

Bruxelles, 11 marzo 2026
(OR. en)

7240/26

EF 66
ECOFIN 329
FSC 6
ESMA
ESRB
ECB
EIOPA
SRB
EBA

NOTA DI TRASMISSIONE

Origine:	Segretaria generale della Commissione europea, firmato da Martine DEPREZ, direttrice
Destinatario:	Thérèse BLANCHET, segretaria generale del Consiglio dell'Unione europea
n. doc. Comm.:	COM(2026) 119 final
Oggetto:	RELAZIONE DELLA COMMISSIONE AL CONSIGLIO E AL PARLAMENTO EUROPEO sulla preparazione del settore finanziario dell'UE

Si trasmette in allegato, per le delegazioni, il documento COM(2026) 119 final.

All.: COM(2026) 119 final



Bruxelles, 10.3.2026
COM(2026) 119 final

**RELAZIONE DELLA COMMISSIONE AL CONSIGLIO E AL PARLAMENTO
EUROPEO**

sulla preparazione del settore finanziario dell'UE

1. Introduzione

L'Unione europea, in molteplici settori, è posta di fronte a rischi crescenti e minacce senza precedenti che spaziano da una maggiore incertezza, dalle tensioni e dai conflitti geopolitici ai rischi relativi alla cibersicurezza e alla manipolazione delle informazioni, fino ai cambiamenti climatici e ai rischi crescenti posti da pericoli naturali. Al fine di potenziare la capacità dell'UE di anticipare, prevenire e rispondere a tali minacce, il 26 marzo 2025 la Commissione e il Servizio europeo per l'azione esterna (SEAE) hanno presentato congiuntamente la strategia per l'Unione della preparazione¹. Il settore finanziario dell'UE svolge un ruolo fondamentale nel preservare in ogni situazione le funzioni vitali sociali. Per tale motivo, nell'ambito della strategia per l'Unione della preparazione e in attuazione dell'azione 25 dell'allegato della comunicazione congiunta, la Commissione sta effettuando una valutazione completa del livello di preparazione nel settore finanziario. In particolare, sta valutando la capacità del settore di continuare a svolgere, in qualsiasi situazione, le sue funzioni essenziali, come effettuare pagamenti e finanziare l'economia.

La normativa dell'UE in materia di servizi finanziari si basa su una solida tradizione di prudenza, precauzione, resilienza e anticipazione. Gli obiettivi sono chiari: preservare la stabilità finanziaria, la risoluzione ordinata degli enti finanziari in dissesto, la gestione delle crisi e l'assicurazione dei depositi, la tutela degli investitori e l'integrità del mercato. L'UE ha completato una revisione globale delle proprie norme prudenziali e dell'architettura di vigilanza bancaria a seguito della grande crisi finanziaria iniziata nel 2007. Tali riforme hanno rafforzato le istituzioni finanziarie dell'UE, i suoi mercati dei capitali e i fornitori di infrastrutture del mercato finanziario.

Oggi il settore finanziario dell'UE ha raggiunto un elevato livello di resilienza consolidando tre pilastri: i) capitale basato sul rischio per le banche e gli istituti finanziari, ii) requisiti in materia di governance e trasparenza e iii) meccanismi di cooperazione in materia di vigilanza tra gli Stati membri e i diversi settori. L'UE ha messo in atto politiche e principi che producono valutazioni continue dei rischi di eventi estremi che interessano i quadri relativi al rischio operativo, la continuità operativa e i piani di emergenza.

Negli ultimi anni il quadro dell'UE è stato messo alla prova da diversi episodi di crisi, quali la pandemia di COVID-19, l'aggressione dell'Ucraina da parte della Russia, la crisi bancaria regionale degli Stati Uniti e la crisi di Credit Suisse nel 2023, blackout elettrici, attacchi informatici e incidenti ibridi. Di fronte a tali crisi, il settore finanziario dell'UE ha dato prova di solidità e resilienza. Le autorità a livello nazionale e dell'UE hanno agito in modo rapido ed efficace.

In generale, la preparazione non è statica, è una condizione dinamica e orientata al futuro che richiede un ciclo continuo di pianificazione, formazione, equipaggiamento, sperimentazione, valutazione e miglioramento. Impone altresì di prestare attenzione alla prontezza ad affrontare tutti i pericoli anticipando i rischi, sviluppando capacità, coordinando i vari settori (governo,

¹ La Commissione e il SEAE hanno pubblicato una [comunicazione congiunta](#) sulla [strategia per l'Unione della preparazione](#).

privato, pubblico) e traendo insegnamenti dagli eventi passati per costruire comunità resilienti in grado di prevenire le crisi, nonché di proteggersi e riprendersi dalle stesse. Ciò vale anche per il settore finanziario.

La presente relazione offre una panoramica dello stato attuale di preparazione del settore finanziario dell'UE, basandosi su un dialogo costante con la Banca centrale europea, le autorità europee di vigilanza, il Comitato europeo per il rischio sistemico, il Comitato di risoluzione unico, gli Stati membri e il settore dei servizi finanziari.

