzano il monitoraggio delle frodi e chiariscono le responsabilità dei prestatori di servizi di pagamento e la disciplina dei rimborsi. Sono previste specifiche tutele per i consumatori vittime di frodi da impersonificazione del proprio prestatore di servizi di pagamento.

10 Il MVU ha nel tempo rafforzato le attività e gli strumenti di vigilanza sulla resilienza operativa; ad esempio, ha condotto nel 2024 il *cyber resilience stress test* su 109 banche significative, nell'ambito del quale ha valutato la capacità di rispondere a un attacco grave e ripristinare l'operatività.

eventuali canali di contagio; iii) la supervisione sulle terze parti rilevanti nazionali ed europee, nell'ambito della vigilanza sui fornitori critici introdotta dal DORA.

Riporto di seguito i risultati emersi dalla nostra attività relativa a: i) l'adeguamento al DORA; ii) la valutazione degli incidenti; iii) i rischi di terza parte.

Nel dicembre 2024, la Banca d'Italia ha chiesto agli intermediari direttamente vigilati un'autovalutazione del livello di adeguamento alle nuove norme[11]. Le evidenze raccolte indicano progressi nel rafforzamento del monitoraggio del rischio, nelle competenze, anche degli organi sociali, e negli investimenti; emerge tuttavia l'esigenza di continuare a rafforzare i sistemi di controllo, la sicurezza delle infrastrutture informatiche, i meccanismi per ridurre l'impatto di attacchi informatici e l'adeguamento dei contratti con i fornitori.

Con specifico riferimento ai modelli di IA, la Vigilanza ha ribadito la centralità del DORA e ha chiesto la definizione di un piano di interventi volto a rafforzare la sicurezza informatica e la resilienza operativa entro la fine del 2026[12].

Il DORA ha introdotto inoltre una nuova disciplina per la segnalazione degli incidenti ICT[13] che amplia il perimetro dei soggetti obbligati e armonizza criteri, definizioni e modalità di raccolta delle informazioni. Le Autorità dispongono così di una base informativa di vigilanza più ampia e omogenea, che contribuisce alla valutazione dei rischi operativi e delle minacce cibernetiche, delle tendenze e dei rimedi comuni.

---

11 Le valutazioni, svolte con il coinvolgimento delle funzioni di controllo e approvate dall'organo amministrativo, dovevano essere trasmesse alla Vigilanza entro il 30 aprile 2025.

12 Cfr. Comunicazione del 17 luglio indirizzata agli intermediari direttamente vigilati (https://www.bancaditalia.it/compiti/vigilanza/avvisi-pub/2026.07.17-comunicazione/Comunicazione-al-mercato-in-materia-di-resilienza-operativa-digitale-e-modelli-avanzati-di-intelligenza-artificiale.pdf). Il MVU ha inviato analoga comunicazione il 7 luglio scorso alle banche significative, chiedendo la predisposizione del piano entro il 31 ottobre 2026 (Addressing AI-enabled cybersecurity threats). Ulteriori comunicazioni sono state pubblicate in pari data dal Comitato europeo per il rischio sistemico (CERS) (https://www.esrb.europa.eu/pub/pdf/warnings/esrb.warning260625_on_systemic_cyber_risks_stemming_from_frontier_ai_models~ef424708cf.en.pdf) e, il 31 luglio scorso, dalle autorità europee di vigilanza dei tre settori finanziari (https://www.eba.europa.eu/sites/default/files/2026-07/9c0d597c-79ff-482f-a3fe-d9ad66e96bac/JC%202026%2025_ESA%20Statement%20on%20frontier%20AI%20models.pdf).

13 Le norme DORA prevedono la segnalazione all'Autorità dei soli incidenti classificati come "gravi", quali ad esempio (i) gli accessi non autorizzati alle reti e ai sistemi informativi che possono determinare la perdita di dati; (ii) gli incidenti che interessano servizi critici e soddisfano almeno due degli ulteriori criteri di rilevanza previsti dalle norme (tra cui numero di clienti e transazioni interessati, durata del disservizio, perdite di dati, estensione geografica dell'incidente e impatto economico e reputazionale).

