COMMISSIONE
EUROPEA

Bruxelles, 24.9.2020
COM(2020) 595 final

2020/0266 (COD)

Proposta di

REGOLAMENTO DEL PARLAMENTO EUROPEO E DEL CONSIGLIO

relativo alla resilienza operativa digitale per il settore finanziario e che modifica i regolamenti (CE) n. 1060/2009, (UE) n. 648/2012, (UE) n. 600/2014 e (UE) n. 909/2014

(Testo rilevante ai fini del SEE)

{SEC(2020) 307 final} - {SWD(2020) 198 final} - {SWD(2020) 199 final}

RELAZIONE

1. CONTESTO DELLA PROPOSTA

- Motivi e obiettivi della proposta

La presente proposta fa parte del pacchetto sulla finanza digitale, un pacchetto di misure volte a consentire e sostenere ulteriormente il potenziale della finanza digitale in termini di innovazione e concorrenza, attenuando nel contempo i rischi che ne derivano. Essa è in linea con le priorità della Commissione di preparare l'Europa per l'era digitale e costruire un'economia pronta per le sfide del futuro e al servizio dei cittadini. Il pacchetto sulla finanza digitale comprende una nuova strategia in materia di finanza digitale per il settore finanziario dell'UE[1] avente lo scopo di garantire che l'Unione abbracci la rivoluzione digitale e ne assuma la guida con le imprese europee innovative in prima linea, offrendo alle imprese e ai consumatori i benefici della finanza digitale. Oltre alla presente proposta, il pacchetto comprende anche una proposta di regolamento in materia di mercati delle cripto-attività[2], una proposta di regolamento relativa a un regime pilota sulle infrastrutture di mercato della tecnologia di registro distribuito (DLT)[3] e una proposta di direttiva volta a chiarire o modificare determinate norme collegate dell'UE in materia di servizi finanziari[4].La digitalizzazione e la resilienza operativa del settore finanziario sono le due facce della medesima medaglia. Le tecnologie digitali, o tecnologie dell'informazione e della comunicazione (TIC), offrono opportunità ma presentano anche rischi, che occorre comprendere e gestire adeguatamente, soprattutto in periodi di stress.

I responsabili politici e le autorità di vigilanza hanno pertanto dedicato un'attenzione sempre maggiore ai rischi connessi alla dipendenza dalle TIC, cercando in particolare di accrescere la resilienza delle imprese tramite la definizione di norme e il coordinamento del lavoro di regolamentazione e di vigilanza. Tale lavoro si è svolto a livello sia internazionale che europeo, tanto sul piano intersettoriale quanto in una serie di settori specifici, tra cui quello dei servizi finanziari.

I rischi relativi alle TIC continuano però a rappresentare una sfida per la resilienza operativa, le prestazioni e la stabilità del sistema finanziario dell'UE. La riforma che è seguita alla crisi finanziaria del 2008 ha rafforzato in primo luogo la resilienza finanziaria[5] del settore finanziario dell'UE, affrontando solo indirettamente i rischi relativi alle TIC in alcuni ambiti, nel quadro di misure volte a contrastare in generale i rischi operativi.

Le modifiche alla legislazione dell'UE in materia di servizi finanziari introdotte dopo la crisi hanno creato un codice unico che disciplina gran parte dei rischi finanziari associati ai servizi finanziari ma non hanno affrontato in maniera esaustiva il problema della resilienza operativa

---

1 Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni, relativa a una strategia in materia di finanza digitale per l'UE, (COM(2020) 591 del 24 settembre 2020).

2 Proposta di regolamento del Parlamento europeo e del Consiglio relativo ai mercati delle cripto-attività e che modifica la direttiva (UE) 2019/1937 (COM(2020) 593).

3 Proposta di regolamento del Parlamento europeo e del Consiglio relativo a un regime pilota per le infrastrutture di mercato basate sulla tecnologia di registro distribuito (COM(2020) 594).

4 Proposta di direttiva del Parlamento europeo e del Consiglio che modifica le direttive 2006/43/CE, 2009/65/CE, 2009/138/CE, 2011/61/UE, 2013/36/UE, 2014/65/UE, (UE) 2015/2366 e (UE) 2016/2341 (COM(2020) 596).

5 Le diverse misure adottate miravano essenzialmente a incrementare le risorse di capitale e la liquidità delle entità finanziarie, nonché a ridurre i rischi di credito e di mercato.

digitale. Le misure adottate in relazione a quest'ultimo aspetto erano contraddistinte da una serie di elementi che ne limitavano l'efficacia. Ad esempio, spesso si è trattato di misure concepite come direttive di armonizzazione minima o regolamenti basati sui principi che lasciavano ampio spazio ad approcci divergenti nell'ambito del mercato unico. Inoltre i rischi relativi alle TIC hanno ricevuto un'attenzione limitata o incompleta nel contesto della copertura dei rischi operativi. Infine queste misure variano a seconda della legislazione settoriale in materia di servizi finanziari. Pertanto l'intervento a livello di Unione europea non ha corrisposto pienamente a quanto necessario alle entità finanziarie europee per garantire una gestione dei rischi operativi che consenta di resistere e reagire all'impatto degli incidenti connessi alle TIC e di riprendersi dai relativi effetti. Non ha neppure fornito alle autorità di vigilanza finanziaria gli strumenti più adeguati per adempiere il loro mandato di prevenire l'instabilità finanziaria derivante dalla materializzazione di tali rischi relativi alle TIC.

L'assenza di norme dettagliate e complete sulla resilienza operativa digitale a livello di UE ha portato alla proliferazione di iniziative di regolamentazione (ad esempio sui test di resilienza operativa digitale) e di approcci di vigilanza (ad esempio per quanto riguarda le dipendenze da terzi nel settore delle TIC) a livello nazionale. L'azione a livello di Stati membri ha tuttavia un effetto limitato, a causa della natura transfrontaliera dei rischi relativi alle TIC. Per di più la mancanza di coordinamento delle iniziative nazionali ha dato luogo a sovrapposizioni, incoerenze, duplicazione di requisiti, elevati costi amministrativi e di conformità (soprattutto per le entità finanziarie transfrontaliere) oppure ha impedito di individuare e quindi affrontare i rischi relativi alle TIC. Questa situazione determina la frammentazione del mercato unico, compromette la stabilità e l'integrità del settore finanziario dell'UE e mette a repentaglio la protezione dei consumatori e degli investitori.

È pertanto necessario mettere a punto un quadro dettagliato e completo sulla resilienza operativa digitale per le entità finanziarie dell'UE. Tale quadro approfondirà la dimensione della gestione dei rischi digitali del codice unico, e in particolare migliorerà e razionalizzerà la gestione dei rischi relativi alle TIC da parte delle entità finanziarie, istituirà test accurati dei sistemi di TIC e accrescerà la consapevolezza da parte delle autorità di vigilanza dei rischi informatici e degli incidenti connessi alle TIC cui sono esposte le entità finanziarie, conferirà inoltre alle autorità di vigilanza finanziaria poteri di sorveglianza sui rischi dovuti alla dipendenza delle entità finanziarie da fornitori terzi di servizi di TIC. La proposta istituirà un meccanismo coerente di segnalazione degli incidenti, che contribuirà a ridurre gli oneri amministrativi per le entità finanziarie e a rafforzare l'efficacia della vigilanza.

- Coerenza con le disposizioni vigenti nel settore normativo interessato

La presente proposta si inserisce in un lavoro più ampio, in corso a livello europeo e internazionale, per rafforzare la cibersicurezza nei servizi finanziari e affrontare in generale i rischi operativi[6].

Risponde inoltre al parere tecnico congiunto[7] formulato nel 2019 dalle autorità europee di vigilanza (AEV) che invitava ad adottare un approccio più coerente nei confronti dei rischi relativi alle TIC in campo finanziario, raccomandando alla Commissione di rafforzare, in maniera proporzionata, la resilienza operativa digitale del settore dei servizi finanziari

[6] Comitato di Basilea per la vigilanza bancaria, *Cyber-resilience: Range of practices*, dicembre 2018 e *Principles for sound management of operational risk (PSMOR)*, ottobre 2014.

[7] Joint Advice of the European Supervisory Authorities to the European Commission on the need for legislative improvements relating to ICT risk management requirements in the EU financial sector, JC 2019 26 (2019).

mediante una specifica iniziativa settoriale dell'UE. Il parere delle AEV costituiva la risposta al piano d'azione per le tecnologie finanziarie adottato dalla Commissione nel 2018[8].

- Coerenza con le altre normative dell'Unione

Come affermato dalla presidente von der Leyen nei suoi orientamenti politici[9] e come si legge nella comunicazione "Plasmare il futuro digitale dell'Europa"[10], è fondamentale che l'Europa colga tutti i vantaggi dell'era digitale e rafforzi la sua industria e la sua capacità di innovazione entro limiti sicuri ed etici. La strategia europea per i dati[11] stabilisce quattro pilastri, ovvero protezione dei dati, diritti fondamentali, sicurezza e cibersicurezza, come prerequisiti essenziali per una società che, grazie all'uso dei dati, disponga di maggiori strumenti. Più di recente il Parlamento europeo ha avviato i lavori su una relazione in materia di finanza digitale, che esorta tra l'altro ad adottare un approccio comune sulla ciberresilienza del settore finanziario[12].Un quadro legislativo che rafforzi la resilienza operativa digitale delle entità finanziarie dell'UE è coerente con questi obiettivi politici. La proposta sosterrebbe inoltre le politiche volte a favorire la ripresa dopo la pandemia di COVID-19, in quanto garantirebbe che l'accresciuta dipendenza dalla finanza digitale vada di pari passo con la resilienza operativa.

L'iniziativa conserverebbe i benefici connessi al quadro orizzontale sulla cibersicurezza (ad esempio la direttiva sulla sicurezza delle reti e dei sistemi informativi, direttiva NIS) mantenendo il settore finanziario nel proprio ambito di applicazione. Il settore finanziario rimarrebbe strettamente associato all'organismo di cooperazione NIS e le autorità di vigilanza finanziaria potrebbero scambiare informazioni pertinenti nell'ambito dell'ecosistema NIS esistente. L'iniziativa sarebbe coerente con la direttiva sulle infrastrutture critiche europee, di cui attualmente è in corso una revisione volta a migliorare la protezione e la resilienza delle infrastrutture critiche rispetto alle minacce non informatiche. Questa proposta è infine pienamente in linea con la strategia per l'Unione della sicurezza[13] che auspica un'iniziativa per la resilienza operativa digitale nel settore finanziario, considerata l'elevata dipendenza di quest'ultimo dai servizi di TIC e la sua elevata vulnerabilità agli attacchi informatici.

2. BASE GIURIDICA, SUSSIDIARIETÀ E PROPORZIONALITÀ

- Base giuridica

La proposta di regolamento si basa sull'articolo 114 TFUE.

---

8 Commissione europea, *Piano d'azione per le tecnologie finanziarie* (COM(2018) 0109 final).

9 Presidente Ursula von der Leyen, Orientamenti politici per la prossima Commissione europea, 2019-2024, https://ec.europa.eu/commission/sites/beta-political/files/political-guidelines-next-commission_it.pdf.

10 Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni, *Plasmare il futuro digitale dell'Europa* (COM(2020) 67 final).

11 Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni, *Una strategia europea per i dati* (COM(2020) 66 final).

12 Relazione recante raccomandazioni alla Commissione sulla finanza digitale: rischi emergenti legati alle cripto-attività - sfide a livello della regolamentazione e della vigilanza nel settore dei servizi, degli istituti e dei mercati finanziari (2020/2034(INL)) https://oeil.secure.europarl.europa.eu/oeil/popups/ficheprocedure.do?reference=2020/2034(INL)&l=en.

13 Comunicazione della Commissione al Parlamento europeo, al Consiglio europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni sulla strategia dell'UE per l'Unione della sicurezza (COM(2020) 605 final).

Essa elimina gli ostacoli che si frappongono all'istituzione del mercato interno dei servizi finanziari e ne migliora il funzionamento, armonizzando le norme applicabili nel settore della gestione e della segnalazione dei rischi relativi alle TIC, dei relativi test e dei rischi relativi alle TIC derivanti da terzi. Le disparità che si riscontrano attualmente in questo settore a livello legislativo e di vigilanza, sia a livello nazionale che di Unione europea, ostacolano il mercato unico dei servizi finanziari, poiché le entità finanziarie impegnate in attività transfrontaliere si trovano a dover soddisfare prescrizioni normative o aspettative di vigilanza differenti, quando non addirittura in sovrapposizione, e potenzialmente tali da intralciare le libertà di stabilimento e la liberazione prestazione di servizi. La differenza di norme falsa anche la concorrenza tra entità finanziarie dello stesso tipo attive in Stati membri diversi. Inoltre in settori in cui l'armonizzazione è assente, parziale o limitata, la definizione di norme o approcci nazionali divergenti, già in vigore oppure in via di adozione e attuazione a livello nazionale, può costituire un deterrente per le libertà del mercato unico dei servizi finanziari. Questa osservazione vale in particolare nel caso dei quadri per l'esecuzione dei test operativi digitali e per la sorveglianza dei fornitori terzi di servizi di TIC critici.

Dato che la proposta incide su varie direttive del Parlamento europeo e del Consiglio adottate sulla base dell'articolo 53, paragrafo 1, TFUE, contestualmente viene adottata una proposta di direttiva per introdurre le necessarie modifiche a dette direttive.

- Sussidiarietà

L'alto grado di interconnessione tra i servizi finanziari, la cospicua attività transfrontaliera delle entità finanziarie e l'estesa dipendenza dell'intero settore finanziario da fornitori terzi di servizi di TIC richiedono una forte resilienza operativa digitale, che rappresenta una questione di interesse comune per mantenere la solidità dei mercati finanziari dell'UE. Le disparità derivanti da regimi non uniformi o parziali, da sovrapposizioni o dalla molteplicità di prescrizioni applicabili alle medesime entità finanziarie operanti a livello transfrontaliero o che detengono numerose autorizzazioni[14] nell'ambito del mercato unico si possono affrontare in maniera efficace solo a livello di Unione europea.

La presente proposta armonizza la componente operativa digitale di un settore profondamente integrato e interconnesso, che già dispone, in quasi tutti gli altri ambiti principali, di un sistema unico di regolamentazione e vigilanza. Per quanto riguarda questioni come la segnalazione degli incidenti connessi alle TIC, solo norme armonizzate a livello di Unione potrebbero ridurre gli oneri amministrativi e i costi finanziari derivanti dalla segnalazione di un medesimo incidente a differenti autorità nazionali e dell'Unione. L'azione dell'UE è necessaria anche per agevolare il riconoscimento reciproco dei test avanzati sulla resilienza operativa digitale per le entità operanti a livello transfrontaliero, le quali, in assenza di norme dell'Unione, sono o possono essere soggette a quadri diversi nei differenti Stati membri. Solo un'azione a livello di Unione può colmare le differenze tra gli approcci ai test adottati dagli Stati membri. Un'azione estesa a tutta l'UE è necessaria anche per sopperire alla carenza di adeguati poteri di sorveglianza per monitorare i rischi causati da fornitori terzi di servizi di TIC, compresi i rischi di concentrazione e di contagio per il settore finanziario dell'UE.

[14] La stessa entità finanziaria può detenere autorizzazioni a operare quale banca, impresa di investimento e istituto di pagamento, ciascuna delle quali rilasciata da una diversa autorità di vigilanza in uno o più Stati membri.

- Proporzionalità

Le norme proposte non vanno al di là di quanto necessario per conseguire gli obiettivi della proposta. Riguardano soltanto gli aspetti che gli Stati membri non possono disciplinare da soli e in cui gli oneri e i costi amministrativi sono commisurati agli obiettivi specifici e generali da conseguire.

Per quanto riguarda l'ambito di applicazione e l'intensità, la proporzionalità è concepita mediante il ricorso a criteri di valutazione qualitativi e quantitativi. Tali criteri mirano a garantire che le nuove norme si estendano a tutte le entità finanziarie, ma allo stesso tempo siano adeguate ai rischi e alle esigenze delle loro specifiche caratteristiche in termini di dimensioni e profilo commerciale. La proporzionalità è integrata anche nelle norme in materia di gestione dei rischi relativi alle TIC, test di resilienza digitale, segnalazione di incidenti gravi connessi alle TIC e sorveglianza dei fornitori terzi di servizi di TIC critici.

- Scelta dell'atto giuridico

Le misure necessarie per disciplinare la gestione dei rischi relativi alle TIC, la segnalazione dei rischi connessi alle TIC nonché i test e la sorveglianza dei fornitori terzi di servizi di TIC critici devono essere inserite in un regolamento, allo scopo di garantire che le prescrizioni dettagliate siano efficacemente e direttamente applicabili in maniera uniforme, fatte salve la proporzionalità e le norme specifiche previste del presente regolamento. Un approccio coerente ai rischi operativi digitali contribuisce ad accrescere la fiducia nel sistema finanziario e ne preserva la stabilità. Dal momento che il ricorso a un regolamento serve a ridurre la complessità della regolamentazione, favorisce la convergenza della vigilanza e accresce la certezza del diritto, il presente regolamento contribuisce pure a limitare i costi di conformità a carico delle entità finanziarie, specialmente per quelle che operano a livello transfrontaliero, circostanza questa che, a sua volta, parteciperebbe all'eliminazione delle distorsioni della concorrenza.

Il presente regolamento cancella inoltre le disparità legislative e la disomogeneità degli approcci normativi o di vigilanza ai rischi relativi alle TIC rimuovendo in tal modo gli ostacoli al mercato unico dei servizi finanziari, in particolare per quanto riguarda il regolare esercizio della libertà di stabilimento e della libera prestazione di servizi per le entità finanziarie con una presenza transfrontaliera.

Infine il codice unico è stato sviluppato in gran parte per mezzo di regolamenti, ed è opportuno che la scelta dello strumento giuridico da utilizzare per l'aggiornamento che introduce la componente della resilienza operativa digitale si attenga a quelle operate in precedenza.

3. RISULTATI DELLE VALUTAZIONI EX POST, DELLE CONSULTAZIONI DEI PORTATORI DI INTERESSI E DELLE VALUTAZIONI D'IMPATTO

- Valutazioni ex post/Vaglio di adeguatezza della legislazione vigente

Finora la legislazione dell'Unione in materia di servizi finanziari non ha disciplinato la resilienza operativa, né ha affrontato su un piano generale i rischi derivanti dalla digitalizzazione, neppure quella le cui norme si occupano più in generale della dimensione del rischio operativo (di cui i rischi relativi alle TIC costituiscono una sottocomponente). Fino a oggi gli interventi dell'Unione hanno contribuito ad affrontare esigenze e problemi sorti sulla scia della crisi finanziaria del 2008: gli enti creditizi non erano sufficientemente capitalizzati, i mercati finanziari non erano sufficientemente integrati e fino a quel momento

l'armonizzazione era stata mantenuta a livelli minimi. All'epoca i rischi relativi alle TIC non erano considerati una priorità, e di conseguenza il quadro giuridico dei diversi sottosettori finanziari si è evoluto senza alcun coordinamento. L'azione dell'Unione ha comunque raggiunto l'obiettivo di assicurare la stabilità finanziaria e di fissare un unico insieme armonizzato di norme prudenziali e di condotta sul mercato, applicabile alle entità finanziarie in tutta l'UE. Dal momento che i fattori su cui in passato si è fondato l'intervento legislativo dell'Unione non hanno dato luogo a norme specifiche o generali per affrontare il diffuso utilizzo delle tecnologie digitali e i rischi che ne derivano in campo finanziario, lo svolgimento di una valutazione esplicita appare difficile. Ciascun pilastro del presente regolamento riflette un esercizio di valutazione implicito e le conseguenti modifiche legislative.

- Consultazioni dei portatori di interessi

La Commissione ha consultato i portatori di interessi durante tutto il processo di elaborazione della presente proposta; in particolare:

i) la Commissione ha condotto un'apposita consultazione pubblica aperta (dal 19 dicembre 2019 al 19 marzo 2020)[15];

ii) la Commissione ha consultato l'opinione pubblica tramite una valutazione d'impatto iniziale (dal 19 dicembre 2019 al 16 gennaio 2020)[16];

iii) i servizi della Commissione hanno consultato gli esperti degli Stati membri in seno al gruppo di esperti sull'attività bancaria, i pagamenti e le assicurazioni (CEGBPI) in due distinte occasioni (18 maggio 2020 e 16 luglio 2020)[17];

iv) i servizi della Commissione hanno organizzato un webinar dedicato alla resilienza operativa digitale nell'ambito della serie di eventi di sensibilizzazione sulla finanza digitale tenutisi nel 2020 (Digital Finance Outreach) (19 maggio 2020).