2. Preparazione nel mercato unico dell'UE

A livello dell'UE, la preparazione nel settore finanziario è migliorata negli ultimi anni grazie a misure legislative e alla creazione di strutture di governance a livello di Unione che riflettono la natura transfrontaliera del settore finanziario dell'UE. La governance si basa su due pilastri: la normativa dell'UE e le autorità dell'UE. Questa struttura è integrata da una serie di misure adottate a livello della zona euro, regionale (con la partecipazione di diversi Stati membri) e di Stati membri.

2.1 Normativa dell'UE che disciplina il settore finanziario

Il settore finanziario è disciplinato sia da una normativa settoriale che da una normativa trasversale.

Normativa settoriale

La normativa settoriale comprende la direttiva e il regolamento sui requisiti patrimoniali (CRD/CRR)², la direttiva Solvibilità II³, la direttiva relativa ai mercati degli strumenti finanziari II (MiFID II)⁴, il regolamento sulle infrastrutture del mercato europeo (EMIR)⁵ e il regolamento sui depositari centrali di titoli (CSDR)⁶. Tali atti legislativi stabiliscono requisiti prudenziali per garantire la resilienza, la stabilità e il corretto funzionamento degli enti finanziari, delle infrastrutture finanziarie e del sistema finanziario.

² Direttiva 2013/36/UE del Parlamento europeo e del Consiglio, del 26 giugno 2013, sull'accesso all'attività degli enti creditizi e sulla vigilanza prudenziale sugli enti creditizi e sulle imprese di investimento, che modifica la direttiva 2002/87/CE e abroga le direttive 2006/48/CE e 2006/49/CE (CRD); regolamento (UE) n. 575/2013 del Parlamento europeo e del Consiglio, del 26 giugno 2013, relativo ai requisiti prudenziali per gli enti creditizi e le imprese di investimento e che modifica il regolamento (UE) n. 648/2012 (CRR).

³ Testo consolidato: direttiva 2009/138/CE del Parlamento europeo e del Consiglio, del 25 novembre 2009, in materia di accesso ed esercizio delle attività di assicurazione e di riassicurazione (solvibilità II).

⁴ Direttiva 2014/65/UE del Parlamento europeo e del Consiglio, del 15 maggio 2014, relativa ai mercati degli strumenti finanziari e che modifica la direttiva 2002/92/CE e la direttiva 2011/61/UE (MiFID II).

⁵ Regolamento (UE) n. 648/2012 del Parlamento europeo e del Consiglio, del 4 luglio 2012, sugli strumenti derivati OTC, le controparti centrali e i repertori di dati sulle negoziazioni (EMIR).

⁶ Regolamento (UE) n. 909/2014 del Parlamento europeo e del Consiglio, del 23 luglio 2014, relativo al miglioramento del regolamento titoli nell'Unione europea e ai depositari centrali di titoli e recante modifica delle direttive 98/26/CE e 2014/65/UE e del regolamento (UE) n. 236/2012.

Dal punto di vista della preparazione, diversi atti legislativi settoriali stabiliscono prescrizioni che disciplinano la gestione dei rischi operativi, la resilienza operativa, la resilienza delle TIC, la continuità operativa e la gestione delle crisi. Ad esempio, nel settore bancario, il CRR/la CRD, la direttiva sul risanamento e la risoluzione delle banche (BRRD)⁷, il regolamento sul meccanismo di risoluzione unico (SRMR)⁸ e la direttiva relativa ai sistemi di garanzia dei depositi (direttiva SGD)⁹ garantiscono che le banche abbiano la resilienza necessaria per resistere a un'ampia gamma di rischi potenziali, compresi gli eventi estremi. Le banche dovrebbero attuare solidi quadri di governance e di gestione del rischio, comprendenti piani rafforzati di continuità operativa, comunicazione e risanamento, per affrontare efficacemente un'ampia gamma di rischi. Le caratteristiche principali delle misure volte ad affrontare gli scenari di rischio, sia precauzionali che reattive, comprendono requisiti ex ante specifici per le banche, quali i piani di risanamento e i piani di risoluzione, come previsto dall'SRMR e dalla BRRD.

Oltre alle banche, le imprese di assicurazione disciplinate dalla direttiva Solvibilità II, le imprese di investimento disciplinate dalla direttiva MiFID II e le infrastrutture di mercato, quali le controparti centrali (CCP) e i depositari centrali di titoli, sono soggette a requisiti analoghi per garantire la resilienza operativa, la gestione dei rischi informatici, la continuità operativa e la gestione delle crisi. Tali requisiti sono integrati da prescrizioni volte a migliorare la pianificazione del risanamento e della risoluzione, ove necessario. Anche la gestione patrimoniale e l'intermediazione finanziaria non bancaria sono soggette a un quadro normativo dell'UE ampio e sempre più completo, che comprende la direttiva sugli organismi d'investimento collettivo in valori mobiliari, la direttiva sui gestori di fondi di investimento alternativi e il regolamento sui fondi comuni monetari. Tali strumenti impongono obblighi in materia di gestione del rischio, gestione della liquidità, leva finanziaria, valutazione e trasparenza, al fine di promuovere la stabilità del settore. L'azione volta a creare l'Unione del risparmio e degli investimenti sviluppando la capacità del settore finanziario dell'UE di collegare i risparmi a investimenti produttivi, migliorando in tal modo la condivisione dei rischi e la diversificazione in tutto il settore finanziario dell'UE, ne migliorerà la resilienza e la preparazione complessive.