Le segnalazioni ricevute dagli intermediari nazionali[14] sono coerenti con le evidenze disponibili a livello internazionale: nel 2025 sono stati registrati 101 eventi, oggetto di 137 segnalazioni, dovuti in larga misura a malfunzionamenti del *software* e problemi di rete. L'interruzione dei servizi, rilevata in circa il 70 per cento dei casi, resta la principale conseguenza. Gli eventi legati alla sicurezza cibernetica hanno rappresentato il 23 per cento del totale. I fornitori ICT sono stati coinvolti in oltre la metà degli eventi notificati, a conferma della crescente importanza del rischio di terza parte. I primi nove mesi del 2026 confermano tale andamento: circa un quarto delle 92 segnalazioni ricevute (relative a 68 eventi) ha riguardato la sicurezza cibernetica; quasi il 60 per cento è riconducibile a fornitori terzi.

Gli approfondimenti sulle segnalazioni degli incidenti mostrano un generale allineamento degli intermediari ai requisiti previsti dal DORA; restano tuttavia margini di miglioramento nella corretta classificazione degli eventi, nei processi organizzativi volti ad avviare le misure rimediali e nella capacità di attuare interventi correttivi concreti e duraturi.

Le valutazioni sul rischio di terza parte beneficiano dei dati raccolti con i Registri delle informazioni (RoI), che devono essere inviati alla Vigilanza. Dalle nostre evidenze[15], emergono circa 3.600 fornitori e subfornitori, 'catene' complesse fino a cinque livelli, circa 9.600 contratti e oltre 2,6 miliardi di euro di spesa annua. Circa la metà dei rapporti sostiene funzioni critiche o importanti.

L'attività di vigilanza conferma l'esigenza di continuare a rafforzare l'effettivo controllo svolto sui servizi critici e sui fornitori strategici, mediante un'appropriata selezione delle controparti, la definizione dei livelli di servizio, la mappatura delle catene di subfornitura. L'adeguamento al DORA dei contratti già in essere può rivelarsi complesso quando gli intermediari hanno un limitato potere negoziale verso i fornitori più rilevanti.

Il DORA ha infine introdotto la sorveglianza europea sui fornitori ICT critici. L'attuale elenco comprende diciannove operatori e include quelli principali attivi a livello globale nei servizi *cloud* e nelle infrastrutture tecnologiche utilizzate dal settore finanziario[16]; la lista non comprende imprese italiane. Le Autorità europee valutano se tali fornitori dispongono di regole interne, processi e meccanismi di sicurezza idonei a gestire i rischi che possono determinare impatti per il settore

---

14 https://www.bancaditalia.it/compiti/vigilanza/analisi-sistema/approfondimenti-banche-int/Quadro-segnaletico-di-Vigilanza-dei-gravi-incidenti-ICT-Analisi-orizzontale-2025.pdf.

15 I dati non comprendono i RoI dei gruppi bancari significativi italiani, né quelli degli intermediari italiani appartenenti a gruppi europei di competenza del MVU o di altre autorità europee competenti.

16 List of designated CTPPs.pdf

finanziario. La Banca d'Italia partecipa ai Gruppi di vigilanza congiunti europei e al Forum di Sorveglianza, contribuendo a valutare la solidità delle difese, le vulnerabilità comuni, nonché eventuali implicazioni per la stabilità del sistema finanziario[17].

L'attività delle autorità nazionali ed europee ha consentito di rafforzare la trasparenza dei modelli operativi, dei controlli e dei profili di rischio dei fornitori ICT, favorendo anche migliori processi di *due diligence* e la maggiore consapevolezza del rischio di terza parte da parte degli intermediari. La concentrazione e la limitata sostituibilità dei fornitori di servizi ICT richiedono comunque un monitoraggio rafforzato**,** adeguati presidi di continuità operativa e strategie di uscita concretamente praticabili.