La consultazione pubblica si prefiggeva lo scopo di fornire informazioni alla Commissione per la definizione di un potenziale quadro intersettoriale dell'UE per la resilienza operativa digitale nel settore dei servizi finanziari. Dalle risposte è emerso un ampio sostegno all'introduzione di un quadro dedicato, che concentri le azioni sulle quattro aree oggetto della consultazione; è stata peraltro sottolineata l'esigenza di garantire la proporzionalità nonché di esaminare e illustrare attentamente l'interazione con le norme orizzontali della direttiva NIS. La Commissione ha ricevuto due risposte sulla valutazione d'impatto iniziale, nelle quali i rispondenti hanno trattato aspetti specifici relativi al proprio settore di attività.

Nel corso della riunione del CEGBPI, organizzata il 18 maggio 2020, gli Stati membri hanno espresso un convinto sostegno al rafforzamento della resilienza operativa digitale del settore finanziario, da realizzare tramite le azioni previste nell'ambito dei quattro elementi delineati dalla Commissione. Gli Stati membri hanno altresì ribadito la necessità di una chiara articolazione delle nuove norme con quelle concernenti il rischio operativo (nel quadro della

[15] https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12090-Digital-Operational-Resilience-of-Financial-Services-DORFS-Act-/public-consultation.

[16] https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12090-Digital-Operational-Resilience-of-Financial-Services-DORFS-Act-.

[17] https://ec.europa.eu/info/business-economy-euro/banking-and-finance/regulatory-process-financial-services/expert-groups-comitology-and-other-committees/expert-group-banking-payments-and-insurance_en.

legislazione dell'UE in materia di servizi finanziari) e con le norme orizzontali in materia di cibersicurezza (direttiva NIS). Durante la seconda riunione alcuni Stati membri hanno posto l'accento sull'esigenza di assicurare la proporzionalità e di tener presente la situazione specifica delle piccole imprese o delle controllate di grandi gruppi, nonché sulla necessità di conferire un mandato forte alle ANC (autorità nazionali competenti) partecipanti all'attività di sorveglianza.

La proposta si basa inoltre sui riscontri ricevuti nelle riunioni con i portatori di interessi e con le autorità e le istituzioni dell'UE, di cui ha tenuto conto. I portatori di interessi, compresi i fornitori terzi di servizi di TIC, si sono mostrati nel complesso favorevoli. Dall'analisi dei riscontri ricevuti emerge anzitutto l'invito a preservare la proporzionalità e a seguire, nell'elaborazione delle norme, un approccio basato su principi e rischi. Per quanto riguarda le istituzioni, l'apporto principale è stato offerto dal Comitato europeo per il rischio sistemico (CERS), dalle AEV, dall'Agenzia dell'Unione europea per la cibersicurezza (ENISA) e dalla Banca centrale europea (BCE), oltre che dalle autorità competenti degli Stati membri.

- Assunzione e uso di perizie

Nell'elaborare la presente proposta, la Commissione si è basata su prove qualitative e quantitative raccolte da fonti riconosciute, tra cui i due pareri tecnici congiunti delle AEV. A queste si aggiungono contributi riservati e le relazioni pubblicamente disponibili delle autorità di vigilanza, degli organismi internazionali di normazione e dei principali istituti di ricerca, nonché il contributo quantitativo e qualitativo dei portatori di interessi individuati in tutto il settore finanziario mondiale.

- Valutazione d'impatto

La presente proposta è accompagnata da una valutazione d'impatto[18], che è stata presentata al comitato per il controllo normativo il 29 aprile 2020 e approvata il 29 maggio 2020. Il comitato per il controllo normativo ha raccomandato miglioramenti in alcuni ambiti al fine di: i) fornire maggiori informazioni sulle modalità per garantire la proporzionalità; ii) evidenziare meglio in che misura l'opzione prescelta differisca dal parere tecnico congiunto delle AEV, e il motivo per cui tale opzione sarebbe quella ottimale; iii) precisare meglio le modalità di interazione della proposta con la vigente legislazione dell'UE, comprese le norme attualmente in corso di revisione. La valutazione d'impatto è stata adeguata per tener conto di questi punti, considerando altresì osservazioni più dettagliate formulate dallo stesso comitato.

La Commissione ha esaminato una serie di opzioni per lo sviluppo di un quadro di resilienza operativa digitale:

- "nessun provvedimento". Le norme sulla resilienza operativa continuerebbero a fondarsi sull'attuale insieme di disposizioni dell'UE in materia di servizi finanziari (che registra varie divergenze), in parte sulla direttiva sulla sicurezza delle reti e dei sistemi informativi (direttiva NIS) e sui regimi nazionali vigenti o futuri;
- opzione 1 – rafforzamento delle riserve di capitale. Si introdurrebbero riserve di capitale aggiuntive per rafforzare la capacità delle entità finanziarie di assorbire le

[18] Commission Staff Working Document - Impact Assessment Report Accompanying the document Regulation of the European Parliament and of the Council on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014 and (EU) No 909/2014, (SWD(2020) 198 del 24 settembre 2020).

perdite che potrebbero verificarsi a causa della mancanza di resilienza operativa digitale;

- opzione 2 – introdurre un atto sulla resilienza operativa digitale dei servizi finanziari. Consentire un quadro complessivo a livello dell'UE con norme coerenti che rispondano alle esigenze di resilienza operativa digitale di tutte le entità finanziarie regolamentate e istituire un quadro di sorveglianza per i fornitori terzi di servizi di TIC critici;
- opzione 3 – un atto sulla resilienza operativa digitale dei servizi finanziari unito alla vigilanza centralizzata sui fornitori terzi di servizi di TIC critici. Oltre all'atto sulla resilienza operativa digitale (opzione 2) si istituirebbe una nuova autorità incaricata di vigilare sulla fornitura di servizi da parte dei fornitori terzi di servizi di TIC critici.

È stata scelta la seconda opzione, che realizza la maggior parte degli obiettivi previsti in maniera efficace, efficiente e coerente con altre politiche dell'Unione. Questa opzione è quella preferita dalla maggior parte dei portatori di interessi.

L'opzione prescelta comporterebbe costi sia una tantum che ricorrenti[19]. I costi una tantum, che dipendono principalmente dagli investimenti in sistemi informatici. sono difficili da quantificare, data la diversa situazione dei complessi ambienti informatici delle imprese e in particolare dei loro sistemi informatici preesistenti. Ciò nonostante per le grandi imprese tali costi saranno probabilmente limitati, alla luce dei cospicui investimenti in TIC da queste già effettuati. Anche per le imprese più piccole i costi non dovrebbero essere elevati, in quanto si applicherebbero misure proporzionate, dato il minor rischio.

L'opzione prescelta avrebbe effetti positivi, in termini di impatto economico, sociale e ambientale, sulle PMI che operano nel settore dei servizi finanziari. Grazie alla proposta, per le PMI sarà più facile comprendere quali siano le norme da applicare, e i costi di conformità diminuiranno di conseguenza.

Il principale impatto sociale dell'opzione prescelta riguarderebbe i consumatori e gli investitori. Una maggiore resilienza operativa digitale del sistema finanziario dell'UE diminuirebbe il numero e i costi medi degli incidenti. La società nel suo complesso trarrebbe vantaggio dall'accresciuta fiducia nel settore dei servizi finanziari.

Infine, in termini di impatto ambientale, l'opzione prescelta incoraggerebbe un uso maggiore delle infrastrutture e dei servizi di TIC di ultima generazione, prevedibilmente destinati a diventare più sostenibili dal punto di vista ambientale.

- Adeguatezza normativa e semplificazione

Eliminando le sovrapposizioni tra gli obblighi di segnalazione degli incidenti connessi alle TIC si ridurrebbero gli oneri amministrativi e i costi associati. Inoltre l'armonizzazione dei test di resilienza operativa digitale, con il riconoscimento reciproco nell'ambito del mercato unico, ridurrà i costi in particolare per le imprese transfrontaliere, che altrimenti potrebbero trovarsi costrette a effettuare molteplici test nei vari Stati membri[20].

19 *Ibidem, pagg. 89-94.*
20 *Ibidem.*

- Diritti fondamentali

L'UE si è impegnata a garantire elevati livelli di protezione dei diritti fondamentali. Tutti i meccanismi volontari di condivisione delle informazioni tra entità finanziarie promosse dal presente regolamento sarebbero attuati in ambienti sicuri nel pieno rispetto delle norme dell'Unione in materia di protezione dei dati, in particolare del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio[21], soprattutto allorché il trattamento di dati personali è necessario per il perseguimento di un legittimo interesse da parte del titolare del trattamento.

4. INCIDENZA SUL BILANCIO

In termini di incidenza sul bilancio, dal momento che il presente regolamento rafforza il ruolo delle AEV conferendo loro i poteri per sorvegliare adeguatamente i fornitori terzi di servizi di TIC critici, la proposta comporterebbe l'impiego di maggiori risorse, in particolare per lo svolgimento delle missioni di vigilanza (come ispezioni in loco e online e gli audit) e il ricorso a personale che possieda specifiche competenze in materia di sicurezza delle TIC.

L'entità e la ripartizione di tali costi dipenderanno dall'ampiezza dei nuovi poteri di sorveglianza e dai (precisi) compiti che le AEV dovranno svolgere. Per quanto riguarda le nuove risorse di personale, l'ABE, l'ESMA e l'EIOPA avranno bisogno in totale di 18 dipendenti a tempo pieno (ETP) (sei per ciascuna autorità) quando le varie disposizioni della proposta entreranno in applicazione (per un importo stimato di 15,71 milioni di EUR per il periodo 2022-2027). Le AEV dovranno sostenere anche costi informatici aggiuntivi, spese di missione per le ispezioni in loco e costi di traduzione (per un importo stimato di 12 milioni di EUR per il periodo 2022-2027), nonché altre spese amministrative (secondo le stime 2,48 milioni di EUR per il periodo 2022-2027). Pertanto l'impatto totale dei costi ammonta, secondo le stime, a circa 30,19 milioni di EUR per il periodo 2022-2027.

Si noti inoltre che il numero degli effettivi (ad esempio nuovi membri del personale e altre spese connesse ai nuovi compiti) necessari alla sorveglianza diretta dipenderà, nel corso del tempo, dall'evoluzione del numero e delle dimensioni dei fornitori terzi di servizi di TIC critici da sorvegliare, ma la spesa corrispondente sarà interamente finanziata dalle commissioni pagate da questi partecipanti al mercato. Non si prevede perciò alcun impatto sugli stanziamenti di bilancio dell'UE (a eccezione del personale aggiuntivo), poiché tali costi saranno interamente finanziati dalle commissioni in questione.

L'impatto finanziario e sul bilancio della presente proposta è spiegato in dettaglio nella scheda finanziaria legislativa allegata.

5. ALTRI ELEMENTI

- Piani attuativi e modalità di monitoraggio, valutazione e segnalazione

La proposta comprende un piano generale per il monitoraggio e la valutazione dell'impatto sugli obiettivi specifici, che impone alla Commissione di svolgere un riesame almeno tre anni dopo l'entrata in vigore e di comunicarne i risultati principali al Parlamento europeo e al Consiglio.

[21] Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati) (GU L 119 del 4.5.2016, pag. 1).

Il riesame dovrebbe svolgersi conformemente agli orientamenti per legiferare meglio della Commissione.

- Illustrazione dettagliata delle singole disposizioni della proposta

La proposta si articola in vari settori d'intervento principali, che costituiscono pilastri essenziali interconnessi inclusi in maniera consensuale negli orientamenti e nelle migliori pratiche a livello europeo e internazionale allo scopo di promuovere la resilienza informatica e operativa del settore finanziario.

Ambito di applicazione del regolamento e applicazione proporzionale delle misure richieste (articolo 2)

Per garantire la coerenza delle prescrizioni in materia di gestione dei rischi relativi alle TIC applicabili al settore finanziario, il regolamento copre un ampio ventaglio di entità finanziarie regolamentate a livello di Unione, ossia enti creditizi, istituti di pagamento, istituti di moneta elettronica, imprese di investimento, fornitori di servizi per le cripto-attività, depositari centrali di titoli, controparti centrali, sedi di negoziazione, repertori di dati sulle negoziazioni, gestori di fondi di investimento alternativi e società di gestione, fornitori di servizi di comunicazione dati, imprese di assicurazione e di riassicurazione, intermediari assicurativi, intermediari riassicurativi e intermediari assicurativi a titolo accessorio, enti pensionistici aziendali o professionali, agenzie di rating del credito, revisori legali e società di revisione, amministratori di indici di riferimento critici e fornitori di servizi di crowdfunding.

Tale copertura favorisce l'applicazione omogenea e coerente di tutte le componenti della gestione del rischio nei settori connessi alle TIC, salvaguardando contemporaneamente la parità di condizioni tra le entità finanziarie per quanto riguarda gli obblighi normativi in materia di rischi relativi alle TIC. Allo stesso tempo il regolamento riconosce l'esistenza di differenze significative tra le entità finanziarie in termini di dimensioni, profilo commerciale o esposizione al rischio digitale. Dato che le entità finanziarie più grandi dispongono di maggiori risorse, solo le entità finanziarie che non rientrano nella definizione di microimprese hanno l'obbligo, ad esempio, di introdurre complesse disposizioni di governance e funzioni di gestione dedicate, di effettuare valutazioni approfondite dopo modifiche di rilievo delle infrastrutture di reti e dei sistemi informativi, di compiere periodicamente analisi dei rischi sui sistemi di TIC esistenti, di ampliare i test sulla continuità operativa e i piani di risposta e ripristino per descrivere gli scenari di passaggio tra le infrastrutture di TIC primarie e le attrezzature ridondanti. Inoltre solo le entità finanziarie identificate come significative ai fini dei test avanzati di resilienza digitale dovranno svolgere test di penetrazione basati su minacce.

Nonostante l'ampio ambito di applicazione soggettivo, il regolamento non è esaustivo. In particolare non riguarda gli operatori del sistema secondo la definizione di cui all'articolo 2, lettera p), della direttiva 98/26/CE[22] concernente il carattere definitivo del regolamento nei sistemi di pagamento e nei sistemi di regolamento titoli (direttiva sul carattere definitivo del regolamento), né i partecipanti al sistema, a meno che non si tratti di entità finanziarie regolamentate a livello di Unione e in quanto tali comprese nel presente regolamento a proprio titolo (ossia enti creditizi, imprese di investimento, controparti centrali). Inoltre esula

[22] Direttiva 98/26/CE del Parlamento europeo e del Consiglio, del 19 maggio 1998, concernente il carattere definitivo del regolamento nei sistemi di pagamento e nei sistemi di regolamento titoli (GU L 166 dell'11.6.1998, pag. 45).

dall'ambito di applicazione del regolamento il registro dell'Unione per le quote di emissioni che, ai sensi della direttiva 2003/87/CE[23], opera sotto l'egida della Commissione europea.

Tali esclusioni dalla direttiva sul carattere definitivo del regolamento tengono conto della necessità di riesaminare ulteriormente questioni giuridiche e politiche concernenti gli operatori del sistema e i partecipanti al sistema nel quadro della direttiva, tenendo debitamente in considerazione l'impatto dei quadri normativi che attualmente si applicano ai sistemi di pagamento[24] gestiti dalle banche centrali. Dato che tali questioni possono comportare aspetti che restano distinti dalle materie trattate dal presente regolamento, la Commissione continuerà a valutare la necessità e l'incidenza di un'ulteriore estensione dell'ambito di applicazione del regolamento in oggetto a entità e infrastrutture di TIC che attualmente ne sono escluse.

Prescrizioni relative alla governance (articolo 4)

Il presente regolamento mira a favorire un migliore allineamento delle strategie commerciali delle entità finanziarie e della gestione dei rischi relativi alle TIC. A tale scopo, l'organo di gestione sarà tenuto a mantenere un ruolo attivo e cruciale nel dirigere il quadro di gestione dei rischi relativi alle TIC e dovrà garantire il rispetto di una scrupolosa igiene informatica. La piena responsabilità dell'organo di gestione nella gestione dei rischi relativi alle TIC dell'entità finanziaria costituirà un principio generale da tradurre poi in una serie di prescrizioni specifiche, come l'attribuzione di responsabilità e ruoli precisi per tutte le funzioni relative alle TIC, l'impegno costante nel controllo del monitoraggio della gestione dei rischi relativi alle TIC nonché l'intera gamma di processi di approvazione e controllo e l'adeguata allocazione di investimenti e formazione relativi alle TIC.

Prescrizioni relative alla gestione dei rischi relativi alle TIC (articoli da 5 a 14)

La resilienza operativa digitale si fonda su una serie di prescrizioni e principi chiave concernenti il quadro di gestione dei rischi relativi alle TIC, conformemente al parere tecnico congiunto delle AEV. Tali prescrizioni, ispirate alle pertinenti norme, linee guida e raccomandazioni fissate a livello internazionale, nazionale e settoriale, vertono su funzioni specifiche nella gestione dei rischi relativi alle TIC (identificazione, protezione e prevenzione, individuazione, risposta e ripristino, apprendimento, evoluzione e comunicazione). Per tenere il passo con il rapido sviluppo del contesto delle minacce informatiche, le entità finanziarie devono: istituire e mantenere strumenti e sistemi di TIC resilienti, tali da ridurre al minimo l'impatto dei rischi relativi alle TIC; identificare costantemente tutte le fonti di rischi relativi alle TIC; introdurre misure di protezione e prevenzione; individuare tempestivamente le attività anomale; mettere in atto strategie di continuità operativa e piani di ripristino in caso di disastro come parte integrante della strategia di continuità operativa. Gli ultimi elementi sono necessari per effettuare un tempestivo ripristino dopo gli incidenti connessi alle TIC, in particolare gli attacchi informatici, limitando i danni e privilegiando una ripresa sicura delle attività. Il regolamento, di per sé, non impone una standardizzazione specifica, ma si fonda su norme tecniche riconosciute a livello europeo e internazionale oppure sulle migliori pratiche del settore, nella misura in cui queste siano pienamente conformi alle istruzioni delle autorità di vigilanza sull'utilizzo e l'integrazione di tali norme internazionali. Il presente regolamento

[23] Direttiva 2003/87/CE del Parlamento europeo e del Consiglio, del 13 ottobre 2003, che istituisce un sistema per lo scambio di quote di emissioni dei gas a effetto serra nella Comunità e che modifica la direttiva 96/61/CE del Consiglio (GU L 275 del 25.10.2003, pag. 32).

[24] In particolare il regolamento della Banca centrale europea (UE) n. 795/2014, del 3 luglio 2014, sui requisiti di sorveglianza per i sistemi di pagamento di importanza sistemica.

tratta altresì dell'integrità, la sicurezza e la resilienza delle infrastrutture e attrezzature fisiche che supportano l'uso della tecnologia nonché del personale e dei processi collegati alle TIC, nell'ambito dell'impronta digitale delle operazioni delle entità finanziarie.

Segnalazione di incidenti connessi alle TIC (articoli da 15 a 20)

L'armonizzazione e la razionalizzazione delle segnalazioni di incidenti connessi alle TIC sono realizzati, in primo luogo, tramite una prescrizione generale che impone alle entità finanziarie di stabilire e attuare un processo di gestione per monitorare e registrare gli incidenti connessi alle TIC, seguita dall'obbligo di classificare gli incidenti sulla base di criteri precisati nel regolamento e ulteriormente definiti dalle AEV per specificare le soglie di rilevanza. In secondo luogo, devono essere segnalati alle autorità competenti soltanto gli incidenti connessi alle TIC ritenuti gravi. Per il trattamento della segnalazione dovrebbe essere utilizzato un modello comune, seguendo una procedura armonizzata messa a punto dalle AEV. Le entità finanziarie dovrebbero inviare segnalazioni iniziali, intermedie e finali, informando utenti e clienti qualora l'incidente abbia o possa avere un impatto sui loro interessi finanziari. Le autorità competenti devono fornire dettagli pertinenti sugli incidenti ad altre istituzioni o autorità: le AEV, la BCE e i punti di contatto unici designati ai sensi della direttiva (UE) 2016/1148.