La Banca centrale europea (BCE), che è l'autorità di vigilanza unica per le banche in 21 Stati membri, e le autorità nazionali competenti all'interno e all'esterno della zona euro pongono la resilienza finanziaria e operativa delle banche al centro delle loro priorità di vigilanza. Le banche sono incoraggiate in particolare a tenere in debito conto i rischi geopolitici e a integrarli

⁷ Direttiva 2014/59/UE del Parlamento europeo e del Consiglio, del 15 maggio 2014, che istituisce un quadro di risanamento e risoluzione degli enti creditizi e delle imprese di investimento e che modifica la direttiva 82/891/CEE del Consiglio, e le direttive 2001/24/CE, 2002/47/CE, 2004/25/CE, 2005/56/CE, 2007/36/CE, 2011/35/UE, 2012/30/UE e 2013/36/UE e i regolamenti (UE) n. 1093/2010 e (UE) n. 648/2012, del Parlamento europeo e del Consiglio (BRRD).

⁸ Regolamento (UE) n. 806/2014 del Parlamento europeo e del Consiglio, del 15 luglio 2014, che fissa norme e una procedura uniformi per la risoluzione degli enti creditizi e di talune imprese di investimento nel quadro del meccanismo di risoluzione unico e del Fondo di risoluzione unico e che modifica il regolamento (UE) n. 1093/2010 (SRMR)

⁹ Direttiva 2014/49/UE del Parlamento europeo e del Consiglio, del 16 aprile 2014, relativa ai sistemi di garanzia dei depositi (direttiva SGD).

nei loro processi di gestione dei rischi. A tal proposito le banche dovrebbero considerare le esposizioni verso controparti di paesi terzi, i potenziali impatti di sanzioni straniere sulle esposizioni e le dipendenze da fornitori esterni di servizi e infrastrutture. Inoltre le banche dovrebbero mettere a punto un solido quadro di governance e una protezione dalle minacce informatiche e da altre minacce che possono incidere sulla loro resilienza operativa. Ciò comprende misure volte ad aumentare la sicurezza e a fornire protezione dai danni fisici. Oltre alle misure specifiche per l'ente, il quadro prudenziale per il settore bancario dell'UE affronta anche canali di rischio più ampi a livello sistemico e transfrontaliero.

Il quadro per la gestione delle crisi crea un insieme di strumenti da utilizzare quando la sostenibilità economica del fornitore di una funzione critica è a rischio. Il quadro riveduto per la gestione delle crisi bancarie e l'assicurazione dei depositi, su cui è stato raggiunto un accordo politico nel giugno 2025, segna un passo importante per rendere il sistema di gestione delle crisi dell'UE ancora più efficace, in particolare per le banche di piccole e medie dimensioni.

Un aspetto importante della preparazione nel settore finanziario è la disponibilità di strumenti di pagamento per il pubblico, sia in contanti che in modalità elettronica. Per garantire la disponibilità di **contante** in ogni circostanza, a livello dell'Eurosistema, una misura fondamentale è il mantenimento di scorte strategiche comuni di banconote in euro. La BCE è l'organo centrale decisionale e di coordinamento e realizza esercitazioni periodiche di gestione delle crisi, compresa la potenziale comunicazione in caso di crisi. A livello nazionale, le banche centrali nazionali (BCN) mantengono piani di continuità operativa per garantire che i prelievi di contante e i depositi rimangano disponibili.

Parallelamente, la proposta relativa al corso legale delle banconote e delle monete in euro, presentata dalla Commissione il 28 giugno 2023, mira a garantire che il contante in euro rimanga ampiamente accettato per i pagamenti e facilmente accessibile ai cittadini, alle imprese e agli enti pubblici in tutta la zona euro. L'obbligo di mantenere un'adeguata infrastruttura per il contante in tempi normali favorisce la disponibilità di contante in situazioni di emergenza. La proposta della Commissione non includeva una disposizione sulla resilienza, che però è stata aggiunta dal Consiglio nel suo mandato negoziale, imponendo agli Stati membri di disporre di un piano di resilienza in termini di liquidità o di una combinazione di misure equivalenti.

Inoltre la direttiva relativa ai servizi di pagamento 3 (PSD3), sulla quale è stato raggiunto un accordo politico nel novembre 2025, mira a promuovere l'accesso al contante nei negozi consentendo ai dettaglianti di offrire prelievi di contante senza acquisto (ossia la fornitura di contante nei punti vendita), fino a un certo limite. Ciò rende più comodo l'uso del contante, in particolare nelle zone rurali, chiarendo le norme per i dettaglianti e i gestori di ATM.

Oltre alla disponibilità di contante, è fondamentale mantenere la continuità dei **servizi di pagamento**, compresi i pagamenti tramite carta, i pagamenti con trasferimento da conto a conto (anche tramite telefoni cellulari), l'accesso ai conti di pagamento e la possibilità di effettuare depositi, al fine di mantenere la fiducia del pubblico nel sistema finanziario, tutelare l'ordine pubblico e garantire il funzionamento di base dell'economia in caso di perturbazioni diffuse, garantendo al pubblico un accesso continuo ai servizi di base.