Un'attenzione specifica è rivolta inoltre alla sicurezza dei servizi di pagamento e al contrasto alle frodi, in particolare all'adeguatezza dei presidi relativi all'autenticazione e al monitoraggio delle transazioni. L'evoluzione delle tecniche di frode, sempre più spesso basate sulla manipolazione del cliente, richiede il continuo adeguamento dei sistemi di prevenzione e la capacità di rilevare tempestivamente comportamenti e transazioni anomali.

Sono previsti specifici meccanismi di ripartizione delle responsabilità e di rimborso per le frodi già realizzate; il cliente può rivolgersi all'Arbitro Bancario Finanziario (ABF) per risolvere in via stragiudiziale le controversie con l'intermediario, anche per valutare la corretta applicazione delle regole sull'autenticazione e la condotta delle parti[18].

4. La cooperazione tra le Autorità

La resilienza operativa digitale non può essere perseguita efficacemente da una singola Autorità. Le citate interdipendenze operative e tecnologiche, la complessità delle catene di fornitura e i possibili effetti sistemici degli incidenti richiedono solidi meccanismi di cooperazione, che favoriscano lo scambio informativo e il coordinamento tra Autorità finanziarie, Autorità competenti in materia di sicurezza cibernetica, nonché la collaborazione tra Autorità e operatori.

---

17 I Gruppi di vigilanza congiunti (*Joint Examination Teams* - JET) comprendono esperti delle Autorità europee e nazionali che svolgono la sorveglianza sui fornitori critici. Il Forum di Sorveglianza persegue il coordinamento tra l'attività delle Autorità di vigilanza competenti.

18 Nel 2025 le controversie relative agli utilizzi fraudolenti sono cresciute del 21 per cento. Le evidenze tratte dai ricorsi all'ABF e dagli esposti della clientela integrano il patrimonio informativo della Vigilanza.

In attuazione del decreto legislativo di adeguamento al DORA (D. Lgs. 23/2025), la Banca d'Italia sta definendo protocolli di collaborazione con le altre Autorità competenti (Consob, IVASS e COVIP), con l'ACN e la Guardia di Finanza. La collaborazione comprende scambi informativi, assistenza tecnica, meccanismi di coordinamento e risposta rapida agli incidenti operativi e cibernetici.

Nei rapporti con l'ACN, particolare attenzione è riservata al raccordo tra DORA e NIS2 e alle attività che interessano soggetti essenziali o importanti ai sensi della normativa europea sulla sicurezza cibernetica, inclusi i fornitori critici. Con la Guardia di Finanza lo scambio riguarda incidenti e minacce informatiche rilevanti per prevenire, accertare e reprimere gli illeciti economico-finanziari.

La prevenzione e il contrasto dei rischi cibernetici beneficiano anche della cooperazione pubblico-privato del CERT Finanziario italiano (CERTFin), co-presieduto dalla Banca d'Italia e dall'ABI. Vi partecipano IVASS e Consob, oltre a circa 80 operatori bancari e assicurativi. L'esperienza maturata dal 2017 mostra che lo scambio di informazioni sugli eventi cyber, la condivisione di buone prassi e la collaborazione con organismi analoghi rafforzano la preparazione dei singoli operatori e del sistema nel suo complesso. Alla prevenzione contribuiscono anche l'educazione finanziaria e digitale e le iniziative di sensibilizzazione, quali le campagne "I Navigati Informati e Sicuri"[19], che aiutano gli utenti a riconoscere tentativi di frode e forme di impersonificazione sempre più sofisticate. La consapevolezza della clientela costituisce un presidio importante, che si affianca, senza sostituirla, alla responsabilità degli intermediari nell'adottare adeguati sistemi di prevenzione e controllo.