Per avviare tra entità finanziarie e autorità competenti un dialogo che contribuisca a ridurre al minimo l'impatto e a individuare i rimedi opportuni, la segnalazione degli incidenti gravi connessi alle TIC dovrebbe essere integrata da riscontri e orientamenti delle autorità di vigilanza.

Infine occorre esplorare ulteriormente la possibilità di centralizzare a livello di Unione le segnalazioni di incidenti connessi alle TIC, mediante una relazione congiunta delle AEV, della BCE e dell'ENISA che valuti la fattibilità dell'istituzione di un polo unico dell'UE per la segnalazione degli incidenti gravi connessi alle TIC da parte delle entità finanziarie.

Test di resilienza operativa digitale (articoli da 21 a 24)

Le capacità e le funzioni incluse nel quadro di gestione dei rischi relativi alle TIC devono essere sottoposte periodicamente a test per accertarne il grado di preparazione, identificarne punti deboli, carenze o lacune, verificarne la capacità di attuare tempestivamente misure correttive. Il presente regolamento prevede un'applicazione proporzionata delle prescrizioni in materia di test di resilienza operativa digitale, in funzione delle dimensioni e del profilo commerciale e di rischio delle entità finanziarie: tutte le entità dovrebbero svolgere test sui sistemi e gli strumenti di TIC, ma solo quelle identificate dalle autorità competenti (in base ai criteri del presente regolamento, ulteriormente definiti dalle AEV) come significative e mature sotto il profilo informatico dovrebbero avere l'obbligo di svolgere prove avanzate mediante test di penetrazione basati su minacce. Il presente regolamento fissa anche prescrizioni per i tester e impone il riconoscimento in tutta l'Unione dei risultati dei test di penetrazione basati su minacce per le entità finanziarie operanti in vari Stati membri.

Rischi relativi alle TIC derivanti da terzi (articoli da 25 a 39)

Il regolamento è concepito per garantire un solido monitoraggio dei rischi relativi alle TIC derivanti da terzi. Tale obiettivo si realizzerà in primo luogo con il rispetto delle norme basate su principi che si applicano al monitoraggio, da parte delle entità finanziarie, del rischio derivante dai fornitori terzi di TIC. In secondo luogo, il presente regolamento armonizza gli elementi essenziali del servizio e dei rapporti con i fornitori terzi di TIC. Questi elementi coprono gli aspetti minimi considerati cruciali per consentire il monitoraggio completo, da parte dell'entità finanziaria, del rischio derivante da fornitori terzi di TIC in tutte le fasi del rapporto con tali fornitori: stipula, esecuzione, estinzione e fase post-contrattuale.

In particolare, i contratti che disciplinano il rapporto dovranno contenere una descrizione completa dei servizi, l'indicazione delle località in cui i dati devono essere trattati, descrizioni complete del livello dei servizi accompagnate da obiettivi di prestazione quantitativi e qualitativi, disposizioni pertinenti in materia di accessibilità, disponibilità, integrità, sicurezza e protezione dei dati personali, nonché garanzie per l'accesso, il ripristino e la restituzione in caso di inadempienze dei fornitori terzi di servizi di TIC, termini di preavviso e obblighi di segnalazione dei fornitori terzi di servizi di TIC, diritti di accesso, ispezione e audit da parte dell'entità finanziaria o di un terzo designato a tale scopo, chiari diritti di estinzione e strategie di uscita dedicate. Dato che alcuni di questi elementi contrattuali possono essere standardizzati, il regolamento incoraggia il ricorso volontario a clausole contrattuali standard per l'utilizzo del servizio di cloud computing che dovranno essere definite dalla Commissione.

Il regolamento intende infine promuovere la convergenza per quanto riguarda gli approcci di vigilanza ai rischi relativi alle TIC derivanti da terzi nel settore finanziario, sottoponendo i fornitori terzi di servizi di TIC critici a un quadro di sorveglianza dell'Unione. Tramite un nuovo quadro legislativo armonizzato, all'AEV designata come autorità di sorveglianza capofila per ciascun fornitore terzo di servizi di TIC critico sono conferiti poteri idonei a garantire l'adeguato monitoraggio su scala paneuropea dei fornitori di servizi tecnologici che assolvono una funzione critica per il funzionamento del settore finanziario. Il quadro di sorveglianza previsto dal presente regolamento si fonda sull'architettura istituzionale esistente nel settore dei servizi finanziari, per cui il comitato congiunto delle AEV garantisce il coordinamento intersettoriale in tutte le questioni concernenti i rischi relativi alle TIC, conformemente ai propri compiti in materia di cibersicurezza, coadiuvato dal sottocomitato pertinente (forum di sorveglianza) che svolge il lavoro preparatorio per le singole decisioni e per le raccomandazioni collettive rivolte ai fornitori terzi di servizi di TIC critici.

Condivisione delle informazioni (articolo 40)

Per sensibilizzare in merito ai rischi relativi alle TIC, ridurne al minimo la propagazione, sostenere le capacità di difesa e le tecniche di individuazione delle minacce delle entità finanziarie, il regolamento consente a queste ultime di stipulare accordi per scambiarsi informazioni e dati sulle minacce informatiche.

2020/0266 (COD)

Proposta di

REGOLAMENTO DEL PARLAMENTO EUROPEO E DEL CONSIGLIO

relativo alla resilienza operativa digitale per il settore finanziario e che modifica i regolamenti (CE) n. 1060/2009, (UE) n. 648/2012, (UE) n. 600/2014 e (UE) n. 909/2014

(Testo rilevante ai fini del SEE)

IL PARLAMENTO EUROPEO E IL CONSIGLIO DELL'UNIONE EUROPEA,

visto il trattato sul funzionamento dell'Unione europea, in particolare l'articolo 114,

vista la proposta della Commissione europea,

previa trasmissione del progetto di atto legislativo ai parlamenti nazionali,

visto il parere della Banca centrale europea[25],

visto il parere del Comitato economico e sociale europeo[26],

deliberando secondo la procedura legislativa ordinaria,

considerando quanto segue:

(1) Nell'era digitale le tecnologie dell'informazione e della comunicazione (TIC) sostengono sistemi complessi impiegati nelle quotidiane attività sociali. Mantengono in funzione i principali settori delle nostre economie, tra cui la finanza, e migliorano il funzionamento del mercato unico. Il crescente grado di digitalizzazione e interconnessione amplifica d'altra parte i rischi relativi alle TIC, rendendo l'intera società, e in particolare il sistema finanziario, più vulnerabile alle minacce informatiche o alle perturbazioni delle TIC. L'uso onnipresente dei sistemi di TIC e l'elevata digitalizzazione e connettività sono oggi caratteristiche fondamentali di tutte le attività delle entità finanziarie dell'Unione, ma la resilienza digitale non è ancora sufficientemente integrata nei loro quadri operativi.

(2) Negli ultimi decenni l'uso delle TIC ha conquistato un ruolo essenziale nella finanza e oggi riveste una rilevanza critica nell'esecuzione delle consuete funzioni quotidiane di tutte le entità finanziarie. La digitalizzazione riguarda ad esempio i pagamenti, che hanno gradualmente abbandonato i metodi del contante e del cartaceo per passare a soluzioni digitali, la compensazione e il regolamento dei titoli, la negoziazione elettronica e algoritmica, le operazioni di prestito e finanziamento, la finanza tra pari, i rating del credito, la sottoscrizione di assicurazioni, la gestione dei crediti e le operazioni di back-office. Non solo l'intero settore finanziario è diventato in larga misura digitale, ma la digitalizzazione ha anche approfondito le interconnessioni e le dipendenze all'interno del settore e nei confronti di infrastrutture di terzi e fornitori terzi di servizi.

[25] [*aggiungere riferimento*] GU C del , pag. .
[26] [*aggiungere riferimento*] GU C del , pag. .

(3) In una relazione del 2020 incentrata sul rischio informatico sistemico[27], il Comitato europeo per il rischio sistemico (CERS) ha ribadito che l'attuale elevato livello di interconnessione tra entità finanziarie, mercati finanziari e infrastrutture del mercato finanziario, e in particolare l'interdipendenza dei rispettivi sistemi di TIC, costituisce una potenziale vulnerabilità sistemica dal momento che incidenti informatici localizzati potrebbero rapidamente diffondersi da una qualunque delle circa 22 000 entità finanziarie dell'Unione[28] all'intero sistema finanziario, senza trovare alcun ostacolo nelle frontiere geografiche. Gravi violazioni delle TIC che si verifichino in ambito finanziario non si limitano a colpire entità finanziarie isolate, bensì spianano anche la strada alla propagazione di vulnerabilità localizzate attraverso tutti i canali di trasmissione finanziaria e possono provocare conseguenze avverse per la stabilità del sistema finanziario dell'Unione, dando luogo a pressanti richieste di liquidità e a una generale perdita di fiducia nei mercati finanziari.

(4) Negli ultimi anni i rischi relativi alle TIC hanno richiamato l'attenzione di responsabili politici e organismi di regolamentazione e normazione che, a livello nazionale, europeo e internazionale, hanno cercato di migliorare la resilienza, fissare norme e coordinare il lavoro di regolamentazione o vigilanza. A livello internazionale il comitato di Basilea per la vigilanza bancaria, il comitato per i pagamenti e le infrastrutture di mercato, il consiglio per la stabilità finanziaria, l'istituto per la stabilità finanziaria, nonché i gruppi di paesi riuniti nel G7 e nel G20, si propongono di fornire alle autorità competenti e agli operatori del mercato di differenti giurisdizioni gli strumenti per potenziare la resilienza dei rispettivi sistemi finanziari.

(5) Benché a livello nazionale ed europeo siano state adottate iniziative politiche e legislative mirate, i rischi relativi alle TIC continuano a rappresentare una sfida per la resilienza operativa, le prestazioni e la stabilità del sistema finanziario dell'Unione. La riforma che è stata introdotta sulla scia della crisi finanziaria del 2008 ha rafforzato in primo luogo la resilienza finanziaria del settore finanziario dell'Unione, mirando a salvaguardare la competitività e la stabilità dell'Unione in una prospettica economica, prudenziale e di condotta sul mercato. Benché si inseriscano nel quadro del rischio operativo, la sicurezza delle TIC e la resilienza digitale hanno occupato un posto meno rilevante nell'agenda normativa dopo la crisi e sono state potenziate solo in alcuni settori del panorama delle politiche e della normativa dell'Unione in materia di servizi finanziari, o soltanto in alcuni Stati membri.

(6) Il piano d'azione per le tecnologie finanziarie della Commissione europea del 2018[29] ha sottolineato la fondamentale importanza di una maggiore resilienza del settore finanziario dell'Unione, anche da un punto di vista operativo, allo scopo di garantirne

---

27 ESRB report Systemic Cyber Risk, febbraio 2020, https://www.esrb.europa.eu/pub/pdf/reports/esrb.report200219_systemiccyberrisk~101a09685e.en.pdf.

28 Secondo la valutazione d'impatto che accompagna il riesame svolto dalle autorità europee di vigilanza (SWD(2017) 308), vi sono circa 5 665 enti creditizi, 5 934 imprese di investimento, 2 666 imprese di assicurazione, 1 573 EPAP, 2 500 società di gestione degli investimenti, 350 infrastrutture di mercato (come controparti centrali, borse valori, internalizzatori sistemici, repertori di dati sulle negoziazioni e sistemi multilaterali di negoziazione), 45 agenzie di rating del credito e 2 500 tra istituti di pagamento e istituti di moneta elettronica autorizzati. Si tratta in totale di circa 21 233 entità, senza contare le entità di crowdfunding, i revisori legali e le imprese di revisione contabile, i fornitori di servizi per le cripto-attività e gli amministratori degli indici di riferimento.

29 Comunicazione della Commissione al Parlamento europeo, al Consiglio, alla Banca centrale europea, al Comitato economico e sociale europeo e al Comitato delle regioni, *Piano d'azione per le tecnologie finanziarie: per un settore finanziario europeo più competitivo e innovativo* (COM/2018/0109 final), https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=CELEX%3A52018DC0109.

il buon funzionamento e la sicurezza tecnologica nonché la rapida ripresa dopo incidenti e violazioni delle TIC, consentendo in ultima analisi una fornitura efficace e ordinata dei servizi finanziari in tutta l'UE, anche in situazioni di stress, e preservando nel contempo la fiducia dei consumatori e degli operatori del mercato.

(7) Nell'aprile 2019 l'Autorità bancaria europea (ABE), l'Autorità europea degli strumenti finanziari e dei mercati (ESMA) e l'Autorità europea delle assicurazioni e delle pensioni aziendali e professionali (EIOPA) (definite collettivamente "Autorità europee di vigilanza" o "AEV") hanno pubblicato congiuntamente due pareri tecnici in cui si invocava l'adozione di un approccio coerente ai rischi relativi alle TIC nel settore finanziario e si raccomandava di potenziare, in maniera proporzionata, la resilienza operativa digitale del settore dei servizi finanziari tramite un'iniziativa settoriale dell'Unione.

(8) Il settore finanziario dell'Unione è regolamentato da un codice unico armonizzato ed è disciplinato da un sistema europeo di vigilanza finanziaria. Le disposizioni sulla resilienza operativa digitale e sulla sicurezza delle TIC non sono tuttavia ancora armonizzate in maniera completa o coerente, benché nell'era digitale la resilienza operativa digitale sia un elemento fondamentale della stabilità finanziaria e dell'integrità del mercato, non meno importante, ad esempio, delle norme comuni riguardanti gli aspetti prudenziali o la condotta sul mercato. Sarebbe quindi opportuno perfezionare il codice unico e il sistema di vigilanza per coprire anche questa componente, ampliando i mandati delle autorità di vigilanza finanziaria incaricate di monitorare e tutelare la stabilità finanziaria e l'integrità del mercato.

(9) Le disparità legislative e la disomogeneità degli approcci normativi o di vigilanza ai rischi relativi alle TIC ostacolano il mercato unico dei servizi finanziari e intralciano il regolare esercizio della libertà di stabilimento e la libera prestazione di servizi per le entità finanziarie con una presenza transfrontaliera. Può risultarne falsata anche la concorrenza tra entità finanziarie dello stesso tipo attive in Stati membri diversi. In particolare nei settori in cui l'armonizzazione a livello di Unione è stata assai limitata - come i test di resilienza operativa digitale - o assente - come il monitoraggio dei rischi relativi alle TIC derivanti da terzi - le disparità provocate dagli sviluppi previsti a livello nazionale potrebbero produrre ostacoli ulteriori al funzionamento del mercato unico, a danno dei partecipanti al mercato e della stabilità finanziaria.

(10) A livello di Unione le disposizioni sui rischi relativi alle TIC sono state finora trattate in modo soltanto parziale con carenze o sovrapposizioni in settori importanti, come la segnalazione degli incidenti connessi alle TIC e i test di resilienza operativa digitale, con conseguenti incoerenze dovute alla divergenza delle norme nazionali o al sovrapporsi di norme la cui applicazione risulta inefficiente sotto il profilo dei costi. Si tratta di una situazione particolarmente dannosa per un settore come quello finanziario, che si contraddistingue per l'intenso ricorso alle TIC; i rischi tecnologici non conoscono frontiere e il settore finanziario offre i suoi servizi su base transfrontaliera sia all'interno che all'esterno dell'Unione.

Le singole entità finanziarie che sono attive a livello transfrontaliero o detengono varie autorizzazioni (ad esempio, un'entità finanziaria può detenere autorizzazioni a operare quale banca, impresa di investimento e istituto di pagamento, ciascuna delle quali rilasciata da una diversa autorità competente in uno o più Stati membri) devono superare sfide operative poste dai rischi relativi alle TIC e dalla necessità di attenuare autonomamente gli impatti avversi degli incidenti connessi alle TIC in maniera coerente ed efficiente sotto il profilo dei costi.

(11) Dal momento che il codice unico non è accompagnato da un quadro generale per i rischi operativi o relativi alle TIC, è necessario armonizzare ulteriormente le principali prescrizioni sulla resilienza operativa digitale per tutte le entità finanziarie. Le capacità e la resilienza complessiva che le entità finanziarie acquisirebbero, sulla base di queste prescrizioni fondamentali, per resistere alle indisponibilità operative contribuirebbero a preservare la stabilità e l'integrità dei mercati finanziari dell'Unione e perciò a mantenere elevato il livello di protezione degli investitori e dei consumatori nell'Unione. Poiché il presente regolamento si propone di contribuire al regolare funzionamento del mercato unico, dovrebbe basarsi sulle disposizioni dell'articolo 114 TFUE interpretate conformemente alla giurisprudenza costante della Corte di giustizia dell'Unione europea.

(12) Il presente regolamento mira a consolidare e aggiornare le prescrizioni in materia di rischi relativi alle TIC trattati finora separatamente nei diversi regolamenti e direttive. Tali atti giuridici dell'Unione riguardavano le principali categorie di rischio finanziario (ad esempio rischio di credito, rischio di mercato, rischio di controparte e rischio di liquidità, rischio di condotta sul mercato), ma nel momento in cui sono stati adottati non potevano trattare in maniera globale tutte le componenti della resilienza operativa. Le prescrizioni sui rischi operativi ulteriormente sviluppate in questi atti giuridici dell'Unione hanno sovente privilegiato il tradizionale approccio quantitativo alla gestione dei rischi (ossia la definizione di un requisito patrimoniale a copertura dei rischi relativi alle TIC) rispetto a requisiti qualitativi mirati, in grado di promuovere le capacità tramite prescrizioni concernenti le capacità di protezione, individuazione, contenimento, ripristino e rimedio in relazione agli incidenti connessi alle TIC, oppure con la definizione di capacità di segnalazione e test digitali. Questo complesso di direttive e regolamenti si prefiggeva principalmente lo scopo di trattare le norme essenziali in materia di vigilanza prudenziale e integrità o condotta sul mercato.

Tramite il presente esercizio, che consolida e aggiorna le norme sui rischi relativi alle TIC, tutte le disposizioni in materia di rischio digitale nel settore finanziario sarebbero coerentemente riunite per la prima volta in un unico atto legislativo. La presente iniziativa dovrebbe pertanto colmare le lacune o porre rimedio alle incoerenze di taluni fra i predetti atti legislativi, anche per quanto riguarda la terminologia utilizzata, e dovrebbe fare esplicito riferimento ai rischi relativi alle TIC tramite norme specifiche in materia di capacità di gestione dei rischi relativi alle TIC, segnalazione, test e monitoraggio dei rischi derivanti da terzi.

(13) Nell'affrontare i rischi relativi alle TIC è opportuno che le entità finanziarie seguano lo stesso approccio e le stesse norme basate su principi. La coerenza contribuisce ad accrescere la fiducia nel sistema finanziario e a preservarne la stabilità, soprattutto in tempi in cui l'intensissimo uso di infrastrutture, piattaforme e sistemi di TIC comporta maggiori rischi digitali.

Il rispetto di un'igiene informatica di base dovrebbe anche evitare l'imposizione di costi elevati per l'economia, riducendo al minimo l'impatto e i costi delle perturbazioni a livello di TIC.

(14) Il ricorso a un regolamento serve a ridurre la complessità normativa, favorisce la convergenza della vigilanza, incrementa la certezza del diritto e contribuisce nel contempo a limitare i costi di conformità, specialmente per le entità finanziarie che operano a livello transfrontaliero, riducendo altresì le distorsioni della concorrenza. La scelta di un regolamento per istituire un quadro comune sulla resilienza operativa digitale delle entità finanziarie sembra pertanto il metodo più idoneo per garantire

l'applicazione omogenea e coerente di tutte le componenti della gestione dei rischi relativi alle TIC da parte dei settori finanziari dell'Unione.

(15) Accanto alla legislazione sui servizi finanziari, la direttiva (UE) 2016/1148 del Parlamento europeo e del Consiglio[30] rappresenta l'attuale quadro generale per la cibersicurezza a livello di Unione. Fra i sette settori critici, questa direttiva si applica anche a tre tipi di entità finanziarie, ossia enti creditizi, sedi di negoziazione e controparti centrali. Dal momento però che la direttiva (UE) 2016/1148 introduce un meccanismo di identificazione a livello nazionale per gli operatori di servizi essenziali, in pratica solo alcuni enti creditizi, sedi di negoziazione e controparti centrali identificati dagli Stati membri rientrano nel suo ambito di applicazione e sono quindi tenuti a rispettare le prescrizioni in materia di notifica degli incidenti e sicurezza connessi alle TIC contenute nella direttiva stessa.