L'attuale direttiva relativa servizi di pagamento 2 (PSD2) disciplina altri aspetti, tra cui la gestione dei rischi operativi e di sicurezza e la segnalazione di incidenti gravi. L'obiettivo è rafforzare la sicurezza e la resilienza dei sistemi di pagamento in tutta l'UE.

L'Eurosistema promuove la sicurezza e l'efficienza dei sistemi di pagamento. Ha introdotto obblighi di sorveglianza per affrontare i principali scenari di rischio individuati in relazione all'ecosistema europeo dei pagamenti. I quadri stabiliscono una serie completa di prescrizioni per la gestione dei rischi operativi. Tra questi figurano misure per la gestione della continuità operativa e il ripristino tempestivo, unitamente a disposizioni specifiche per la sicurezza delle informazioni, la ciberresilienza, la sicurezza fisica, l'esternalizzazione, la gestione dei rischi informatici e altri ambiti correlati. Il quadro riguarda gli strumenti di pagamento elettronici (quali carte, addebiti diretti, bonifici, moneta elettronica e portafogli digitali), nonché gli schemi (ad esempio le reti di carte) e le applicazioni (ad esempio i portafogli elettronici) che ne consentono l'uso.

Per fornire una maggiore protezione, l'articolo 15 del regolamento della BCE sui sistemi di pagamento di importanza sistemica (SPIS) stabilisce altri obblighi. Ad esempio, richiede che i sistemi assicurino il ripristino entro due ore (anche attraverso l'uso di siti secondari) e che i gestori di SPIS siano in grado di completare il regolamento di tutti i pagamenti dovuti in un giorno entro la fine del giorno lavorativo in cui si è verificato l'incidente.

Il progetto di creare un euro digitale — una forma digitale di contante, che integri il contante fisico e le soluzioni di pagamento private — offrirebbe al pubblico un metodo di pagamento supplementare, promuovendo nel contempo l'inclusione digitale e finanziaria. In quanto primo sistema di pagamento paneuropeo unificato, l'euro digitale contribuirebbe altresì a salvaguardare il ruolo internazionale dell'euro. Rafforzando l'autonomia strategica aperta dell'UE e ampliando la gamma di strumenti di pagamento disponibili, il progetto relativo all'euro digitale mira a migliorare ulteriormente la resilienza complessiva dei servizi di pagamento. Per quanto riguarda la proposta relativa al corso legale, il Consiglio ha aggiunto disposizioni supplementari volte a rafforzare ulteriormente la resilienza dell'euro digitale. In tale contesto, i portafogli di identità digitale dell'UE (EUDI) saranno interoperabili con le interfacce utente dell'euro digitale, garantendo un'autenticazione degli utenti sicura e senza discontinuità¹⁰.

Normativa intersettoriale nel settore finanziario

A integrazione della normativa finanziaria di cui sopra, il regolamento relativo alla resilienza operativa digitale (DORA) è un atto legislativo specifico per il settore finanziario che si applica all'intero settore finanziario dell'UE. Riguarda 20 diversi tipi di entità finanziarie, tra cui enti

¹⁰ Il quadro europeo relativo a un'identità digitale istituisce un ecosistema sicuro e affidabile per l'identificazione e l'autenticazione digitali e l'uso di prove digitali che sarà a disposizione di tutti i cittadini dell'UE entro la fine del 2026. I portafogli europei di identità digitale apporteranno benefici diretti alla resilienza e alla preparazione alle crisi del settore finanziario dell'UE, fornendo protezione dalle frodi e dal furto di identità nei pagamenti, nell'onboarding dei clienti e in altri servizi finanziari.

creditori, prestatori di servizi di pagamento, infrastrutture dei mercati finanziari, compagnie di assicurazione, agenzie di rating del credito e gestori di patrimoni.

Il regolamento DORA pone un forte accento sulla resilienza delle entità finanziarie, sul loro livello di preparazione per resistere a potenziali perturbazioni nel settore delle TIC e sulla gestione dei rischi derivanti dalla dipendenza delle entità finanziarie da fornitori terzi di servizi TIC, compresi i rischi sistemici e di concentrazione posti dai fornitori di TIC che sono critici per il settore finanziario dell'UE. Il regolamento DORA istituisce un quadro armonizzato e solido per rafforzare la capacità del settore finanziario dell'UE di prevenire le perturbazioni connesse alle TIC, farvi fronte, rispondervi e riprendersi dalle stesse. Le entità finanziarie devono istituire un quadro generale per la gestione dei rischi informatici, che comprenda la governance, l'inventario degli attivi, l'individuazione dei rischi, la protezione, l'individuazione, la risposta, il ripristino e il miglioramento continuo. Ciò garantisce che le vulnerabilità e la resilienza dei sistemi e dei processi siano gestite in modo proattivo. Le entità finanziarie sono inoltre tenute a individuare, classificare e segnalare alle autorità competenti gli incidenti gravi connessi alle TIC utilizzando definizioni, soglie e tempistiche concordate per consentire risposte coordinate tra le giurisdizioni. Il regolamento DORA impone test e valutazioni periodiche dei loro processi, strumenti e dispositivi di resilienza e preparazione.