La crescente dimensione transfrontaliera dei pagamenti, degli incidenti cibernetici e delle frodi digitali rende anche la cooperazione internazionale essenziale. Da alcuni anni partecipiamo ai lavori del G7 Cyber Expert Group (CEG) insieme alle altre banche centrali e Autorità, anche attraverso esercitazioni periodiche che coinvolgono gli operatori.

Contribuiamo inoltre con la Consob, l'IVASS, il MEF, la COVIP e l'ACN allo sviluppo del coordinamento europeo per i rischi cibernetici transfrontalieri realizzato in attuazione del DORA (*EU Systemic Cyber Incident Coordination Framework*, EU-SCICF). A livello nazionale, tali attività si svolgono nell'ambito

---

[19] L'ultima edizione della campagna "I Navigati", avviata a inizio ottobre, è promossa dal CERTFin con Banca d'Italia, IVASS, ABI, Polizia di Stato e numerosi intermediari, con il patrocinio dell'ACN, del Garante per la protezione dei dati personali e dell'AgCom. La campagna mira a rafforzare la consapevolezza di cittadini e imprese sui rischi delle frodi online, comprese quelle basate sull'IA, promuovendo comportamenti digitali più sicuri attraverso iniziative informative online e sul territorio.

del CODISE, che riunisce Autorità e operatori di rilevanza sistemica della piazza finanziaria italiana, conduce esercitazioni e sviluppa analisi e scenari di resilienza anche in coordinamento con le Autorità di altri settori.

Il valore della cooperazione non consiste comunque solo nel raccogliere informazioni, ma nel trasformarle in decisioni operative. Servono fiducia, regole chiare di classificazione e uso delle informazioni, qualità dei dati e tempestività. La robustezza del sistema condiziona quella dei singoli e, allo stesso tempo, le vulnerabilità dei singoli possono propagarsi e compromettere la resilienza complessiva: intermediari, infrastrutture di mercato, sistemi di pagamento, fornitori e Autorità devono conoscere le rispettive dipendenze tecnologiche e prepararsi a operare insieme in condizioni avverse.

Conclusioni

La trasformazione digitale offre opportunità importanti al sistema finanziario, aumenta i rischi operativi e cibernetici e rafforza il legame tra innovazione tecnologica, resilienza operativa e stabilità finanziaria.

Il rispetto formale delle regole non basta. Gli intermediari devono comprendere e anticipare i riflessi dell'evoluzione digitale, governare le dipendenze tecnologiche, preservare le funzioni essenziali e i servizi critici, adottare piani di investimento in tecnologie, in controlli e in competenze, valutare i rischi derivanti dal ricorso da terze parti. La velocità di adattamento è ormai diventata anche un fattore strategico per preservare la sostenibilità nel tempo del modello operativo.

La resilienza non può pertanto essere delegata alle sole funzioni tecniche, ma rappresenta un obiettivo aziendale prioritario, che richiede il pieno coinvolgimento dei vertici e implica scelte strategiche, organizzative e di investimento.

Il rafforzamento della resilienza è quindi una responsabilità condivisa tra intermediari, fornitori tecnologici e Autorità, che devono contribuire, secondo le proprie responsabilità, alla costruzione di un ecosistema sicuro e capace di preservare la fiducia dei cittadini e delle imprese.

La Banca d'Italia sostiene l'innovazione e la trasformazione digitale del settore finanziario e contribuisce a mitigarne i rischi. Negli scorsi mesi, abbiamo intensificato il confronto con le Autorità nazionali ed estere, gli operatori finanziari e i fornitori di servizi ICT per ribadire che lo sviluppo dell'innovazione, delle competenze e della capacità di governo dei rischi rafforzano la sicurezza e la resilienza del sistema finanziario.

Questa pubblicazione è stata stampata
su carta certificata Ecolabel UE
(numero di registrazione: FR/011/001)

Inoltre l'impatto ambientale connesso con il ciclo di vita della carta utilizzata
è stato compensato con l'acquisto di crediti di carbonio e piantando alberi in aree del territorio italiano.

Grafica e stampa a cura della Divisione Editoria e stampa della Banca d'Italia