(16) Dal momento che il presente regolamento accresce il livello di armonizzazione delle componenti della resilienza digitale, introducendo prescrizioni in materia di gestione dei rischi relativi alle TIC e segnalazione di incidenti connessi alle TIC più rigorose rispetto a quelle contenute nell'attuale legislazione dell'UE sui servizi finanziari, determina un incremento dell'armonizzazione anche rispetto alle prescrizioni di cui alla direttiva (UE) 2016/1148. Di conseguenza il presente regolamento costituisce una lex specialis rispetto alla direttiva (UE) 2016/1148.

È essenziale mantenere un saldo rapporto tra il settore finanziario e il quadro orizzontale di cibersicurezza dell'Unione, in modo da garantire la coerenza con le strategie di cibersicurezza già adottate dagli Stati membri e da permettere alle autorità di vigilanza finanziaria di venire a conoscenza degli incidenti informatici che colpiscono altri settori contemplati dalla direttiva (UE) 2016/1148.

(17) Per consentire un processo di apprendimento intersettoriale e attingere efficacemente alle esperienze di altri settori nella lotta alle minacce informatiche, le entità finanziarie di cui alla direttiva (UE) 2016/1148 dovrebbero continuare a far parte dell'"ecosistema" di quella direttiva (ad esempio il gruppo di cooperazione NIS e i CSIRT).

Le AEV e le autorità nazionali competenti, rispettivamente, dovrebbero poter partecipare alle discussioni strategiche delle politiche e ai lavori tecnici del gruppo di cooperazione NIS, nonché agli scambi di informazioni e a una cooperazione più approfondita con i punti di contatto unici designati ai sensi della direttiva (UE) 2016/1148. Le autorità competenti previste dal presente regolamento dovrebbero anche consultare i CSIRT nazionali designati ai sensi dell'articolo 9 della direttiva (UE) 2016/1148 e collaborare con loro.

(18) È inoltre importante garantire la coerenza con la direttiva sulle infrastrutture critiche europee, di cui attualmente è in corso una revisione volta a migliorare la protezione e la resilienza delle infrastrutture critiche rispetto alle minacce non informatiche, con possibili implicazioni per il settore finanziario[31].

---

30 Direttiva (UE) 2016/1148 del Parlamento europeo e del Consiglio, del 6 luglio 2016, recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione (GU L 194 del 19.7.2016, pag. 1).

31 Direttiva 2008/114/CE del Consiglio, dell'8 dicembre 2008, relativa all'individuazione e alla designazione delle infrastrutture critiche europee e alla valutazione della necessità di migliorarne la protezione (GU L 345 del 23.12.2008, pag. 75).

(19) I fornitori di servizi di cloud computing sono una delle categorie di fornitori di servizi digitali contemplati dalla direttiva (UE) 2016/1148. In quanto tali, sono soggetti a una vigilanza ex post da parte delle autorità nazionali designate ai sensi di detta direttiva; tale vigilanza si limita alle prescrizioni in materia di notifica degli incidenti e sicurezza delle TIC previste da quello strumento giuridico. Dal momento che il quadro di sorveglianza istituito dal presente regolamento si applica a tutti i fornitori terzi di servizi di TIC critici, compresi i fornitori di servizi di cloud computing quando forniscono servizi di TIC a entità finanziarie, tale quadro dovrebbe essere considerato complementare alla vigilanza svolta ai sensi della direttiva (UE) 2016/1148. Inoltre, in assenza di un quadro orizzontale dell'Unione applicabile indistintamente a tutti i settori e che istituisca un'autorità per la sorveglianza digitale, il quadro di sorveglianza istituito dal presente regolamento dovrebbe estendersi ai fornitori di servizi di cloud computing.

(20) Per mantenere il pieno controllo sui rischi relativi alle TIC le entità finanziarie devono dotarsi di capacità generali che consentano una gestione dei rischi relativi alle TIC forte ed efficace, accanto a strategie e meccanismi specifici per la segnalazione degli incidenti connessi alle TIC, test su processi, controlli e sistemi di TIC e infine per la gestione dei rischi relativi alle TIC derivanti da terzi. È opportuno rendere più rigorosi gli obblighi in materia di resilienza operativa digitale per il sistema finanziario, consentendo tuttavia un'applicazione proporzionata delle prescrizioni a carico delle entità finanziarie che sono microimprese ai sensi della raccomandazione della Commissione 2003/361/CE[32].

(21) Le soglie e le tassonomie per la segnalazione degli incidenti connessi alle TIC variano sensibilmente a livello nazionale. È possibile trovare un terreno comune grazie al lavoro compiuto in materia dall'Agenzia dell'Unione europea per la cibersicurezza (ENISA)[33] e dal gruppo di cooperazione NIS per le entità finanziarie istituito ai sensi della direttiva (UE) 2016/1148, ma in merito a soglie e tassonomie si registrano ancora o possono emergere divergenze di approcci per le altre entità finanziarie. Ne deriva una molteplicità di prescrizioni che le entità finanziarie devono rispettare, soprattutto quando operano in varie giurisdizioni dell'Unione oppure quando fanno parte di un gruppo finanziario. Tali divergenze possono inoltre ostacolare la creazione di nuovi meccanismi uniformi o centralizzati dell'Unione, volti ad accelerare il processo di segnalazione e a coadiuvare uno scambio di informazioni rapido e regolare tra le autorità competenti: elemento essenziale, quest'ultimo, per affrontare i rischi relativi alle TIC nell'eventualità di attacchi su vasta scala con conseguenze potenzialmente sistemiche.

(22) Per consentire alle autorità competenti di assolvere le proprie funzioni di vigilanza ottenendo un panorama completo di natura, frequenza, rilevanza e impatto degli incidenti connessi alle TIC e per agevolare lo scambio di informazioni tra le autorità pubbliche competenti, comprese le autorità di contrasto e le autorità di risoluzione, è necessario stabilire norme che integrino il regime di segnalazione degli incidenti connessi alle TIC con le prescrizioni attualmente assenti nella legislazione del

---

32 Raccomandazione della Commissione, del 6 maggio 2003, relativa alla definizione delle microimprese, piccole e medie imprese (GU L 124 del 20.5.2003, pag. 36).

33 ENISA Reference Incident Classification Taxonomy, https://www.enisa.europa.eu/publications/reference-incident-classification-taxonomy.

sottosettore finanziario, eliminando altresì le sovrapposizioni e le duplicazioni eventualmente esistenti in modo da diminuire i costi. È pertanto essenziale armonizzare il regime di segnalazione degli incidenti connessi alle TIC chiedendo a tutte le entità finanziarie di riferire soltanto alle rispettive autorità competenti. Alle AEV si dovrebbe poi conferire il potere di precisare ulteriormente gli elementi da inserire nella segnalazione degli incidenti connessi alle TIC come la tassonomia, i limiti temporali, le serie di dati, i modelli e le soglie applicabili.

(23) In alcuni sottosettori finanziari sono state elaborate prescrizioni in materia di test di resilienza operativa digitale in numerosi quadri nazionali privi di coordinamento che affrontavano i medesimi problemi in modo differente. Ne è scaturita una duplicazione di costi per le entità finanziarie transfrontaliere, che rende difficile il reciproco riconoscimento dei risultati. La mancanza di coordinamento tra i sistemi di test può pertanto provocare la segmentazione del mercato unico.

(24) Inoltre, qualora non si richiedano test, non è possibile individuare le vulnerabilità che mettono ulteriormente a repentaglio la stabilità e l'integrità dell'entità finanziaria e, in ultima analisi, quella dell'intero settore. Senza un intervento dell'Unione, i test in materia di resilienza operativa digitale continuerebbero a essere disomogenei e non vi sarebbe alcun riconoscimento reciproco dei relativi risultati fra le diverse giurisdizioni. È inoltre improbabile che altri sottosettori finanziari adottino tali regimi su scala significativa; pertanto essi si lascerebbero sfuggire i potenziali benefici, come l'individuazione di vulnerabilità e rischi, la verifica di capacità di difesa e continuità operativa, nonché l'accresciuta fiducia di consumatori, fornitori e partner commerciali. Per porre rimedio a tali sovrapposizioni, divergenze e carenze è necessario stabilire norme volte a coordinare i test che devono essere svolti da entità finanziarie e autorità competenti, agevolando così il riconoscimento reciproco dei test avanzati per le entità finanziarie più importanti.

(25) La dipendenza delle entità finanziarie dai servizi di TIC è causata in parte dalla loro necessità di adattarsi all'emergere di un'economia mondiale digitale sempre più competitiva, di accrescere la propria efficienza commerciale e di soddisfare la domanda dei consumatori. La natura e la portata di questa dipendenza ha conosciuto negli ultimi anni un'evoluzione costante, che ha prodotto una riduzione dei costi dell'intermediazione finanziaria, ha favorito l'espansione e la scalabilità delle imprese nello sviluppo delle attività finanziarie, offrendo d'altra parte un'ampia gamma di strumenti TIC per la gestione di complessi processi interni.

(26) L'ampio uso dei servizi di TIC è testimoniato dalla complessità degli accordi contrattuali: le entità finanziarie incontrano spesso difficoltà nel negoziare condizioni contrattuali che siano conformi a norme prudenziali o ad altre prescrizioni normative cui sono sottoposte oppure nell'applicare diritti specifici, quali i diritti di accesso o di audit, quando tali diritti siano previsti negli accordi. Inoltre raramente i contratti di questo tipo contengono salvaguardie sufficienti per un monitoraggio esauriente dei processi di subappalto, e privano in tal modo l'entità finanziaria della capacità di valutare tali rischi associati. Ancora, dal momento che i fornitori terzi di servizi di TIC spesso offrono servizi standardizzati a una clientela differenziata, tali contratti non sono sempre idonei a soddisfare le esigenze individuali o specifiche dei soggetti del settore finanziario.

(27) Nonostante talune norme generali in materia di esternalizzazione, contenute in alcuni atti legislativi adottati dall'Unione nel settore dei servizi finanziari, il monitoraggio della dimensione contrattuale non è sempre saldamente radicato nella legislazione

dell'UE. In assenza di norme dell'Unione che si applichino in maniera chiara e mirata alle disposizioni contrattuali stipulate con fornitori terzi di servizi di TIC, la fonte esterna dei rischi relativi alle TIC rimane una questione non adeguatamente affrontata. È pertanto necessario fissare alcuni principi fondamentali che indirizzino la gestione, da parte delle entità finanziarie, dei rischi relativi alle TIC derivanti da terzi, accompagnandola con una serie di diritti contrattuali di base concernenti vari elementi dell'esecuzione e dell'estinzione dei contratti; ciò allo scopo di sancire alcune garanzie minime su cui possa fondarsi la capacità delle entità finanziarie di monitorare efficacemente tutti i rischi che si profilino a livello di servizi di TIC forniti da terzi.

(28) Per quanto riguarda le dipendenze da terzi nel settore delle TIC e i rischi relativi alle TIC derivanti da terzi si registra una carenza di omogeneità e convergenza. Nonostante gli sforzi per intervenire nel settore specifico dell'esternalizzazione, come le raccomandazioni del 2017 in materia di esternalizzazione a fornitori di servizi cloud[34], la questione del rischio sistemico potenzialmente derivante dall'esposizione del settore finanziario a un ristretto numero di fornitori terzi di servizi di TIC critici è quasi ignorata nella legislazione dell'Unione. Tale carenza a livello dell'UE è aggravata dall'assenza di strumenti e mandati specifici che consentano alle autorità nazionali di vigilanza di acquisire una valida comprensione delle dipendenze da terzi nel settore delle TIC e di monitorare adeguatamente i rischi provocati dalla concentrazione di tali dipendenze.

(29) Tenendo presenti i potenziali rischi sistemici derivanti dalla diffusione delle pratiche di esternalizzazione e dalla concentrazione dei servizi di TIC forniti da terzi, e alla luce dell'inadeguatezza dei meccanismi nazionali che consentono agli organismi finanziari superiori di quantificare, qualificare e rettificare le conseguenze dei rischi relativi alle TIC che interessano i fornitori terzi di servizi di TIC critici, è necessario stabilire un adeguato quadro di sorveglianza dell'Unione che preveda il monitoraggio costante delle attività di quei fornitori terzi di servizi di TIC che sono fornitori critici per le entità finanziarie.

(30) Di fronte a minacce alle TIC che si fanno sempre più complesse e sofisticate, la validità delle misure di individuazione e prevenzione dipende in larga misura da una costante condivisione di dati sulle minacce e sulle vulnerabilità tra le entità finanziarie. La condivisione delle informazioni contribuisce a una maggiore consapevolezza delle minacce informatiche; ciò a sua volta accresce la capacità delle entità finanziarie di impedire che le minacce si trasformino in incidenti concreti e consente alle entità finanziarie di arginare in maniera più efficace gli effetti degli incidenti connessi alle TIC e di effettuare un ripristino più efficiente. In assenza di orientamenti a livello di Unione, numerosi fattori, tra cui in particolare l'incertezza sulla compatibilità con le norme in materia di protezione dei dati, antitrust e responsabilità, hanno apparentemente ostacolato la condivisione dei dati.

(31) Inoltre i dubbi sul tipo di informazioni che è possibile condividere con altri partecipanti al mercato, o con autorità diverse da quelle di vigilanza (come l'ENISA per i contributi analitici o l'Europol per le attività di contrasto), possono determinare la mancata comunicazione di informazioni preziose. Le informazioni condivise rimangono limitate e frammentate in termini quantitativi e qualitativi: gli scambi pertinenti avvengono per lo più a livello locale (tramite iniziative nazionali) e non

[34] Raccomandazioni in materia di esternalizzazione a fornitori di servizi cloud (EBA/REC/2017/03), ora abrogate dagli Orientamenti in materia di esternalizzazione dell'ABE (EBA/GL/2019/02).

esistono meccanismi di condivisione delle informazioni estesi in maniera omogenea a tutta l'Unione e corrispondenti alle esigenze di un settore finanziario integrato.

(32) È quindi opportuno incoraggiare le entità finanziarie a sfruttare collettivamente, sul piano strategico, tattico e operativo, le conoscenze e le esperienze pratiche che hanno acquisito a livello individuale al fine di accrescere le proprie capacità di valutare e monitorare adeguatamente le minacce informatiche, difendersi dai loro effetti e rispondervi. È perciò necessario promuovere il diffondersi a livello europeo di meccanismi volontari di condivisione delle informazioni i quali, se attuati in ambienti sicuri, aiuterebbero la comunità finanziaria a prevenire le minacce e a rispondervi collettivamente, contenendo rapidamente la diffusione dei rischi relativi alle TIC e prevenendo il potenziale contagio tramite i canali finanziari. Tali meccanismi dovrebbero essere completamente conformi alle norme del diritto dell'Unione vigenti in materia di concorrenza[35] e operare nel pieno rispetto delle norme dell'UE sulla protezione dei dati, in particolare il regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio[36], soprattutto nel contesto del trattamento dei dati personali necessario per il perseguimento del legittimo interesse del titolare del trattamento o di terzi, ai sensi dell'articolo 6, paragrafo 1, lettera f), dello stesso regolamento.

(33) Nonostante l'ampia portata prevista dal presente regolamento, l'applicazione delle norme in materia di resilienza operativa digitale dovrebbe tener conto delle differenze significative che si registrano tra le entità finanziarie in termini di dimensioni, profilo commerciale o esposizione al rischio digitale. Come principio generale, al momento di destinare risorse e capacità all'attuazione del quadro per la gestione dei rischi relativi alle TIC, le entità finanziarie dovrebbero trovare il giusto equilibrio tra le proprie esigenze nel campo delle TIC, da un lato, e le dimensioni e il profilo commerciale, dall'altro; le autorità competenti dovrebbero invece valutare e riesaminare costantemente l'approccio che guida tale distribuzione.

(34) Poiché le entità finanziarie più grandi possono disporre di maggiori risorse e possono destinare rapidamente fondi allo sviluppo di strutture di governance, elaborando varie strategie aziendali, è opportuno imporre l'introduzione di meccanismi di governance più complessi solo alle entità finanziarie che non sono microimprese ai sensi del presente regolamento. Tali entità sono meglio attrezzate, in particolare per istituire funzioni gestionali dedicate alla vigilanza sugli accordi con i fornitori terzi di servizi di TIC o per affrontare la gestione delle crisi, per organizzare la gestione dei rischi secondo il modello delle tre linee di difesa o ancora per adottare un documento a livello di risorse umane che esponga in maniera esaustiva le politiche sui diritti di accesso.

Secondo la stessa logica, soltanto queste entità finanziarie dovrebbero essere tenute a svolgere valutazioni approfondite dopo modifiche di rilievo delle infrastrutture e dei processi delle reti e dei sistemi informativi, a compiere periodicamente analisi dei rischi sui sistemi di TIC esistenti o ad ampliare i testi sulla continuità operativa e i

---

35 Comunicazione della Commissione, Linee direttrici sull'applicabilità dell'articolo 101 del trattato sul funzionamento dell'Unione europea agli accordi di cooperazione orizzontale (GU C 11 del 14.1.2011, pag. 1).

36 Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati) (GU L 119 del 4.5.2016, pag. 1).

piani di risposta e ripristino per descrivere gli scenari di passaggio tra le infrastrutture TIC primarie e le attrezzature ridondanti.

(35) Inoltre, dal momento che solo le entità finanziarie identificate come significative ai fini dei test avanzati di resilienza digitale dovrebbero essere tenute a svolgere test di penetrazione basati su minacce, i processi amministrativi e i costi finanziari derivanti dallo svolgimento di tali test dovrebbero riguardare soltanto una esigua percentuale delle entità finanziarie. Infine, allo scopo di alleviare gli oneri di regolamentazione, soltanto alle entità finanziarie diverse dalle microimprese si dovrebbe chiedere di comunicare regolarmente alle autorità competenti tutti i costi e le perdite provocati dalle perturbazioni delle TIC, nonché i risultati degli esami effettuati dopo l'incidente in occasione di gravi perturbazioni a livello di TIC.

(36) Per garantire il pieno allineamento e la coerenza complessiva tra le strategie commerciali delle entità finanziarie, da un lato, e la gestione dei rischi relativi alle TIC, dall'altro, è opportuno richiedere all'organo di gestione di mantenere un ruolo attivo e fondamentale nella guida e nell'adeguamento del quadro di gestione dei rischi relativi alle TIC e della strategia globale di resilienza digitale. L'organo di gestione dovrebbe adottare un approccio che non consideri solamente i mezzi per assicurare la resilienza dei sistemi di TIC, ma si estenda anche alle persone e ai processi mediante un ventaglio di strategie che promuovano, a ciascun livello dell'azienda e per tutto il personale, un forte senso di consapevolezza dei rischi informatici nonché l'impegno a rispettare a tutti i livelli una rigorosa igiene informatica.

La responsabilità principale dell'organo di gestione nell'affrontare i rischi relativi alle TIC di un'entità finanziaria dovrebbe concretizzarsi nel principio guida di tale approccio complessivo, tradotto ulteriormente nel costante impegno dell'organo di gestione a controllare il monitoraggio della gestione dei rischi relativi alle TIC.

(37) Inoltre la piena responsabilità dell'organo di gestione si accompagna alla definizione di un livello di investimenti in TIC e di un bilancio complessivo dell'entità finanziaria tali da conseguire una resilienza operativa digitale di base.

(38) Sulla scia di norme, linee guida, raccomandazioni o approcci alla gestione dei rischi informatici fissati a livello internazionale, nazionale e settoriale[37], il presente regolamento promuove una serie di funzioni che favoriscono una strutturazione complessiva della gestione dei rischi relativi alle TIC. Nella misura in cui le principali capacità introdotte dalle entità finanziarie soddisfano le esigenze degli obiettivi previsti dalle funzioni (identificazione, protezione e prevenzione, individuazione, risposta e ripristino, apprendimento, evoluzione e comunicazione) indicate nel presente regolamento le entità finanziarie conservano la libertà di impiegare modelli di gestione dei rischi relativi alle TIC strutturati o categorizzati in maniera diversa.