Le entità finanziarie devono inoltre gestire i rischi associati al ricorso a fornitori terzi di servizi TIC, in particolare i fornitori terzi critici. Il regolamento DORA impone alle entità finanziarie di effettuare controlli di dovuta diligenza in relazione ai rischi di concentrazione prima di stipulare nuovi contratti con fornitori terzi di TIC. Il regolamento DORA prevede un meccanismo di sorveglianza nell'ambito del quale le tre autorità europee di vigilanza (AEV)¹¹ vigilano sui fornitori terzi critici di servizi TIC su scala paneuropea, rafforzando la resilienza operativa digitale complessiva in tutto il settore finanziario dell'UE. Nel novembre 2025 le AEV hanno pubblicato l'elenco dei fornitori terzi critici di servizi TIC designati nell'ambito del regolamento DORA. Il quadro DORA è particolarmente adatto a gestire la cibersecurity, la connettività, la preparazione e i rischi operativi con una forte dimensione internazionale.

Il settore finanziario è disciplinato, oltre che dal regolamento DORA, che è una *lex specialis* per il settore finanziario, anche da accordi di cooperazione orizzontale sulla resilienza fisica e digitale a norma della direttiva sulla resilienza dei soggetti critici (CER)¹² e della direttiva NIS 2.

La direttiva CER istituisce un quadro generale per affrontare la resilienza dei soggetti critici rispetto a tutti i rischi. Impone valutazioni dei rischi, strategie nazionali e misure di resilienza specifiche per i soggetti critici designati al fine di garantire che siano in grado di continuare a svolgere funzioni vitali della società. Sebbene la direttiva includa il settore bancario e le infrastrutture dei mercati finanziari come settori critici, il settore finanziario non rientra

¹¹ Le tre AEV sono l'Autorità bancaria europea (ABE), l'Autorità europea delle assicurazioni e delle pensioni aziendali e professionali (EIOPA) e l'Autorità europea per gli strumenti finanziari e i mercati (ESMA).

¹² Direttiva (UE) 2022/2557 del Parlamento europeo e del Consiglio, del 14 dicembre 2022, relativa alla resilienza dei soggetti critici e che abroga la direttiva 2008/114/CE del Consiglio. L'articolo 5, paragrafo 5, della direttiva prevede che la Commissione, in cooperazione con gli Stati membri, sviluppi un modello comune volontario per la presentazione delle relazioni in ottemperanza dell'articolo 5, paragrafo 4, della direttiva.

nell'ambito di applicazione di tutte le prescrizioni sostanziali della CER, in quanto è soggetto a prescrizioni molto più specifiche a norma del regolamento DORA. Tuttavia il settore finanziario rimane nell'ambito di applicazione della direttiva CER per quanto riguarda gli accordi di cooperazione orizzontale.

La direttiva NIS 2 fornisce un quadro più ampio per la cibersicurezza in vari settori critici. Il regolamento DORA è considerato una *lex specialis* rispetto alla direttiva NIS 2, il che significa che, anziché la direttiva NIS 2, si applicano le prescrizioni relative alla gestione dei rischi e alla segnalazione degli incidenti di cui al regolamento DORA, in quanto atto giuridico settoriale dell'Unione. Come comunicato dalla Commissione nei suoi orientamenti sull'applicazione dell'articolo 4, paragrafi 1 e 2, della direttiva NIS 2¹³, alcune disposizioni della direttiva NIS 2 che sono essenziali per garantire la preparazione e conseguire un elevato livello di resilienza delle entità finanziarie continuano ad applicarsi, tra cui l'obbligo di adottare una strategia per la cibersicurezza e di istituire un quadro nazionale di gestione delle crisi informatiche (con l'obbligo di designare autorità di gestione delle crisi informatiche e di adottare piani nazionali di risposta agli incidenti e alle crisi di cibersicurezza su vasta scala) che riguardano il settore bancario e quello delle infrastrutture dei mercati finanziari. Inoltre i gruppi di intervento per la sicurezza informatica in caso di incidente ("CSIRT") e la rete europea delle organizzazioni di collegamento per le crisi informatiche ("EU-CyCLONe") dovrebbero svolgere i loro compiti per quanto riguarda il settore bancario e quello delle infrastrutture dei mercati finanziari.

Le misure di preparazione delineate per il settore finanziario sono concepite per trovare un equilibrio tra la necessità di resilienza e il principio di proporzionalità. Gli obblighi normativi e in materia di vigilanza sono adattati alle dimensioni, alla complessità e all'importanza sistemica degli enti al fine di evitare di imporre un onere sproporzionato alle entità più piccole. Per evitare inutili oneri amministrativi, quadri armonizzati come il regolamento DORA razionalizzano le prescrizioni in tutto il settore, garantendo la coerenza e riducendo nel contempo la duplicazione degli sforzi.

2.2 Autorità dell'UE: strumenti e cooperazione

Alle autorità dell'UE sono forniti strumenti specifici che possono essere attivati in situazioni di emergenza e che mantengono dispositivi di preparazione volti a garantire la continuità operativa. Ad esempio, i rispettivi regolamenti istitutivi hanno attribuito alle tre AEV poteri di emergenza. Una volta che una situazione di emergenza è stata formalmente riconosciuta dal Consiglio (a norma dell'articolo 18 dei regolamenti relativi alle AEV), tali autorità possono limitare temporaneamente le attività finanziarie ai sensi dell'articolo 9 mediante decisioni individuali. Svolgono inoltre una funzione di coordinamento generale tra le autorità nazionali e nell'ambito del Sistema europeo di vigilanza finanziaria (SEVIF) (articolo 31).

¹³ C(2023)6068.

Come indicato in precedenza, la BCE è l'autorità di vigilanza unica per le banche dei 21 Stati membri che partecipano al meccanismo di vigilanza unico, garantendo una vigilanza prudenziale coerente in tutta l'area. Il Comitato di risoluzione unico è l'autorità di risoluzione unica per tali Stati membri, responsabile della risoluzione ordinata delle banche in dissesto, salvaguardando in tal modo la stabilità finanziaria e riducendo al minimo i costi per i contribuenti.

Al fine di rafforzare la resilienza operativa, tutte le autorità dell'UE hanno messo a punto procedure interne di continuità operativa, preparazione e gestione degli incidenti critici per gestire una serie di pericoli. Verificano regolarmente tali misure per garantire la continuità operativa e individuare i processi operativi più urgenti da svolgere in caso di emergenza e a quale livello.

Data la necessità di preservare l'integrità e il corretto funzionamento del mercato unico e alla luce dell'elevato grado di interconnessione e del rischio di effetti di ricaduta nel settore finanziario dell'UE, il coordinamento tra le diverse autorità dell'UE e il coinvolgimento degli Stati membri sono essenziali per anticipare e gestire le crisi che possono interessare più parti dell'UE contemporaneamente. Un coinvolgimento tempestivo e una cooperazione rapida sono essenziali sia nella fase di pianificazione che in ogni fase della crisi. Per agevolare la cooperazione e lo scambio di informazioni che possono essere pertinenti anche in caso di crisi, diverse autorità dell'UE hanno concluso strumenti di cooperazione reciproca o con le autorità nazionali competenti o le autorità nazionali di risoluzione, oppure hanno concluso protocolli d'intesa (ad esempio, il protocollo d'intesa tra la BCE e il comitato di risoluzione unico (SRB), e stanno inoltre conducendo simulazioni per garantire un'adeguata preparazione alle crisi.

Una tappa importante in questo lavoro è il quadro dell'Unione europea per il coordinamento sistemico degli incidenti informatici (EU-SCICF), istituito dalle AEU nel gennaio 2025. Tale quadro fornisce una base strategica per la cooperazione in caso di incidenti informatici significativi¹⁴. Mira a facilitare una rapida condivisione delle informazioni e risposte comuni mettendo in atto protocolli per valutare e attenuare le minacce in tutti gli Stati membri dell'UE.

Inoltre, nel giugno 2025, il Consiglio ha adottato un programma per la gestione delle crisi informatiche¹⁵ quale importante guida per gli Stati membri al fine di migliorarne la preparazione, le capacità di individuazione e la risposta agli incidenti di cibersicurezza, sulla base di tutti i meccanismi pertinenti, compresi quelli creati dalla direttiva NIS 2, dal regolamento DORA (EU-SCICF) e dal regolamento sulla ciber-solidarietà.

Nell'ambito di tale quadro possono essere effettuate esercitazioni periodiche per garantire che le capacità di prontezza e risposta restino solide ed efficaci. Inoltre, a livello internazionale, il protocollo di risposta agli incidenti informatici del G7 mira a unificare gli sforzi di risposta

¹⁴ L'EU-SCICF attua inoltre l'articolo 49 del regolamento DORA al fine di rafforzare il coordinamento con altri quadri di crisi dell'UE.

¹⁵ Raccomandazione del Consiglio, del 6 giugno 2025, relativa a un programma dell'UE per la gestione delle crisi informatiche (*GU C*, C/2025/3445, 20.6.2025, *ELI*: <http://data.europa.eu/eli/C/2025/3445/oj>).

globale alle minacce alla cibersicurezza che incidono sul settore finanziario e a garantire risposte tempestive e coordinate tra le giurisdizioni.

Ciascuna autorità dell'UE effettua valutazioni periodiche dei rischi e adotta altre misure per individuare i rischi più rilevanti rispetto al proprio mandato e alle proprie funzioni. Le valutazioni dei rischi sono condotte in collaborazione con le autorità nazionali, il che contribuisce a sviluppare una comprensione condivisa e più approfondita del panorama dei rischi e dei rischi da considerare prioritari. Le valutazioni dei rischi spesso confluiscono nei sistemi di allarme rapido che, a loro volta, fanno parte dei quadri di preparazione delle autorità dell'UE. Inoltre gli accordi esistenti in materia di regolamentazione e vigilanza tra le autorità dell'UE e i portatori di interessi del settore privato consentono di proseguire il dialogo sulle aspettative reciproche in materia di preparazione¹⁶.