(39) Per tenere il passo con l'evoluzione del contesto delle minacce informatiche, le entità finanziarie dovrebbero dotarsi di sistemi di TIC aggiornati, affidabili e provvisti di capacità sufficienti non solo per garantire il trattamento dei dati necessario per la prestazione dei loro servizi, ma anche per assicurare una resilienza tecnologica che

[37] CPMI-IOSCO, *Guidance on cyber resilience for financial market infrastructures*, https://www.bis.org/cpmi/publ/d146.pdf; G7 *Fundamental Elements of Cybersecurity for the Financial Sector*, https://www.ecb.europa.eu/paym/pol/shared/pdf/G7_Fundamental_Elements_Oct_2016.pdf; NIST Cybersecurity Framework, https://www.nist.gov/cyberframework; FSB *CIRR toolkit*, https://www.fsb.org/2020/04/effective-practices-for-cyber-incident-response-and-recovery-consultative-document.

consenta alle entità finanziarie di fare adeguatamente fronte alle esigenze di trattamento supplementari che possono derivare da condizioni di stress del mercato o da altre situazioni avverse. Il presente regolamento non comporta una standardizzazione di specifici strumenti, tecnologie o sistemi di TIC, ma si affida a un utilizzo idoneo, da parte delle entità finanziarie, di norme tecniche riconosciute a livello europeo e internazionale (ad esempio ISO) o delle migliori pratiche del settore, nella misura in cui tale utilizzo sia pienamente conforme alle specifiche istruzioni delle autorità di vigilanza sull'utilizzo e l'integrazione delle norme internazionali.

(40) È necessario adottare piani efficienti di continuità operativa e di ripristino che consentano alle entità finanziarie di risolvere tempestivamente e rapidamente gli incidenti connessi alle TIC, e in particolare gli attacchi informatici, limitando i danni e privilegiando la ripresa delle attività e le azioni di ripristino. I sistemi di backup dovrebbero iniziare il trattamento senza indebiti ritardi, ma l'inizio di quest'attività non dovrebbe in alcun modo mettere a repentaglio l'integrità e la sicurezza della rete e dei sistemi informativi, né la riservatezza dei dati.

(41) Il presente regolamento permette alle entità finanziarie di fissare il tempo massimo di ripristino in maniera flessibile, tenendo conto della natura e della criticità della funzione pertinente nonché di eventuali esigenze commerciali specifiche, ma per fissare tali obiettivi si dovrebbe imporre una valutazione del potenziale impatto sull'efficienza del mercato.

(42) Le conseguenze più significative degli attacchi informatici si amplificano quando hanno luogo nel settore finanziario, che corre in misura assai maggiore il rischio di diventare l'obiettivo di propagatori malintenzionati che perseguono guadagni finanziari direttamente alla fonte. Per attenuare tali rischi e scongiurare il pericolo che i sistemi di TIC perdano l'integrità o divengano indisponibili, nonché per evitare la violazione di dati riservati e prevenire danni alle infrastrutture fisiche delle TIC, è opportuno migliorare sensibilmente la segnalazione, da parte delle entità finanziarie, degli incidenti gravi connessi alle TIC.

È opportuno anche armonizzare la segnalazione degli incidenti connessi alle TIC chiedendo a tutte le entità finanziarie di riferire soltanto alle rispettive autorità competenti. Tutte le entità finanziarie sarebbero tenute a effettuare tali segnalazioni, ma non tutte dovrebbero esserne interessate allo stesso modo, giacché si dovrebbe procedere a una calibrazione delle soglie di rilevanza e dei limiti temporali al fine di cogliere unicamente gli incidenti gravi connessi alle TIC. Una segnalazione diretta consentirebbe alle autorità di vigilanza finanziaria di accedere alle informazioni relative agli incidenti connessi alle TIC. Le autorità di vigilanza finanziaria dovrebbero tuttavia trasmettere tali informazioni alle pubbliche autorità non finanziarie (le competenti autorità NIS, le autorità nazionali per la protezione dei dati e le autorità di contrasto per gli incidenti di natura penale). Le informazioni sugli incidenti connessi alle TIC dovrebbero essere oggetto di comunicazione reciproca: le autorità di vigilanza finanziaria dovrebbero fornire all'entità finanziaria tutti i riscontri o gli orientamenti necessari, mentre le AEV dovrebbero condividere, in forma anonima, i dati sulle minacce e le vulnerabilità concernenti un determinato evento per promuovere una più ampia difesa collettiva.

(43) È opportuno riflettere ulteriormente sulla possibile centralizzazione delle segnalazioni di incidenti connessi alle TIC, con l'istituzione di un unico polo centrale dell'UE che riceva direttamente le segnalazioni pertinenti e le notifichi automaticamente alle competenti autorità nazionali o che si limiti a centralizzare le segnalazioni trasmesse

dalle competenti autorità nazionali e assolva una funzione di coordinamento. Le AEV dovrebbero essere tenute a preparare entro una certa data, in collaborazione con la BCE e l'ENISA, una relazione comune che esamini la praticabilità dell'istituzione di questo polo centrale dell'UE.

(44) Per conseguire una solida resilienza operativa digitale, e in linea con le norme internazionali (ad esempio gli elementi fondamentali del G7 per i test di penetrazione basati su minacce), le entità finanziarie dovrebbero sottoporre periodicamente a test il personale e i sistemi di TIC per valutarne l'efficacia delle capacità di prevenzione, individuazione, risposta e ripristino, allo scopo di scoprire e affrontare le potenziali vulnerabilità in materia di TIC. Per far fronte alle differenze che si riscontrano tra i vari sottosettori finanziari e all'interno di ognuno di essi relativamente alla preparazione delle entità finanziarie in materia di cibersicurezza, i test dovrebbero comprendere un'ampia varietà di strumenti e azioni, da una valutazione dei requisiti di base (ad esempio individuazione e valutazione delle vulnerabilità, analisi open source, valutazioni della sicurezza delle reti, analisi delle carenze, esami della sicurezza fisica, questionari e soluzioni di software di scansione, esami del codice sorgente, ove possibile, test basati su scenari, test di compatibilità, test di prestazione o test end-to-end) fino a test più avanzati (ad esempio i test di penetrazione basati su minacce per quelle entità finanziarie che, dal punto di vista delle TIC, hanno raggiunto la maturità sufficiente per svolgere tali test). I test di resilienza operativa digitale dovrebbero essere pertanto più rigorosi per le entità finanziarie più importanti (come i grandi enti creditizi, le borse valori, i depositari centrali di titoli, le controparti centrali, ecc.). Allo stesso tempo i test di resilienza operativa digitale dovrebbero essere più rilevanti per alcuni sottosettori che assolvono una funzione sistemica fondamentale (ad esempio pagamenti, attività bancaria, compensazione e regolamento) e meno rilevanti per altri sottosettori (ad esempio gestori di patrimoni, agenzie di rating del credito, ecc.). Le entità finanziarie transfrontaliere che esercitano la libertà di stabilimento o la libera prestazione di servizi all'interno dell'Unione europea dovrebbero rispettare le prescrizioni di un'unica serie di test avanzati (ad esempio i test di penetrazione basati su minacce) nel proprio Stato membro di origine; tali test dovrebbero comprendere le infrastrutture delle TIC di tutte le giurisdizioni in cui il gruppo transfrontaliero opera all'interno dell'Unione, permettendo così ai gruppi transfrontalieri di sostenere i costi dei test in un'unica giurisdizione.

(45) Per un solido monitoraggio dei rischi relativi alle TIC derivanti da terzi, è necessario fissare una serie di norme basate su principi che guidino il monitoraggio, da parte delle entità finanziarie, dei rischi che si presentano nel contesto di funzioni esternalizzate a fornitori terzi di servizi di TIC e, più in generale, nel contesto delle dipendenze da terzi nel settore delle TIC.

(46) Un'entità finanziaria dovrebbe rimanere sempre responsabile del rispetto degli obblighi previsti dal presente regolamento. È opportuno organizzare un monitoraggio proporzionato del rischio emergente a livello di fornitori terzi di servizi di TIC, tenendo debitamente conto dell'entità, della complessità e della rilevanza delle dipendenze relative alle TIC, della criticità o dell'importanza dei servizi, dei processi o delle funzioni oggetto degli accordi contrattuali e, in ultima analisi, sulla base di un'attenta valutazione di eventuali impatti sulla continuità e la qualità dei servizi finanziari a livello individuale e di gruppo, a seconda dei casi.

(47) Lo svolgimento di tale monitoraggio dovrebbe seguire un approccio strategico ai rischi relativi alle TIC derivanti da terzi, formalizzato con l'adozione, da parte dell'organo di gestione dell'entità finanziaria, di una strategia dedicata fondata sul costante esame di

tutte le dipendenze da terzi nel settore delle TIC. Affinché le autorità di vigilanza abbiano una visione più completa delle dipendenze da terzi nel settore delle TIC, e allo scopo di offrire ulteriore sostegno al quadro di sorveglianza istituito dal presente regolamento, le autorità di vigilanza finanziaria dovrebbero ricevere periodicamente informazioni essenziali tratte dai registri e dovrebbero avere la possibilità di richiedere estratti ad hoc di questo materiale.

(48) Una meticolosa analisi precontrattuale dovrebbe precedere la conclusione formale degli accordi contrattuali e costituirne la base, mentre l'estinzione dei contratti dovrebbe giustificarsi almeno sulla base di una serie di circostanze che attestino carenze addebitabili al fornitore terzo di servizi di TIC.

(49) Per far fronte all'impatto sistemico del rischio di concentrazione di servizi die TIC forniti da terzi è opportuno promuovere una soluzione equilibrata fondata su un approccio flessibile e graduale, in quanto massimali rigidi o restrizioni rigorose potrebbero intralciare l'attività economica e la libertà contrattuale. Le entità finanziarie dovrebbero valutare meticolosamente le disposizioni contrattuali per verificare la probabilità che tali rischi si presentino, anche mediante analisi approfondite degli accordi di subesternalizzazione, soprattutto quando siano conclusi con fornitori terzi di servizi die TIC stabiliti in un paese terzo. In questa fase, e allo scopo di trovare il giusto equilibrio tra l'imperativo di preservare la libertà contrattuale e quello di garantire la stabilità finanziaria, non si considera opportuno introdurre massimali e limiti rigorosi alle esposizioni verso terzi nel settore delle TIC. Nell'esercizio dei suoi compiti l'AEV designata a effettuare la sorveglianza su ciascun fornitore terzo di servizi di TIC critico ("l'autorità di sorveglianza capofila") dovrebbe accertare con particolare cura di aver compreso a fondo le dimensioni delle interdipendenze e di aver scoperto i casi specifici in cui un elevato grado di concentrazione di fornitori terzi di servizi di TIC critici potrebbe compromettere l'integrità e la stabilità del sistema finanziario dell'Unione, instaurando un dialogo con i fornitori terzi di servizi di TIC critici laddove tale rischio sia identificato[38].

(50) Per riuscire a valutare e a monitorare costantemente la capacità del fornitore terzo di servizi di TIC di erogare in sicurezza i servizi all'entità finanziaria senza effetti avversi sulla resilienza di quest'ultima, è opportuno armonizzare i principali elementi contrattuali per l'intera esecuzione dei contratti con i fornitori terzi di servizi di TIC. Tali elementi coprono solo gli aspetti contrattuali minimi, considerati cruciali per consentire il monitoraggio completo da parte dell'entità finanziaria, nella prospettiva di garantirne la resilienza digitale che si fonda sulla stabilità e la sicurezza del servizio di TIC.

(51) In particolare gli accordi contrattuali dovrebbero contenere le descrizioni complete di funzioni e servizi, l'indicazione delle località in cui si esercitano tali funzioni e ha luogo il trattamento dei dati nonché le descrizioni complete dei livelli di servizio accompagnate da obiettivi di prestazione quantitativi e qualitativi nell'ambito di livelli di servizio concordati, in modo da consentire un monitoraggio efficace da parte dell'entità finanziaria. In una prospettiva analoga, anche le disposizioni in materia di accessibilità, disponibilità, integrità, sicurezza e protezione dei dati personali, nonché

[38] Qualora inoltre si profili il rischio di abusi da parte di un fornitore terzo di servizi di TIC considerato dominante, le entità finanziarie dovrebbero avere la possibilità di presentare una denuncia formale o informale alla Commissione europea o alle autorità nazionali competenti in materia di diritto della concorrenza.

le garanzie di accesso, ripristino e restituzione in caso di insolvenza, risoluzione o cessazione delle operazioni commerciali del fornitore terzo di servizi di TIC, dovrebbero essere considerate elementi essenziali della capacità di un'entità finanziaria di monitorare il rischio derivante da terzi.

(52) Per garantire che le entità finanziarie mantengano il pieno controllo di tutti gli sviluppi che potrebbero comprometterne la sicurezza in materia di TIC, è opportuno definire termini di preavviso e obblighi di comunicazione per il fornitore terzo di servizi di TIC nel caso di sviluppi che possano incidere seriamente sulla capacità di tale fornitore di esercitare efficacemente funzioni critiche o importanti, tra cui la fornitura di assistenza in caso di incidente connesso alle TIC, senza costi supplementari o a un costo stabilito ex ante.

(53) I diritti di accesso, ispezione e audit da parte dell'entità finanziaria o di un terzo designato a tale scopo sono strumenti essenziali per il monitoraggio costante, da parte delle entità finanziarie, delle prestazioni del fornitore terzo di servizi di TIC, insieme alla piena collaborazione di quest'ultimo nel corso delle ispezioni. Allo stesso modo, l'autorità competente dell'entità finanziaria dovrebbe poter godere del diritto, sulla base di preavvisi, di ispezionare e sottoporre ad audit il fornitore terzo di servizi di TIC, fatta salva la riservatezza.

(54) Gli accordi contrattuali dovrebbero prevedere chiari diritti di estinzione, insieme ai relativi termini di preavviso, nonché strategie di uscita dedicate che indichino in particolare periodi di transizione obbligatori durante i quali i fornitori terzi di servizi di TIC dovrebbero continuare a esercitare le pertinenti funzioni, allo scopo di ridurre il rischio di perturbazioni a livello dell'entità finanziaria o di consentire a quest'ultima di passare senza inconvenienti ad altri fornitori terzi di servizi di TIC o, in alternativa, di ricorrere a soluzioni interne, in funzione della complessità del servizio fornito.

(55) Inoltre l'utilizzo volontario di clausole contrattuali standard elaborate dalla Commissione per i servizi di cloud computing può costituire un'ulteriore preziosa risorsa per le entità finanziarie e per i loro fornitori terzi di servizi di TIC, accrescendo il livello di certezza del diritto in merito all'utilizzo di servizi di cloud computing da parte del settore finanziario, in completa conformità con le prescrizioni e le aspettative definite dal regolamento sui servizi finanziari. Questo lavoro si fonda su misure già previste dal piano d'azione per le tecnologie finanziarie del 2018, in cui la Commissione annunciava l'intenzione di incoraggiare e agevolare lo sviluppo di clausole contrattuali tipo per l'esternalizzazione di servizi di cloud computing da parte delle entità finanziarie, basandosi sulle iniziative intersettoriali già intraprese dai portatori di interessi del settore dei servizi di cloud computing che la Commissione ha favorito grazie al coinvolgimento del settore finanziario.

(56) Per promuovere la convergenza e l'efficienza negli approcci di vigilanza ai rischi relativi alle TIC derivanti da terzi nel settore finanziario, rafforzare la resilienza operativa digitale delle entità finanziarie che dipendono da fornitori terzi di servizi di TIC critici per l'esercizio di funzioni operative e contribuire così a preservare la stabilità del sistema finanziario dell'Unione e l'integrità del mercato unico per i servizi finanziari, è opportuno assoggettare i fornitori terzi di servizi di TIC critici a un quadro di sorveglianza dell'Unione.

(57) Dal momento che soltanto per i fornitori terzi di servizi critici si giustifica un trattamento speciale, è opportuno introdurre un meccanismo di designazione finalizzato all'applicazione del quadro di sorveglianza dell'Unione, in modo da tener conto della dimensione e della natura della dipendenza del settore finanziario da tali

fornitori terzi di servizi di TIC; tale meccanismo dovrebbe tradursi in una serie di criteri quantitativi e qualitativi che fissino i parametri di criticità come base per l'inclusione nella sorveglianza. I fornitori terzi di servizi di TIC critici che non sono designati automaticamente in virtù dell'applicazione dei suddetti criteri dovrebbero avere la possibilità di aderire volontariamente al quadro di sorveglianza, mentre i fornitori terzi di servizi di TIC già soggetti ai quadri di meccanismi di sorveglianza istituiti a livello dell'Eurosistema per coadiuvare i compiti di cui all'articolo 127, paragrafo 2, del trattato sul funzionamento dell'Unione europea dovrebbero esserne di conseguenza esentati.

(58) La prescrizione per cui i fornitori terzi di servizi di TIC che sono stati designati come critici devono essere legalmente costituiti nell'Unione non equivale alla localizzazione dei dati, poiché il presente regolamento non contiene ulteriori prescrizioni che impongano di conservare o trattare i dati nell'Unione.

(59) Tale quadro non dovrebbe pregiudicare la competenza degli Stati membri per lo svolgimento di proprie missioni di sorveglianza nei confronti di fornitori terzi di servizi di TIC che non sono critici ai sensi del presente regolamento ma potrebbero essere considerati importanti a livello nazionale.

(60) Per sfruttare l'attuale architettura istituzionale del settore dei servizi finanziari, articolata su vari livelli, il comitato congiunto delle AEV dovrebbe continuare a garantire il coordinamento intersettoriale complessivo su tutte le questioni concernenti i rischi relativi alle TIC, conformemente ai propri compiti in materia di cibersicurezza, coadiuvato da un nuovo sottocomitato (forum di sorveglianza); tale forum dovrebbe svolgere il lavoro preparatorio sia per le singole decisioni rivolte a fornitori terzi di servizi di TIC critici che per le raccomandazioni collettive relative all'analisi comparativa dei programmi di sorveglianza sui fornitori terzi di servizi di TIC critici, nonché all'identificazione delle migliori pratiche riguardanti il rischio di concentrazione delle TIC.

(61) Per far sì che i fornitori terzi di servizi di TIC che assolvono una funzione critica per il funzionamento del settore finanziario siano soggetti a una sorveglianza equilibrata a livello dell'Unione, è opportuno designare una delle AEV come autorità di sorveglianza capofila per ciascun fornitore terzo di servizi di TIC critico.

(62) Le autorità di sorveglianza capofila dovrebbero detenere i poteri necessari per condurre indagini e ispezioni in loco ed esterne presso i fornitori terzi di servizi di TIC critici, accedere a tutti i locali e le sedi pertinenti e ottenere informazioni complete e aggiornate per acquisire un'immagine realistica del tipo, delle dimensioni e dell'impatto dei rischi relativi alle TIC derivanti da terzi cui sono esposte le entità finanziarie e, in ultima analisi, il sistema finanziario dell'Unione.

Affidare alle AEV la sorveglianza principale è un prerequisito per cogliere e affrontare la dimensione sistemica dei rischi relativi alle TIC nel settore finanziario. L'impatto esercitato nell'Unione dai fornitori terzi di servizi di TIC critici e i problemi di rischio di concentrazione delle TIC che possono derivarne esigono un approccio collettivo a livello dell'UE. L'esercizio di molteplici audit e diritti di accesso da parte di varie autorità competenti separate, con un coordinamento scarso o nullo, non permetterebbe di tracciare un quadro completo dei rischi relativi alle TIC derivanti da terzi, e provocherebbe anzi sovrapposizioni, oneri e complessità inutili per i fornitori terzi di servizi di TIC critici posti di fronte a un così gran numero di richieste.

(63) Le autorità di sorveglianza capofila dovrebbero essere inoltre in grado di presentare raccomandazioni su questioni relative ai rischi relativi alle TIC e ai rimedi idonei, opponendosi eventualmente a determinate disposizioni contrattuali suscettibili in ultima analisi di incidere sulla stabilità dell'entità finanziaria o del sistema finanziario. Nell'ambito della loro funzione relativa alla vigilanza prudenziale delle entità finanziarie, le autorità nazionali competenti dovrebbero tener conto del rispetto delle raccomandazioni sostanziali formulate dalle autorità di vigilanza capofila.

(64) Il quadro di sorveglianza non rimpiazza, né in alcun modo o in alcuna parte si sostituisce alla gestione, da parte delle entità finanziarie, dei rischi derivanti dal ricorso a fornitori terzi di servizi di TIC, compreso l'obbligo di monitorare costantemente gli accordi contrattuali stipulati con fornitori terzi di servizi di TIC critici e non incide neppure sulla piena responsabilità delle entità finanziarie per quanto riguarda il rispetto e l'adempimento di tutte le prescrizioni previste dal presente regolamento e dalla pertinente legislazione sui servizi finanziari. Per evitare duplicazioni e sovrapposizioni, è opportuno che le autorità competenti si astengano dall'adozione individuale di misure per il monitoraggio del rischio derivante da fornitori terzi di servizi di TIC critici. Eventuali misure di questo tipo dovrebbero essere coordinate e concordate preliminarmente nel contesto del quadro di sorveglianza.

(65) Per promuovere la convergenza a livello internazionale sulle migliori pratiche da impiegare per il riesame della gestione del rischio digitale derivante da fornitori terzi di servizi di TIC, è opportuno incoraggiare le AEV a stipulare accordi di cooperazione con le competenti autorità normative e di vigilanza di paesi terzi, per favorire lo sviluppo di migliori pratiche nella gestione dei rischi relativi alle TIC derivanti da terzi.

(66) Per sfruttare utilmente la competenza tecnica degli esperti delle autorità competenti in materia di gestione dei rischi relativi alle TIC e del rischio operativo, le autorità di vigilanza capofila dovrebbero tener conto dell'esperienza acquisita dalle autorità di vigilanza nazionali e istituire gruppi destinati a esaminare i singoli fornitori terzi di servizi di TIC critici, riunendo gruppi multidisciplinari che coadiuvino la preparazione e l'effettiva attuazione delle attività di sorveglianza, comprese le ispezioni in loco dei fornitori terzi di servizi di TIC critici, nonché il necessario seguito da dare a queste attività.

(67) Ai fini dell'applicazione del presente regolamento, le autorità competenti dovrebbero detenere tutti i poteri necessari per vigilare, indagare e imporre sanzioni. In linea di principio le sanzioni amministrative dovrebbero essere pubblicate. Poiché è possibile che entità finanziarie e fornitori terzi di servizi di TIC siano stabiliti in Stati membri diversi e siano soggetti a differenti autorità settoriali competenti, è opportuno garantire una stretta cooperazione tra le autorità competenti, compresa la BCE per quanto riguarda i compiti specifici a essa attribuiti dal regolamento (UE) n. 1024/2013 del Consiglio[39], nonché consultazioni con le AEV tramite il reciproco scambio di informazioni e l'offerta di assistenza nel contesto delle attività di vigilanza.

(68) Per quantificare e qualificare ulteriormente i criteri di designazione riguardanti i fornitori terzi di servizi di TIC critici e per armonizzare le commissioni per le attività di sorveglianza, è opportuno delegare alla Commissione il potere di adottare atti ai

[39] Regolamento (UE) n. 1024/2013 del Consiglio, del 15 ottobre 2013, che attribuisce alla Banca centrale europea compiti specifici in merito alle politiche in materia di vigilanza prudenziale degli enti creditizi (GU L 287 del 29.10.2013, pag. 63).

sensi dell'articolo 290 del trattato sul funzionamento dell'Unione europea per quanto riguarda: l'ulteriore precisazione dell'impatto sistemico che un guasto presso un fornitore terzo di servizi di TIC potrebbe esercitare sulle entità finanziarie servite da questo, il numero di enti a rilevanza sistemica a livello globale (G-SII) o di altri enti a rilevanza sistemica (O-SII) che dipendono dal rispettivo fornitore terzo di servizi di TIC, il numero di fornitori terzi di servizi di TIC attivi su uno specifico mercato, i costi del passaggio a un altro fornitore terzo di servizi di TIC, il numero di Stati membri in cui il pertinente fornitore terzo di servizi di TIC offre i propri servizi e in cui operano le entità finanziarie che utilizzano i servizi di tale fornitore, nonché l'importo delle commissioni per le attività di sorveglianza e le relative modalità di pagamento.

È di particolare importanza che durante i lavori preparatori la Commissione svolga adeguate consultazioni, anche a livello di esperti, e che tali consultazioni siano condotte nel rispetto dei principi stabiliti nell'accordo interistituzionale "Legiferare meglio" del 13 aprile 2016[40]. In particolare, al fine di garantire la partecipazione su un piede di parità alla preparazione degli atti delegati, il Parlamento europeo e il Consiglio ricevono tutti i documenti contemporaneamente agli esperti degli Stati membri, e i loro esperti hanno sistematicamente accesso alle riunioni dei gruppi di esperti della Commissione incaricati della preparazione di tali atti delegati.

(69) Dal momento che il presente regolamento, assieme alla direttiva (UE) 20xx/xx del Parlamento europeo e del Consiglio[41], comporta il consolidamento delle disposizioni per la gestione dei rischi relativi alle TIC presenti in una molteplicità di regolamenti e direttive dell'acquis sui servizi finanziari dell'Unione, tra cui i regolamenti (CE) n. 1060/2009, (UE) n. 648/2012, (UE) n. 600/2014 e (UE) n. 909/2014, per garantire completa coerenza è opportuno modificare tali regolamenti per precisare che le pertinenti disposizioni in materia di rischi relativi alle TIC sono stabilite nel presente regolamento.

Le norme tecniche dovrebbero garantire la coerente armonizzazione delle prescrizioni contenute nel presente regolamento. In quanto organismi con una competenza altamente specializzata, le AEV dovrebbero essere incaricate dell'elaborazione di progetti di norme tecniche di regolamentazione che non comportino scelte politiche e della loro presentazione alla Commissione. È opportuno elaborare norme tecniche di regolamentazione nei settori della gestione, della segnalazione e dei test in materia di rischi relativi alle TIC, nonché le prescrizioni principali di un solido monitoraggio dei rischi relativi alle TIC derivanti da terzi.

(70) È particolarmente importante che la Commissione svolga le opportune consultazioni durante i lavori preparatori, anche a livello di esperti. La Commissione e le AEV dovrebbero fare in modo che tutte le entità finanziarie possano applicare tali norme e prescrizioni in misura proporzionata alla propria natura, scala e complessità, nonché alle proprie attività.

(71) Per rendere più agevolmente comparabili le segnalazioni sugli incidenti gravi connessi alle TIC, nonché per garantire la trasparenza sugli accordi contrattuali per l'utilizzo di servizi di TIC offerti da fornitori terzi, è opportuno conferire alle AEV il mandato di elaborare progetti di norme tecniche di attuazione che introducano modelli, formulari e procedure standardizzati per la segnalazione degli incidenti gravi connessi alle TIC da

[40] GU L 123 del 12.5.2016, pag. 1.

[41] [*Inserire il riferimento completo*]

parte delle entità finanziarie nonché modelli standardizzati per il registro delle informazioni. Nell'elaborazione di tali norme le AEV dovrebbero tener conto delle dimensioni e della complessità delle entità finanziarie nonché della natura e del livello di rischio delle loro attività. Alla Commissione si dovrebbe conferire il potere di adottare tali norme tecniche di attuazione mediante atti di esecuzione a norma dell'articolo 291 TFUE e, rispettivamente, dell'articolo 15 dei regolamenti (UE) n. 1093/2010, (UE) n. 1094/2010 e (UE) n. 1095/2010. Dal momento che obblighi ulteriori sono già stati specificati tramite atti delegati e di esecuzione basati su norme tecniche di regolamentazione e di attuazione contenute rispettivamente nei regolamenti (CE) n. 1060/2009, (UE) n. 648/2012, (UE) n. 600/2014 e (UE) n. 909/2014, è opportuno conferire alle AEV, a livello individuale o collettivo tramite il comitato congiunto, il mandato di presentare alla Commissione norme tecniche di regolamentazione e di attuazione in vista dell'adozione di atti delegati e di esecuzione che riprendano e aggiornino le norme vigenti in materia di rischi relativi alle TIC.

(72) Tale esercizio comporterà la successiva modifica dei vigenti atti delegati e di esecuzione adottati in diversi settori della legislazione sui servizi finanziari. È opportuno modificare l'ambito di applicazione degli articoli concernenti il rischio operativo, in base ai quali in quegli atti era stato conferito il mandato di adottare atti delegati e di esecuzione, allo scopo di riprendere nel presente regolamento tutte le disposizioni in materia di resilienza operativa digitale che oggi fanno parte di quei regolamenti.

(73) Poiché gli obiettivi del presente regolamento, ossia l'acquisizione di un elevato livello di resilienza operativa digitale applicabile a tutte le entità finanziarie, non possono essere conseguiti in misura sufficiente dagli Stati membri, in quanto richiedono l'armonizzazione di una molteplicità di norme differenti che attualmente sono contenute in parte in alcuni atti dell'Unione e in parte nei sistemi giuridici di vari Stati membri, ma possono, a motivo della portata o degli effetti dell'azione in questione, essere conseguiti meglio a livello di Unione, l'Unione europea può adottare misure in virtù del principio di sussidiarietà di cui all'articolo 5 del trattato sull'Unione europea. Il presente regolamento si limita a quanto è necessario per conseguire tale obiettivo in ottemperanza al principio di proporzionalità enunciato nello stesso articolo,

HANNO ADOTTATO IL PRESENTE REGOLAMENTO:

CAPO I

DISPOSIZIONI GENERALI

Articolo 1

Oggetto

1. Il presente regolamento stabilisce i seguenti obblighi uniformi in relazione alla sicurezza delle reti e dei sistemi informativi che sostengono i processi commerciali delle entità finanziarie, allo scopo di conseguire un elevato livello di resilienza operativa digitale:

   (a) obblighi applicabili alle entità finanziarie in materia di:

   – gestione dei rischi delle tecnologie dell'informazione e della comunicazione (TIC);

   – segnalazione alle autorità competenti degli incidenti gravi connessi alle TIC;

– test di resilienza operativa digitale;

– condivisione di dati e di informazioni in relazione alle vulnerabilità e alle minacce informatiche;

– misure relative a una solida gestione, da parte delle entità finanziarie, dei rischi relativi alle TIC derivanti da terzi;

(b) obblighi relativi agli accordi contrattuali stipulati tra fornitori terzi di servizi di TIC ed entità finanziarie;

(c) quadro di sorveglianza per i fornitori terzi di servizi di TIC critici, allorché forniscono i loro servizi a entità finanziarie;

(d) norme sulla cooperazione tra autorità competenti e norme sulla vigilanza e l'applicazione da parte delle autorità competenti in relazione a tutte le questioni trattate dal presente regolamento.

2. Quanto alle entità finanziarie identificate come operatori di servizi essenziali ai sensi delle norme nazionali che recepiscono l'articolo 5 della direttiva (UE) 2016/1148, il presente regolamento è considerato un atto giuridico settoriale dell'Unione ai sensi dell'articolo 1, paragrafo 7, della stessa direttiva.

Articolo 2

Ambito di applicazione soggettivo

1. Il presente regolamento si applica alle seguenti entità:

(a) enti creditizi;

(b) istituti di pagamento;

(c) istituti di moneta elettronica;

(d) imprese di investimento;

(e) fornitori di servizi per le cripto-attività, emittenti di cripto-attività, emittenti di token collegati ad attività ed emittenti di token collegati ad attività significativi;

(f) depositari centrali di titoli;

(g) controparti centrali;

(h) sedi di negoziazione;

(i) repertori di dati sulle negoziazioni;

(j) gestori di fondi di investimento alternativi;

(k) società di gestione;

(l) fornitori di servizi di comunicazione dati;

(m) imprese di assicurazione e di riassicurazione;

(n) intermediari assicurativi, intermediari riassicurativi e intermediari assicurativi a titolo accessorio;

(o) enti pensionistici aziendali o professionali;

(p) agenzie di rating del credito;

(q) revisori legali e imprese di revisione:

(r) amministratori degli indici di riferimento critici;

(s) fornitori di servizi di crowdfunding;

(t) repertori di dati sulle cartolarizzazioni;

(u) fornitori terzi di servizi di TIC.

2. Ai fini del presente regolamento le entità di cui alle lettere da a) a t) sono definite collettivamente "entità finanziarie".

Articolo 3

Definizioni

Ai fini del presente regolamento si applicano le definizioni seguenti:

(1) "resilienza operativa digitale": la capacità dell'entità finanziaria di creare, assicurare e riesaminare la propria integrità operativa da un punto di vista tecnologico, garantendo, direttamente o indirettamente, tramite il ricorso ai servizi offerti da fornitori terzi di TIC, l'intera gamma delle capacità connesse alle TIC necessarie per garantire la sicurezza delle reti e dei sistemi informativi impiegati dall'entità finanziaria, su cui si fondano la costante offerta dei servizi finanziari e la loro qualità;

(2) "rete e sistema informativo": una rete e un sistema informativo quali definiti all'articolo 4, punto 1, della direttiva (UE) 2016/1148;

(3) "sicurezza della rete e dei sistemi informativi": la sicurezza della rete e dei sistemi informativi quale definita all'articolo 4, punto 2, della direttiva (UE) 2016/1148;

(4) "rischi relativi alle TIC": qualunque circostanza ragionevolmente identificabile in relazione all'uso della rete e dei sistemi informativi, compresi un malfunzionamento, un superamento di capacità, un guasto, una perturbazione, un deterioramento, un uso improprio, una perdita o altri tipi di eventi dolosi o non dolosi, che, qualora si concretizzi, potrebbe compromettere la sicurezza della rete e dei sistemi informativi, di eventuali strumenti o processi dipendenti dalle tecnologie, della continuazione delle operazioni e dei processi, oppure della fornitura dei servizi, pregiudicando in tal modo l'integrità o la disponibilità dei dati, del software o di eventuali altre componenti dei servizi e delle infrastrutture di TIC, o ancora causando una violazione della riservatezza, un danno alle infrastrutture fisiche di TIC o altri effetti avversi;

(5) "patrimonio di informazioni": una raccolta di informazioni, tangibili o intangibili, che è importante proteggere;

(6) "incidente connesso alle TIC": un evento imprevisto identificato, verificatosi nella rete e nei sistemi informativi e derivante o meno da attività dolose, che compromette la sicurezza della rete e dei sistemi informativi, delle informazioni da essi trattate, conservate o trasmesse, o che ha effetti avversi sulla disponibilità, la riservatezza, la continuità o l'autenticità dei servizi finanziari forniti dall'entità finanziaria;

(7) "incidente grave connesso alle TIC": un incidente connesso alle TIC con un impatto avverso potenzialmente elevato sulla rete e sui sistemi informativi che sostengono funzioni critiche dell'entità finanziaria;

(8) "minaccia informatica": minaccia informatica quale definita all'articolo 2, punto 8, del regolamento (UE) 2019/881 del Parlamento europeo e del Consiglio[42];

(9) "attacco informatico": un incidente doloso connesso alle TIC provocato dal tentativo, da parte dell'autore della minaccia, di distruggere, rivelare, alterare, disabilitare, rubare o utilizzare senza autorizzazione un'attività o ancora accedervi senza autorizzazione;

(10) "dati sulle minacce": informazioni aggregate, trasformate, analizzate, interpretate o arricchite per offrire il contesto necessario al processo decisionale, che recano conoscenze pertinenti e sufficienti per attenuare l'impatto di un incidente connesso alle TIC o di una minaccia informatica, compresi i dettagli tecnici dell'attacco informatico, i responsabili dell'attacco, il loro modus operandi e le loro motivazioni;

(11) "difesa in profondità": una strategia connessa alle TIC che integra persone, processi e tecnologie per erigere una serie di barriere tra vari strati e dimensioni dell'entità;

(12) "vulnerabilità": debolezza, predisposizione o difetto di un'attività, un sistema, un processo o un controllo, di cui una minaccia può approfittare;

(13) "test di penetrazione basato su minacce": un quadro che imita le tattiche, le tecniche e le procedure messe in atto nella vita reale dagli autori delle minacce e percepite come minaccia informatica autentica, che consente di eseguire un test controllato, mirato e fondato su dati (red team) dei reali sistemi di produzione critici dell'entità;

(14) "rischi relativi alle TIC derivanti da terzi": rischi relativi alle TIC cui un'entità finanziaria può essere esposta in relazione al ricorso, da parte di questa, a servizi di TIC offerti da fornitori terzi o da subappaltatori di tali fornitori;

(15) "fornitore terzo di servizi di TIC": un'impresa che fornisce servizi digitali e di dati, compresi i fornitori di servizi di cloud computing, software, servizi di analisi dei dati e centri di dati, ma esclusi i fornitori di componenti hardware e le imprese autorizzate ai sensi del diritto dell'Unione che forniscono servizi di comunicazione elettronica, quali definiti all'articolo 2, punto 4, della direttiva (UE) 2018/1972 del Parlamento europeo e del Consiglio[43];

(16) "servizi di TIC": servizi digitali e di dati forniti attraverso sistemi di TIC a uno o più utenti interni o esterni, compresa la fornitura di dati, l'inserimento di dati, la conservazione di dati, i servizi di trattamento e comunicazione di dati, il monitoraggio dei dati nonché servizi commerciali e di sostegno alle decisioni basati su dati;

(17) "funzione critica o importante": una funzione la cui esecuzione se interrotta, carente o insufficiente comprometterebbe sostanzialmente il costante adempimento, da parte dell'entità finanziaria, delle condizioni e degli obblighi inerenti alla sua autorizzazione o di altri obblighi previsti dalla legislazione sui servizi finanziari applicabile, oppure i suoi risultati finanziari o ancora la solidità o la continuità dei suoi servizi e delle sue attività;

---

42 Regolamento (UE) 2019/881 del Parlamento europeo e del Consiglio, del 17 aprile 2019, relativo all'ENISA, l'Agenzia dell'Unione europea per la cibersicurezza, e alla certificazione della cibersicurezza per le tecnologie dell'informazione e della comunicazione, e che abroga il regolamento (UE) n. 526/2013 ("regolamento sulla cibersicurezza") (GU L 151 del 7.6.2019, pag. 15).

43 Direttiva (UE) 2018/1972 del Parlamento europeo e del Consiglio, dell'11 dicembre 2018, che istituisce il codice europeo delle comunicazioni elettroniche (rifusione) (GU L 321 del 17.12.2018, pag. 36).

(18) "fornitore terzo di servizi di TIC critico": un fornitore terzo di servizi di TIC designato in conformità dell'articolo 29 e soggetto al quadro di sorveglianza di cui agli articoli da 30 a 37;

(19) "fornitore terzo di servizi di TIC stabilito in un paese terzo": un fornitore terzo di servizi di TIC che è una persona giuridica stabilita in un paese terzo, non ha avviato attività economiche/non è presente nell'Unione e ha stipulato un accordo contrattuale con un'entità finanziaria per la fornitura di servizi di TIC;

(20) "subappaltatore di TIC stabilito in un paese terzo": un subappaltatore di TIC che è una persona giuridica stabilita in un paese terzo, non ha avviato attività economiche/non è presente nell'Unione e ha stipulato un accordo contrattuale con un fornitore terzo di servizi di TIC o con un fornitore terzo di servizi di TIC stabilito in un paese terzo;

(21) "rischio di concentrazione delle TIC": l'esposizione a fornitori terzi di servizi di TIC critici, singoli o molteplici e correlati tra loro, che crea un grado di dipendenza tale da detti fornitori che l'indisponibilità, i guasti o altri tipi di carenze che si verificassero presso di loro potrebbero mettere a repentaglio la capacità di un'entità finanziaria, e in ultima analisi dell'intero sistema finanziario dell'Unione, di assolvere funzioni critiche oppure di assorbire altri tipi di effetti avversi, comprese perdite cospicue;

(22) "organo di gestione": organo di gestione quale definito all'articolo 4, paragrafo 1, punto 36, della direttiva 2014/65/UE, all'articolo 3, paragrafo 1, punto 7, della direttiva 2013/36/UE, all'articolo 2, paragrafo 1, lettera s), della direttiva 2009/65/CE, all'articolo 2, paragrafo 1, punto 45, del regolamento (UE) n. 909/2014, all'articolo 3, paragrafo 1, punto 20, del regolamento (UE) 2016/1011 del Parlamento europeo e del Consiglio[44], all'articolo 3, paragrafo 1, lettera u), del regolamento (UE) 20xx/xx del Parlamento europeo e del Consiglio[45] [MICA] oppure le persone equivalenti che gestiscono di fatto l'entità o che assolvono funzioni chiave conformemente alla pertinente legislazione nazionale o dell'Unione;

(23) "ente creditizio": un ente creditizio quale definito all'articolo 4, paragrafo 1, punto 1, del regolamento (UE) n. 575/2013 del Parlamento europeo e del Consiglio[46];

(24) "impresa di investimento": un'impresa di investimento quale definita all'articolo 4, paragrafo 1, punto 1, della direttiva 2014/65/UE;

(25) "istituto di pagamento": un istituto di pagamento quale definito all'articolo 1, paragrafo 1, lettera (d), della direttiva (UE) 2015/2366;

(26) "istituto di moneta elettronica": un istituto di moneta elettronica quale definito all'articolo 2, punto 1, della direttiva 2009/110/CE del Parlamento europeo e del Consiglio[47];

---

44 Regolamento (UE) 2016/1011 del Parlamento europeo e del Consiglio, dell'8 giugno 2016, sugli indici usati come indici di riferimento negli strumenti finanziari e nei contratti finanziari o per misurare la performance di fondi di investimento e recante modifica delle direttive 2008/48/CE e 2014/17/UE e del regolamento (UE) n. 596/2014 (GU L 171 del 29.6.2016, pag. 1).