2.3 Quadri a livello nazionale e regionale

Oltre alla normativa a livello dell'UE, gli Stati membri hanno sviluppato i propri sistemi nazionali di preparazione¹⁷. Tali sistemi vanno generalmente oltre il settore finanziario e riguardano la preparazione della società nel suo complesso a livello nazionale. Per tale motivo, i sistemi nazionali variano da uno Stato membro all'altro, rispecchiando le diverse strutture di governo e amministrative nazionali e l'ambito delle competenze. Allo stesso tempo, tali sistemi nazionali operano all'interno di un quadro coerente dell'UE e interagiscono sempre più con gli accordi a livello dell'UE e i meccanismi di coordinamento transfrontaliero.

La preparazione del settore finanziario è sempre un elemento chiave delle strategie nazionali di preparazione. Il settore è in prima linea nella preparazione, un "esempio" per altri settori. Le strategie nazionali di preparazione per il settore finanziario vanno oltre l'*acquis* dell'UE, concentrandosi sulle questioni operative nazionali. Le differenze tra i sistemi finanziari nazionali (ad esempio le principali caratteristiche del settore bancario nazionale, il grado di utilizzo del contante, l'adozione dell'euro, la partecipazione all'Unione bancaria) si riflettono ovviamente nel modo in cui il livello di preparazione nazionale del settore finanziario è valutato e garantito.

Dato il ruolo centrale svolto dalle autorità pubbliche, in particolare in caso di crisi o incidente grave, è necessario che rimangano disponibili funzioni affidabili di finanziamento a breve termine per evitare carenze di liquidità o di finanziamento a livello del debito sovrano e del settore pubblico più in generale e ripercussioni più ampie per la società in termini di fiducia pubblica e stabilità finanziaria. Tuttavia ciò non si applica allo stesso modo a tutti i quadri di crisi: in particolare, la risoluzione bancaria è concepita per limitare il ricorso a fondi pubblici, attraverso il bail-in e meccanismi di risoluzione finanziati dal settore.

¹⁶ La strategia dell'UE per l'Unione della preparazione riconosce l'importanza di tali partenariati. Le azioni fondamentali 36 e 37 mirano a costituire una task force pubblico-privato per la preparazione e a definire protocolli pubblico-privato per le emergenze in tutti i settori.

¹⁷ Nell'ambito del proprio lavoro volto a realizzare il mandato dell'azione 25 dell'allegato della comunicazione congiunta sulla strategia per l'Unione della preparazione, la Commissione si è inoltre basata sul proseguimento delle discussioni con gli Stati membri relative ai sistemi di preparazione.

Al fine di garantire la resilienza delle funzioni di finanziamento a breve termine dei governi, gli uffici nazionali di gestione del debito hanno elaborato piani di emergenza e di continuità operativa in modo da continuare a operare anche in caso di crisi. Tali accordi sono sempre più integrati da scambi di migliori pratiche e da un coordinamento a livello sia dell'UE che regionale.

Inoltre il meccanismo europeo di stabilità (MES) offre diversi strumenti di assistenza finanziaria volti a salvaguardare la stabilità finanziaria fornendo assistenza ai membri del MES, al fine di rafforzare la capacità della zona euro di gestire le difficoltà del debito sovrano e bancario. Tali strumenti sono intesi ad affrontare le crisi sistemiche e a integrare la preparazione operativa nazionale e dell'UE a scenari di perturbazione più tangibili. Alcuni Stati membri hanno concluso accordi bilaterali per garantire la disponibilità di finanziamenti a breve termine in caso di indisponibilità di una qualsiasi delle funzioni di base dell'ufficio di gestione del debito. Il completamento della modifica in corso del trattato MES rafforzerebbe ulteriormente la rete di sicurezza della zona euro.

Parallelamente, esistono forum di coordinamento regionale, come il meccanismo di cooperazione nordico-baltica, un'importante iniziativa regionale incentrata sui paesi del Mar Baltico. Tali consessi promuovono la collaborazione in materia di vigilanza finanziaria e gestione delle crisi, lo scambio di informazioni sulle valutazioni dei rischi e la pianificazione strategica. Dimostrano in che modo la cooperazione regionale può migliorare la preparazione.

Diversi Stati membri hanno sviluppato partenariati o forum pubblico-privato specifici nel contesto dei loro programmi nazionali di preparazione (che comprendono rappresentanti del settore privato di diversi ambiti).

Nel complesso, tali accordi a livello dell'UE, regionale e nazionale fanno parte di un quadro di preparazione a più livelli, in cui il coordinamento e la cooperazione a livello dell'UE e regionale sono integrati da un'azione nazionale.