45 [*inserire il titolo completo e i dettagli della GU*]

46 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 (GU L 176 del 27.6.2013, pag. 1).

(27) "controparte centrale": una controparte centrale quale definita all'articolo 2, punto 1, del regolamento (UE) n. 648/2012;

(28) "repertorio di dati sulle negoziazioni": un repertorio di dati sulle negoziazioni quale definito all'articolo 2, punto 2, del regolamento (UE) n. 648/2012;

(29) "depositario centrale di titoli": un depositario centrale di titoli quale definito all'articolo 2, paragrafo 1, punto 1, del regolamento (UE) n. 909/2014;

(30) "sede di negoziazione": una sede di negoziazione quale definita all'articolo 4, paragrafo 1, punto 24, della direttiva 2014/65/UE;

(31) "gestore di fondi di investimento alternativi": un gestore di fondi di investimento alternativi quale definito all'articolo 4, paragrafo 1, lettera b), della direttiva 2011/61/UE;

(32) "società di gestione": una società di gestione quale definita all'articolo 2, paragrafo 1, lettera b), della direttiva 2009/65/CE;

(33) "fornitore di servizi di comunicazione dati": un fornitore di servizi di comunicazione dati quale definito all'articolo 4, paragrafo 1, punto 63, della direttiva 2014/65/UE;

(34) "impresa di assicurazione": un'impresa di assicurazione quale definita all'articolo 13, punto 1, della direttiva 2009/138/CE;

(35) "impresa di riassicurazione": un'impresa di riassicurazione quale definita all'articolo 13, punto 4, della direttiva 2009/138/CE;

(36) "intermediario assicurativo": un intermediario assicurativo quale definito all'articolo 2, punto 3, della direttiva (UE) 2016/97;

(37) "intermediario assicurativo a titolo accessorio": un intermediario assicurativo a titolo accessorio quale definito all'articolo 2, punto 4, della direttiva (UE) 2016/97;

(38) "intermediario riassicurativo": un intermediario riassicurativo quale definito all'articolo 2, punto 5, della direttiva (UE) 2016/97;

(39) "ente pensionistico aziendale e professionale": un ente pensionistico aziendale o professionale quale definito all'articolo 6, punto 1, della direttiva 2016/2341;

(40) "agenzia di rating del credito": un'agenzia di rating del credito quale definita all'articolo 3, paragrafo 1, lettera a), del regolamento (CE) n. 1060/2009;

(41) "revisore legale": un revisore legale quale definito all'articolo 2, punto 2, della direttiva 2006/43/CE;

(42) "impresa di revisione contabile": un'impresa di revisione contabile quale definita all'articolo 2, punto 3, della direttiva 2006/43/CE;

(43) "fornitore di servizi per le cripto-attività": un fornitore di servizi per le cripto-attività quale definito all'articolo 3, paragrafo 1, lettera n), del regolamento (UE) 202x/xx [*PO: inserire il riferimento al regolamento MICA*];

---

[47] Direttiva 2009/110/CE del Parlamento europeo e del Consiglio, del 16 settembre 2009, concernente l'avvio, l'esercizio e la vigilanza prudenziale dell'attività degli istituti di moneta elettronica, che modifica le direttive 2005/60/CE e 2006/48/CE e che abroga la direttiva 2000/46/CE (GU L 267 del 10.10.2009, pag. 7).

(44) "emittente di cripto-attività": un emittente di cripto-attività quale definito all'articolo 3, paragrafo 1, lettera h), del [*GU: inserire il riferimento al regolamento MICA*];

(45) "emittente di token collegati ad attività": un emittente di token collegati ad attività quale definito all'articolo 3, paragrafo 1, lettera i), del [*GU: inserire il riferimento al regolamento MICA*];

(46) "emittente di token collegati ad attività significativi": un emittente di token collegati ad attività significativi quale definito all'articolo 3, paragrafo 1, lettera j), del [*GU: inserire il riferimento al regolamento MICA*];

(47) "amministratore di indici di riferimento critici": un amministratore di indici di riferimento critici quale definito all'articolo x, punto x, del regolamento xx/202x [*GU: inserire il riferimento al regolamento sugli indici di riferimento*];

(48) "fornitore di servizi di crowdfunding": un fornitore di servizi di crowdfunding quale definito all'articolo x, paragrafo x, del regolamento (UE) 202x/xx [*PO: inserire il riferimento al regolamento sul crowdfunding*];

(49) "repertorio di dati sulle cartolarizzazioni": un repertorio di dati sulle cartolarizzazioni quale definito all'articolo 2, punto 23, del regolamento (UE) 2017/2402;

(50) "microimpresa": un'entità finanziaria quale definita all'articolo 2, paragrafo 3, dell'allegato della raccomandazione 2003/361/CE.

CAPO II

GESTIONE DEI RISCHI RELATIVI ALLE TIC

SEZIONE I

Articolo 4

Governance e organizzazione

1. Le entità finanziarie predispongono quadri di gestione e di controllo interni che garantiscono una gestione efficace e prudente di tutti i rischi relativi alle TIC.

2. L'organo di gestione dell'entità finanziaria definisce e approva l'attuazione di tutte le disposizioni concernenti il quadro per la gestione dei rischi relativi alle TIC di cui all'articolo 5, paragrafo 1, vigila su tale attuazione e ne risponde.

   Ai fini del primo comma, l'organo di gestione:

   (a) assume la responsabilità finale per la gestione dei rischi relativi alle TIC dell'entità finanziaria;

   (b) definisce chiaramente ruoli e responsabilità per tutte le funzioni connesse alle TIC;

   (c) determina il livello appropriato di tolleranza per i rischi relativi alle TIC dell'entità finanziaria, ai sensi dell'articolo 5, paragrafo 9, lettera b);

   (d) approva e riesamina periodicamente l'attuazione della politica di continuità operativa delle TIC e del piano di ripristino in caso di disastro relativo alle TIC

dell'entità finanziaria, di cui rispettivamente all'articolo 10, paragrafi 1 e 3, oltre a vigilare su detta attuazione;

(e) approva e riesamina periodicamente i piani di audit in materia di TIC, gli audit e le più importanti modifiche a essi apportate;

(f) assegna e riesamina periodicamente il bilancio adeguato per soddisfare le esigenze di resilienza operativa digitale dell'entità finanziaria rispetto a tutti i tipi di risorse, compresa la formazione sui rischi relativi alle TIC e sulle relative competenze per tutto il personale pertinente;

(g) approva e riesamina periodicamente la politica dell'entità finanziaria relativa alle modalità per l'uso dei servizi di TIC prestati dal fornitore terzo di servizi di TIC;

(h) è debitamente informato in merito agli accordi conclusi con i fornitori terzi di servizi di TIC sull'uso di tali servizi, alle eventuali modifiche importanti e pertinenti previste riguardo ai fornitori terzi di servizi di TIC, nonché al potenziale impatto di tali modiche sulle funzioni critiche o importanti soggette agli accordi in questione, e riceve tra l'altro una sintesi dell'analisi del rischio per valutare l'impatto delle modifiche;

(i) è debitamente informato in merito agli incidenti connessi alle TIC e al loro impatto, nonché in merito alle misure di risposta e ripristino e alle misure correttive.

3. Le entità finanziarie diverse dalle microimprese istituiscono un ruolo per il monitoraggio degli accordi conclusi con i fornitori terzi di servizi di TIC per l'uso di tali servizi, oppure designano un dirigente di rango elevato quale responsabile della sorveglianza sulla relativa esposizione al rischio e sulla documentazione pertinente.

4. I membri dell'organo di gestione seguono periodicamente corsi di formazione specifici per acquisire e mantenere aggiornate conoscenze e competenze adeguate per comprendere e valutare i rischi relativi alle TIC e il loro impatto sulle operazioni dell'entità finanziaria.

SEZIONE II

Articolo 5

Quadro per la gestione dei rischi relativi alle TIC

1. Le entità finanziarie predispongono un quadro per la gestione dei rischi relativi alle TIC solido, esaustivo e adeguatamente documentato, che consenta loro di affrontare i rischi relativi alle TIC in maniera rapida, efficiente ed esaustiva, assicurando un elevato livello di resilienza operativa digitale corrispondente alle esigenze, alle dimensioni e alla complessità delle loro attività commerciali.

2. Il quadro per la gestione dei rischi relativi alle TIC di cui al paragrafo 1 comprende strategie, politiche, procedure, strumenti e protocolli in materia di TIC necessari per proteggere adeguatamente ed efficacemente tutte le pertinenti infrastrutture e componenti fisiche, compresi hardware e server, nonché tutti i locali, i centri di dati e le aree designate come sensibili, così da garantire che tutti questi elementi fisici siano adeguatamente protetti contro i rischi, compresi i danneggiamenti e l'accesso o l'uso non autorizzati.

3. Le entità finanziarie riducono al minimo l'impatto dei rischi relativi alle TIC applicando strategie, politiche, procedure, protocolli e strumenti adeguati definiti nel quadro di gestione per i rischi relativi alle TIC. Se richiesto dalle autorità competenti, forniscono informazioni complete e aggiornate sui rischi relativi alle TIC.

4. Nel quadro per la gestione dei rischi relativi alle TIC di cui al paragrafo 1, le entità finanziarie diverse dalle microimprese attuano un sistema di gestione della sicurezza delle informazioni basato su norme internazionali riconosciute e conforme agli orientamenti in materia di vigilanza e lo riesaminano periodicamente.

5. Le entità finanziarie diverse dalle microimprese garantiscono un'opportuna separazione tra funzioni di gestione delle TIC, funzioni di controllo e funzioni di audit interno, secondo il modello delle tre linee di difesa oppure un modello interno di controllo e gestione del rischio.

6. Il quadro per la gestione dei rischi relativi alle TIC di cui al paragrafo 1 è documentato e riesaminato almeno una volta all'anno, nonché in occasione di incidenti gravi connessi alle TIC e in seguito a istruzioni o conclusioni delle autorità di vigilanza formulate a seguito di pertinenti test di resilienza operativa digitale o di processi di audit. Il quadro è costantemente migliorato sulla base degli insegnamenti tratti dall'attuazione e dal monitoraggio.

7. Il quadro per la gestione dei rischi relativi alle TIC di cui al paragrafo 1 è sottoposto ad audit periodici da parte di revisori TIC in possesso di conoscenze, competenze ed esperienze adeguate in materia di rischi relativi alle TIC. La frequenza e l'oggetto degli audit in materia di TIC sono commisurati ai rischi connessi alle TIC cui è esposta l'entità finanziaria.

8. È istituito un processo formale per dare seguito all'audit in materia di TIC, comprendente regole per la verifica tempestiva delle risultanze critiche e l'adozione di rimedi, tenendo conto sia delle conclusioni dell'audit, sia della natura, delle dimensioni e della complessità dei servizi e delle attività delle entità finanziarie.

9. Il quadro per la gestione dei rischi relativi alle TIC di cui al paragrafo 1 comprende una strategia di resilienza digitale che definisce le modalità di attuazione del quadro. A tal fine esso include metodi per affrontare i rischi relativi alle TIC e conseguire specifici obiettivi in materia di TIC:

   (a) spiegando in che modo il quadro per la gestione dei rischi relativi alle TIC sostiene gli obiettivi e la strategia commerciale dell'entità finanziaria;

   (b) fissando il livello di tolleranza per i rischi relativi alle TIC, conformemente alla propensione al rischio dell'entità finanziaria e analizzando la tolleranza d'impatto per le perturbazioni a livello di TIC;

   (c) indicando chiari obiettivi in materia di sicurezza delle informazioni;

   (d) spiegando l'architettura di riferimento a livello di TIC e le eventuali modifiche necessarie per conseguire specifici obiettivi commerciali;

   (e) delineando i differenti meccanismi introdotti per individuare e prevenire gli incidenti connessi alle TIC e per proteggersi dal loro impatto;

   (f) documentando il numero di incidenti gravi connessi alle TIC segnalati, nonché l'efficacia delle misure preventive;

   (g) definendo una strategia olistica di TIC a livello di entità, basata su una varietà di fornitori, che indichi le principali dipendenze da fornitori terzi di servizi di

TIC e che spieghi la logica sottesa alla ripartizione degli appalti tra i fornitori terzi di servizi;

(h) attuando test di resilienza operativa digitale;

(i) delineando una strategia di comunicazione in caso di incidenti connessi alle TIC.

10. Su approvazione delle autorità competenti le entità finanziarie possono delegare a imprese interne o esterne al gruppo i compiti di verifica della conformità alle prescrizioni in materia di gestione dei rischi relativi alle TIC.

Articolo 6

Sistemi, protocolli e strumenti di TIC

1. Le entità finanziarie usano e curano la manutenzione di sistemi, protocolli e strumenti di TIC aggiornati, che soddisfano le condizioni seguenti:

(a) i sistemi e gli strumenti sono idonei alla natura, alla varietà, alla complessità e alle dimensioni delle operazioni a supporto dello svolgimento delle attività delle entità finanziarie;

(b) sono affidabili;

(c) hanno capacità sufficiente per elaborare in maniera accurata i dati necessari per lo svolgimento delle attività e la fornitura dei servizi in tempo utile, nonché per sostenere i picchi di volume di ordini, messaggi od operazioni, a seconda delle necessità, anche in caso di introduzione di nuove tecnologie;

(d) sono tecnologicamente resilienti, in modo da fare adeguatamente fronte alle esigenze di informazioni supplementari richieste da condizioni di stress del mercato o da altre situazioni avverse.

2. Qualora le entità finanziarie si avvalgano di norme tecniche riconosciute a livello internazionale e di pratiche di punta del settore in materia di sicurezza delle informazioni e controlli interni delle TIC, l'utilizzo di tali norme e pratiche avviene in conformità di eventuali raccomandazioni delle autorità di vigilanza sulla loro integrazione.

Articolo 7

Identificazione

1. Nell'ambito del quadro per la gestione dei rischi relativi alle TIC di cui all'articolo 5, paragrafo 1, le entità finanziarie identificano, classificano e documentano adeguatamente tutte le funzioni commerciali connesse alle TIC, i patrimoni di informazioni su cui fondano tali funzioni, nonché le configurazioni del sistema di TIC e le interconnessioni con i sistemi di TIC interni ed esterni. Le entità finanziarie riesaminano, secondo necessità e almeno una volta all'anno, l'adeguatezza della classificazione dei patrimoni di informazioni e di altri documenti eventualmente pertinenti.

2. Le entità finanziarie identificano costantemente tutte le fonti di rischi relativi alle TIC, in particolare l'esposizione al rischio da e verso altre entità finanziarie, e valutano le minacce informatiche e le vulnerabilità pertinenti per le loro funzioni

commerciali e i loro patrimoni di informazioni connessi alle TIC. Le entità finanziarie riesaminano periodicamente, e almeno una volta all'anno, gli scenari di rischio che esercitano un impatto su di loro.

3. Le entità finanziarie diverse dalle microimprese effettuano una valutazione del rischio in occasione di ogni modifica di rilievo dell'infrastruttura della rete e del sistema informativo, dei processi o delle procedure che incidono sulle loro funzioni, dei processi di sostegno o dei patrimoni di informazioni.

4. Le entità finanziarie identificano tutti gli account dei sistemi di TIC, compresi quelli su siti remoti, le risorse di rete e le attrezzature hardware, e tracciano una mappa delle attrezzature fisiche considerate critiche. Effettuano la mappatura della configurazione dei beni a livello di TIC, nonché dei collegamenti e delle interdipendenze tra i diversi beni a livello di TIC.

5. Le entità finanziarie identificano e documentano tutti i processi dipendenti da fornitori terzi di servizi di TIC e identificano le interconnessioni con detti fornitori.

6. Ai fini dei paragrafi 1, 4 e 5 le entità finanziarie mantengono inventari pertinenti e li aggiornano periodicamente.

7. Le entità finanziarie diverse dalle microimprese effettuano periodicamente, e almeno una volta all'anno, una valutazione del rischio specifica per tutti i sistemi di TIC preesistenti, soprattutto prima e dopo la connessione fra tecnologie, applicazioni o sistemi nuovi e vecchi.

Articolo 8

Protezione e prevenzione

1. Allo scopo di proteggere adeguatamente i sistemi di TIC e nella prospettiva di organizzare misure di risposta, le entità finanziarie monitorano e controllano costantemente il funzionamento dei sistemi e degli strumenti di TIC e riducono al minimo l'impatto di tali rischi adottando politiche, procedure e strumenti adeguati per la sicurezza delle TIC.

2. Le entità finanziarie definiscono, acquisiscono e attuano strategie, politiche, procedure, protocolli e strumenti per la sicurezza delle TIC miranti in particolare a garantire la resilienza, la continuità e la disponibilità dei sistemi di TIC, nonché a mantenere standard elevati di sicurezza, riservatezza e integrità dei dati conservati, in uso o in transito.

3. Per conseguire gli obiettivi di cui al paragrafo 2 le entità finanziarie usano tecnologie e processi TIC avanzati che:

   (a) garantiscono la sicurezza dei mezzi di trasferimento delle informazioni;

   (b) riducono al minimo i rischi di corruzione o perdita di dati, di accesso non autorizzato nonché di difetti tecnici che possono ostacolare l'attività commerciale;

   (c) impediscono le fughe di informazioni;

   (d) assicurano la protezione dei dati contro la cattiva amministrazione o rischi relativi al trattamento dei dati, compresa l'inadeguatezza della tenuta di registri.

4. All'interno del quadro per la gestione dei rischi relativi alle TIC di cui all'articolo 5, paragrafo 1, le entità finanziarie:

   (a) elaborano e documentano una politica di sicurezza dell'informazione che definisce le norme per tutelare la riservatezza, l'integrità e la disponibilità di risorse, dati e patrimoni di informazioni a livello di TIC propri e dei propri clienti;

   (b) seguendo un approccio basato sul rischio, realizzano una solida gestione della rete e delle infrastrutture impiegando tecniche, metodi e protocolli adeguati, tra cui l'applicazione di meccanismi automatizzati, per isolare i patrimoni di informazioni colpiti in caso di attacchi;

   (c) attuano politiche che limitano l'accesso fisico e virtuale alle risorse e ai dati del sistema TIC unicamente a quanto è necessario per funzioni e attività legittime e approvate, e stabiliscono a tale scopo una serie di politiche, procedure e controlli concernenti i diritti di accesso e una solida amministrazione degli stessi;

   (d) attuano politiche e protocolli riguardanti robusti meccanismi di autenticazione, basati su norme pertinenti e sistemi di controllo dedicati, per prevenire l'accesso alle chiavi crittografiche in base alle quali i dati sono cifrati sulla scorta dei risultati di processi approvati per la classificazione dei dati e la valutazione del rischio;

   (e) attuano politiche, procedure e controlli per la gestione delle modifiche delle TIC, comprese le modifiche apportate a componenti software, hardware e firmware e le modifiche del sistema o della sicurezza, che adottano un approccio basato sulla valutazione del rischio e sono parte integrante del processo complessivo di gestione delle modifiche dell'entità finanziaria, in modo che tutte le modifiche apportate ai sistemi di TIC siano registrate, testate, valutate, approvate, attuate e verificate in maniera controllata;

   (f) si dotano di politiche idonee ed esaustive in materia di correzioni ed aggiornamenti.

Ai fini della lettera b) le entità finanziarie progettano l'infrastruttura di connessione di rete in modo che sia possibile isolarla istantaneamente e ne assicurano la compartimentazione e la segmentazione, al fine di ridurre al minimo e prevenire il contagio, soprattutto per i processi finanziari interconnessi.

Ai fini della lettera e) il processo di gestione delle modifiche delle TIC è approvato da linee di gestione adeguate e comprende protocolli specifici per le modifiche di emergenza.