3. Prove di stress

Le prove di stress sono un aspetto fondamentale della preparazione, come riconosciuto nella raccomandazione del Consiglio sul rafforzamento della resilienza delle infrastrutture critiche¹⁸. Nel settore finanziario, le prove di stress costituiscono già una parte integrante ed essenziale della vigilanza degli enti finanziari e dei fornitori di infrastrutture del mercato finanziario. Le prove di stress rafforzano la preparazione del settore finanziario simulando gravi crisi (come recessioni, shock climatici o attacchi informatici) in modo da individuare le vulnerabilità del capitale e della liquidità degli enti finanziari. Ciò costringe gli enti e i fornitori a migliorare la gestione del rischio, aumentare le riserve di capitale, perfezionare la pianificazione strategica e rafforzare la resilienza agli shock futuri, migliorando la stabilità finanziaria complessiva e rafforzando la fiducia del mercato.

¹⁸ Raccomandazione del Consiglio, dell'8 dicembre 2022, su un approccio coordinato a livello dell'Unione per rafforzare la resilienza delle infrastrutture critiche (2023/C 20/01).

Le prove di stress contribuiscono inoltre alla preparazione individuando fonti di rischi sistemici e transfrontalieri, tra cui le fonti di instabilità finanziaria globale, le tensioni geopolitiche, gli incidenti informatici e le perturbazioni delle infrastrutture critiche.

Nel **sistema bancario**, l'Autorità bancaria europea (ABE) ha il mandato di avviare e coordinare prove di stress a livello dell'UE per il settore bancario. Sulla base di tale mandato, l'ABE effettua ogni due anni una prova di stress a livello dell'UE che copre circa il 75 % del settore bancario. La direttiva sui requisiti patrimoniali impone inoltre alle autorità competenti di effettuare ove opportuno, ma almeno una volta l'anno, prove di stress prudenziali sugli enti soggetti alla loro vigilanza. Inoltre l'ABE ha emanato orientamenti volti a garantire che le autorità utilizzino una metodologia comune nello svolgimento delle prove di stress prudenziali annuali.

All'interno dell'Unione bancaria, la BCE effettua regolarmente prove di stress, analisi e simulazioni di scenari al fine di orientare il processo di revisione e valutazione prudenziale. La BCE effettua inoltre revisioni mirate della ciberresilienza e degli accordi di esternalizzazione.

Nel **settore dell'assicurazione e dei fondi pensione aziendali o professionali**, l'EIOPA effettua regolarmente ogni tre anni prove di stress a livello dell'UE per le imprese di assicurazione e di riassicurazione e per i fondi pensione aziendali o professionali (EPAP)¹⁹, compresa una componente di rischio informatico e di rischio climatico.

L'Autorità europea degli strumenti finanziari e dei mercati (ESMA) effettua periodicamente prove di stress a livello dell'UE sulla resilienza delle CCP, nel quadro delle valutazioni di cui all'articolo 32 del regolamento ESMA e all'articolo 24 bis del regolamento EMIR. Sebbene tali prove si concentrino sulla resilienza delle CCP agli sviluppi negativi dei mercati, l'ESMA include anche altri tipi di rischi esogeni.

Il Comitato europeo per il rischio sistemico (CERS) elabora scenari avversi per le prove di stress dell'ABE (banche), dell'EIOPA (assicurazioni, fondi pensione) e dell'ESMA (CCP).

La direttiva 2014/49/UE relativa ai sistemi di garanzia dei depositi (SGD) impone agli Stati membri di svolgere i loro compiti a norma della direttiva. I risultati di tali prove sono poi utilizzati dall'ABE per svolgere esami tra pari al fine di esaminare la resilienza degli SGD.

4. Prospettiva futura

Il settore finanziario dell'UE è sostenuto da un quadro di preparazione solido e multidimensionale, costituito da una normativa settoriale specifica, da una normativa trasversale e da meccanismi di cooperazione trasversali a tutti i settori e a tutti gli Stati membri. La preparazione del settore finanziario dell'UE presenta anche una dimensione esterna, grazie

¹⁹ In diversi Stati membri i fondi pensione aziendali o professionali non rientrano nell'ambito di applicazione della direttiva EPAP II e pertanto non sono disciplinati dalle norme dell'UE. Tali fondi pensione non sono soggetti alle prove di stress dell'EIOPA.

alla quale l'UE rafforza non solo la propria stabilità finanziaria, ma anche il proprio ruolo di settore finanziario affidabile e credibile a livello mondiale.

Il settore finanziario dell'UE ha dimostrato la propria resilienza durante le crisi passate. Ha dimostrato la capacità di resistere alle tempeste della pandemia di COVID-19, all'aggressione dell'Ucraina da parte della Russia, alle crisi finanziarie in altre giurisdizioni, agli attacchi informatici e a molti altri eventi.

Tuttavia, alla luce delle minacce senza precedenti e del contesto geopolitico più incerto che l'UE si trova ad affrontare, è importante valutare costantemente il livello di preparazione del settore finanziario dell'UE. L'UE sta portando avanti questo impegno e può avviare gli adeguamenti necessari per garantire azioni preventive e reattive rapide, concertate e proporzionate, sia a livello dell'UE che degli Stati membri, al fine di mantenere una rotta stabile e preservare le funzioni vitali del settore finanziario dell'UE. In futuro, si prevede che lo sviluppo dell'Unione del risparmio e degli investimenti e l'introduzione dell'euro digitale rafforzeranno la resilienza complessiva del settore finanziario dell'UE e il suo livello di preparazione.