Articolo 9

Individuazione

1. Le entità finanziarie predispongono meccanismi per individuare tempestivamente le attività anomale, conformemente all'articolo 15, compresi i problemi di prestazione della rete delle TIC e gli incidenti a esse connessi, nonché per individuare tutti i potenziali singoli punti di guasto importanti.

   Tutti i meccanismi di individuazione di cui al primo comma sono periodicamente testati in conformità dell'articolo 22.

2. I meccanismi di individuazione di cui al paragrafo 1 prevedono molteplici livelli di controllo, definiscono soglie di allarme e criteri per l'avvio dei processi di individuazione degli incidenti connessi alle TIC e di risposta agli stessi e istituiscono meccanismi di allarme automatico per il personale incaricato della risposta agli incidenti connessi alle TIC.

3. Le entità finanziarie dedicano risorse e capacità sufficienti, tenendo conto delle proprie dimensioni e del proprio profilo commerciale e di rischio, al monitoraggio dell'attività degli utenti e al verificarsi di anomalie e incidenti connessi alle TIC, in particolare attacchi informatici.

4. Le entità finanziarie di cui all'articolo 2, paragrafo 1, lettera l), predispongono inoltre sistemi in grado di controllare efficacemente le comunicazioni sulle operazioni per verificarne la completezza, individuare omissioni ed errori palesi e chiederne la ritrasmissione.

Articolo 10

Risposta e ripristino

1. All'interno del quadro per la gestione dei rischi relativi alle TIC di cui all'articolo 5, paragrafo 1, e in base ai requisiti di identificazione stabiliti all'articolo 7, le entità finanziarie predispongono una politica di continuità operativa delle TIC dedicata ed esaustiva come parte integrante della propria politica di continuità operativa.

2. Le entità finanziarie attuano la politica di continuità operativa delle TIC di cui al paragrafo 1 tramite accordi, piani, procedure e meccanismi appositi, appropriati e documentati, allo scopo di:

   (a) registrare tutti gli incidenti connessi alle TIC;

   (b) garantire la continuità delle funzioni critiche dell'entità finanziaria;

   (c) rispondere in maniera rapida, appropriata ed efficace e trovare una soluzione a tutti gli incidenti connessi alle TIC, in particolare (ma non solo) agli attacchi informatici, in modo da limitare i danni e privilegiare la ripresa delle attività e le azioni di ripristino;

   (d) attivare senza indugio piani dedicati che prevedano tecnologie, processi e misure di contenimento idonei a ciascun tipo di incidente connesso alle TIC e a scongiurare danni ulteriori, nonché procedure mirate di risposta e ripristino stabilite in conformità dell'articolo 11;

   (e) stimare in via preliminare impatti, danni e perdite;

   (f) stabilire azioni di comunicazione e gestione delle crisi che assicurino la trasmissione di informazioni aggiornate a tutto il personale interno interessato e ai portatori di interessi esterni, conformemente all'articolo 13, e la segnalazione di tali informazioni alle autorità competenti, conformemente all'articolo 17.

3. All'interno del quadro per la gestione dei rischi relativi alle TIC di cui all'articolo 5, paragrafo 1, le entità finanziarie attuano il piano di ripristino in caso di disastro relativo alle TIC; per le entità finanziarie diverse dalle microimprese tale piano è soggetto a un audit indipendente.

4. Le entità finanziarie predispongono, mantengono e testano periodicamente opportuni piani di continuità operativa delle TIC, in particolare per quanto riguarda le funzioni

critiche o importanti esternalizzate o appaltate tramite accordi con fornitori terzi di servizi di TIC.

5. All'interno della gestione complessiva dei rischi relativi alle TIC, le entità finanziarie:

   (a) testano la politica di continuità operativa delle TIC e il piano di ripristino in caso di disastro relativo alle TIC almeno una volta all'anno e dopo modifiche di rilievo ai sistemi di TIC;

   (b) testano i piani di comunicazione delle crisi istituiti in conformità dell'articolo 13.

   Ai fini della lettera a), le entità finanziarie diverse dalle microimprese inseriscono nei piani dei test scenari di attacchi informatici e di passaggi tra le infrastrutture delle TIC primarie e la capacità ridondante, i backup e le attrezzature ridondanti necessarie per soddisfare gli obblighi di cui all'articolo 11.

   Le entità finanziarie riesaminano periodicamente la politica di continuità operativa delle TIC e il piano di ripristino in caso di disastro relativo alle TIC, tenendo conto dei risultati dei test svolti in conformità del primo comma e delle raccomandazioni formulate sulla base dei controlli di audit o degli esami di vigilanza.

6. Le entità finanziarie diverse dalle microimprese si dotano di una funzione di gestione delle crisi che, in caso di attivazione della politica di continuità operativa delle TIC o del piano di ripristino in caso di disastro relativo alle TIC, fissa procedure chiare per la gestione della comunicazione interna ed esterna delle crisi, in conformità dell'articolo 13.

7. Le entità finanziarie registrano le attività svolte prima e durante le perturbazioni in cui si attiva la politica di continuità operativa delle TIC o il piano di ripristino in caso di disastro relativo alle TIC. Tali registrazioni sono prontamente disponibili.

8. Le entità finanziarie di cui all'articolo 2, paragrafo 1, lettera f), trasmettono alle autorità competenti copie dei risultati dei test di continuità operativa delle TIC o di esercizi analoghi effettuati durante il periodo in esame.

9. Le entità finanziarie diverse dalle microimprese segnalano alle autorità competenti tutti i costi e le perdite causati dalle perturbazioni a livello di TIC e dagli incidenti connessi alle TIC.

Articolo 11

Politiche di backup e metodi di ripristino

1. Al fine di assicurare che i sistemi di TIC siano ripristinati riducendo al minimo il periodo di inattività e limitando la perturbazione, all'interno del proprio quadro per la gestione dei rischi relativi alle TIC le entità finanziarie elaborano:

   (a) la politica di backup che precisi l'ampiezza dei dati soggetti a backup e la frequenza minima del backup, in base alla criticità delle informazioni o alla sensibilità dei dati;

   (b) i metodi di ripristino.

2. I sistemi di backup dovrebbero iniziare il trattamento senza indebiti ritardi, a meno che l'inizio di quest'attività non metta a repentaglio la sicurezza della rete e dei sistemi informativi o l'integrità o la riservatezza dei dati.

3. Nel ripristino dei dati di backup effettuato utilizzando i propri sistemi, le entità finanziarie impiegano sistemi di TIC aventi un contesto operativo differente da quello principale, non direttamente connesso con quest'ultimo e protetto in maniera sicura da qualsiasi accesso non autorizzato o corruzione delle TIC.

   Per le entità finanziarie di cui all'articolo 2, paragrafo 1, lettera g), i piani di ripristino consentono il ripristino di tutte le operazioni in corso al momento della perturbazione, così da permettere alla controparte centrale di continuare a operare con certezza e di completare la liquidazione alla data programmata.

4. Le entità finanziarie mantengono capacità di TIC ridondanti, dotate di risorse e funzionalità sufficienti e idonee a soddisfare le esigenze commerciali.

5. Le entità finanziarie di cui all'articolo 2, paragrafo 1, lettera f), mantengono, o si assicurano che i loro fornitori terzi di servizi di TIC mantengano, almeno un sito secondario di trattamento dati dotato di risorse, capacità, funzionalità e personale sufficienti e adeguati a soddisfare le esigenze commerciali.

   Il sito secondario di trattamento dati è:

   (a) ubicato geograficamente a distanza dal sito primario di trattamento dati per garantire un profilo di rischio distinto e impedire che venga colpito dall'evento che ha interessato il sito primario;

   (b) in grado di garantire la continuità dei servizi critici in maniera identica al sito primario, oppure di fornire il livello di servizi necessario a garantire che l'entità finanziaria svolga le proprie operazioni critiche nell'ambito degli obiettivi di ripristino;

   (c) immediatamente accessibile al personale dell'entità finanziaria per garantire la continuità dei servizi critici qualora il sito primario di trattamento dati divenga indisponibile.

6. Nel determinare gli obiettivi in materia di punti e tempi di ripristino di ciascuna funzione, le entità finanziarie tengono conto del potenziale impatto complessivo sull'efficienza del mercato. Questi obiettivi in materia di tempi garantiscono che i livelli di servizi concordati siano rispettati anche in scenari estremi.

7. Durante il ripristino successivo a un incidente connesso alle TIC le entità finanziarie effettuano molteplici verifiche, compresi i controlli incrociati, per assicurare il più elevato livello di integrità dei dati. Questi controlli sono effettuati anche al momento di ricostruire i dati provenienti da portatori di interessi esterni, per assicurare la piena coerenza di tutti i dati tra i sistemi.

Articolo 12

Apprendimento ed evoluzione

1. Le entità finanziare predispongono capacità e personale idonei alle proprie dimensioni, nonché al rispettivo profilo commerciale e di rischio, per raccogliere informazioni in relazione alle vulnerabilità e alle minacce informatiche, agli incidenti connessi alle TIC, in particolare agli attacchi informatici, e analizzarne i probabili effetti sulla loro resilienza operativa digitale.

2. Dopo gravi perturbazioni a livello di TIC delle loro attività principali, le entità finanziarie predispongono un riesame successivo all'incidente connesso alle TIC che analizzi le cause della perturbazione e identifichi i miglioramenti che è necessario

apportare alle operazioni riguardanti le TIC o nell'ambito della politica di continuità operativa delle TIC di cui all'articolo 10.

Al momento di attuare modifiche, le entità finanziarie diverse dalle microimprese comunicano tali modifiche alle autorità competenti.

Il riesame successivo all'incidente connesso alle TIC di cui al primo comma determina se le procedure stabilite siano state seguite e se le azioni adottate siano state efficaci, anche in relazione:

(a) alla tempestività della risposta agli allarmi di sicurezza e alla determinazione dell'impatto degli incidenti connessi alle TIC e della loro gravità;

(b) alla qualità e alla rapidità dell'analisi forense;

(c) all'efficacia della procedura di attivazione dei livelli successivi di intervento in caso di incidenti all'interno dell'entità finanziaria;

(d) all'efficacia della comunicazione interna ed esterna.

3. Gli insegnamenti tratti dai test sulla resilienza operativa digitale effettuati in conformità degli articoli 23 e 24 e da incidenti connessi alle TIC realmente avvenuti (in particolare attacchi informatici), insieme alle difficoltà riscontrate al momento dell'attivazione della politica di continuità operativa o dei piani di ripristino, e le informazioni pertinenti scambiate con le controparti e valutate nel corso degli esami di vigilanza sono debitamente e costantemente integrati nel processo di valutazione dei rischi relativi alle TIC. Tali risultanze si traducono in opportune revisioni delle relative componenti del quadro per la gestione dei rischi relativi alle TIC di cui all'articolo 5, paragrafo 1.

4. Le entità finanziarie monitorano l'efficacia dell'attuazione della strategia di resilienza digitale stabilita all'articolo 5, paragrafo 9. Tracciano l'evoluzione nel tempo dei rischi relativi alle TIC, analizzano la frequenza, i tipi, le dimensioni e l'evoluzione degli incidenti connessi alle TIC, in particolare gli attacchi informatici e i relativi modelli, al fine di comprendere il livello di esposizione ai rischi relativi alle TIC e migliorare la maturità informatica e la preparazione dell'entità finanziaria.

5. Il personale addetto alle TIC di grado più elevato comunica almeno una volta all'anno all'organo di gestione le risultanze di cui al paragrafo 3 e formula raccomandazioni.

6. Le entità finanziarie elaborano programmi di sensibilizzazione sulla sicurezza delle TIC nonché attività di formazione sulla resilienza operativa digitale, che rappresentano moduli obbligatori nei programmi di formazione del personale. Tali attività riguardano tutti i dipendenti e gli alti dirigenti.

Le entità finanziarie monitorano costantemente i pertinenti sviluppi tecnologici, anche al fine di comprendere i possibili impatti dell'impiego di tali nuove tecnologie sulle prescrizioni in materia di sicurezza delle TIC e sulla resilienza operativa digitale. Si tengono aggiornate sui più recenti processi di gestione dei rischi relativi alle TIC, in modo da contrastare efficacemente le forme nuove o già esistenti di attacchi informatici.

Articolo 13

Comunicazione

1. All'interno del quadro per la gestione dei rischi relativi alle TIC di cui all'articolo 5, paragrafo 1, le entità finanziarie predispongono piani di comunicazione che consentano una divulgazione responsabile di informazioni sugli incidenti connessi alle TIC o sulle vulnerabilità più rilevanti ai clienti e alle controparti nonché al pubblico, a seconda dei casi.

2. All'interno del quadro per la gestione dei rischi relativi alle TIC di cui all'articolo 5, paragrafo 1, le entità finanziarie attuano politiche di comunicazione per il personale e per i portatori di interessi esterni. Le politiche di comunicazione per il personale tengono conto dell'esigenza di operare un distinguo tra il personale coinvolto nella gestione dei rischi relativi alle TIC, in particolare per quanto riguarda la risposta e il ripristino, e il personale che è necessario informare.

3. Nell'entità vi è almeno una persona incaricata di attuare la strategia di comunicazione per gli incidenti connessi alle TIC e assolvere a tal fine il ruolo di portavoce nei confronti del pubblico e dei mezzi di comunicazione.

Articolo 14

Ulteriore armonizzazione di strumenti, metodi, processi e politiche di gestione dei rischi relativi alle TIC

L'Autorità bancaria europea (ABE), l'Autorità europea degli strumenti finanziari e dei mercati (ESMA) e l'Autorità europea delle assicurazioni e delle pensioni aziendali e professionali (EIOPA), in consultazione con l'Agenzia dell'Unione europea per la cibersicurezza (ENISA) elaborano progetti di norme tecniche di regolamentazione ai seguenti fini:

(a) specificare ulteriori elementi da inserire nelle politiche, nelle procedure, nei protocolli e negli strumenti in materia di sicurezza delle TIC di cui all'articolo 8, paragrafo 2, allo scopo di garantire la sicurezza delle reti, introdurre salvaguardie adeguate contro le intrusioni e l'uso improprio dei dati, preservare l'autenticità e l'integrità dei dati, inserire tecniche crittografiche e assicurare un'accurata e pronta trasmissione dei dati senza gravi perturbazioni;

(b) prescrivere le modalità con cui le politiche, le procedure e gli strumenti in materia di sicurezza delle TIC di cui all'articolo 8, paragrafo 2, integrano i controlli di sicurezza nei sistemi fin dall'inizio (sicurezza fin dalla progettazione), consentono l'adeguamento al mutevole contesto delle minacce e prevedono l'uso di tecnologie di difesa in profondità;

(c) specificare ulteriormente le tecniche, i metodi e i protocolli adeguati di cui all'articolo 8, paragrafo 4, lettera b);

(d) sviluppare ulteriori componenti dei controlli sui diritti di gestione dell'accesso di cui all'articolo 8, paragrafo 4, lettera c), e della relativa politica di risorse umane, precisando i diritti di accesso, le procedure per concedere e revocare i diritti, il monitoraggio di comportamenti anomali in relazione ai rischi relativi alle TIC mediante indicatori appropriati, compresi i modelli di utilizzo della rete, gli orari, l'attività informatica e i dispositivi sconosciuti;

(e) elaborare ulteriormente gli elementi specificati all'articolo 9, paragrafo 1, in modo da consentire un'individuazione tempestiva delle attività anomale, e i

criteri di cui all'articolo 9, paragrafo 2, per l'avvio dei processi di individuazione degli incidenti connessi alle TIC e di risposta agli stessi;

(f) specificare ulteriormente le componenti della politica di continuità operativa delle TIC, di cui all'articolo 10, paragrafo 1;

(g) precisare ulteriormente i test previsti dai piani di continuità operativa delle TIC di cui all'articolo 10, paragrafo 5, per garantire che tengano debitamente conto degli scenari in cui la qualità dell'esercizio di una funzione critica o importante si deteriora a un livello inaccettabile o viene meno, e che considerino adeguatamente il potenziale impatto dell'insolvenza o di altre disfunzioni di pertinenti fornitori terzi di servizi di TIC e, se del caso, i rischi politici nelle giurisdizioni dei rispettivi fornitori;

(h) specificare ulteriormente le componenti del piano di ripristino in caso di disastro relativo alle TIC di cui all'articolo 10, paragrafo 3.

L'ABE, l'ESMA e l'EIOPA presentano tali progetti di norme tecniche di regolamentazione alla Commissione entro il [*GU: inserire la data corrispondente a un anno dopo la data di entrata in vigore*].

Alla Commissione è delegato il potere di adottare le norme tecniche di regolamentazione di cui al primo comma conformemente agli articoli da 10 a 14 dei regolamenti (UE) n. 1093/2010, (UE)n. 1094/2010 e (UE) n. 1095/2010.

CAPO III

INCIDENTI CONNESSI ALLE TIC

GESTIONE, CLASSIFICAZIONE e SEGNALAZIONE

Articolo 15

Processo di gestione degli incidenti connessi alle TIC

1. Le entità finanziarie stabiliscono e attuano un processo di gestione degli incidenti connessi alle TIC al fine di individuare, gestire e notificare tali incidenti e predispongono indicatori di allerta precoce come segnali di allarme.

2. Le entità finanziarie istituiscono processi appropriati per garantire, in maniera coerente e integrata, il monitoraggio e il trattamento degli incidenti connessi alle TIC, nonché il relativo seguito, in modo da identificare ed eliminare le cause di fondo e prevenire il verificarsi di tali incidenti.

3. Il processo di gestione degli incidenti connessi alle TIC di cui al paragrafo 1:

(a) stabilisce procedure per identificare, seguire, registrare, categorizzare e classificare gli incidenti connessi alle TIC in base alla loro priorità, nonché alla gravità e alla criticità dei servizi colpiti, conformemente ai criteri di cui all'articolo 16, paragrafo 1;

(b) assegna i ruoli e le responsabilità che è necessario attivare per i diversi scenari e tipi di incidenti connessi alle TIC;

(c) elabora piani per la comunicazione al personale, ai portatori di interessi esterni e ai mezzi di comunicazione conformemente all'articolo 13, nonché per la

notifica ai clienti, le procedure di attivazione dei livelli successivi di intervento, compresi i reclami dei clienti in materia di TIC, e la comunicazione di informazioni alle entità finanziarie che agiscono da controparti, a seconda dei casi;

(d) assicura la segnalazione degli incidenti gravi connessi alle TIC agli alti dirigenti interessati e informa l'organo di gestione in merito a detti incidenti, illustrandone l'impatto e la risposta e i controlli supplementari da introdurre;

(e) stabilisce procedure di risposta agli incidenti connessi alle TIC per attenuarne l'impatto e garantisce tempestivamente l'operatività e la sicurezza dei servizi.

Articolo 16

Classificazione degli incidenti connessi alle TIC

1. Le entità finanziarie classificano gli incidenti connessi alle TIC e ne determinano l'impatto in base ai criteri seguenti:

(a) il numero di utenti o controparti finanziarie colpiti dalla perturbazione provocata dall'incidente connesso alle TIC e il fatto che tale incidente abbia provocato o meno un impatto reputazionale;

(b) la durata dell'incidente connesso alle TIC, compreso il periodo di inattività del servizio;

(c) l'estensione geografica dell'incidente connesso alle TIC, con riferimento alle aree colpite, in particolare se interessa più di due Stati membri;

(d) le perdite di dati derivanti dall'incidente connesso alle TIC, come la perdita di integrità, riservatezza o disponibilità;

(e) la gravità dell'impatto dell'incidente connesso alle TIC sui relativi sistemi dell'entità finanziaria;

(f) la criticità dei servizi colpiti, comprese le operazioni dell'entità finanziaria;

(g) l'impatto economico dell'incidente connesso alle TIC in termini sia assoluti che relativi.

2. Previa consultazione della Banca centrale europea (BCE) e dell'ENISA, le AEV elaborano, tramite il comitato congiunto delle AEV (il "comitato congiunto"), un progetto di norme tecniche di regolamentazione comuni che specifica in maniera più approfondita gli aspetti seguenti:

(a) i criteri di cui al paragrafo 1, comprese le soglie di rilevanza per la determinazione degli incidenti gravi connessi alle TIC che sono soggetti all'obbligo di segnalazione di cui all'articolo 17, paragrafo 1;

(b) i criteri che le autorità competenti devono applicare per valutare la rilevanza degli incidenti gravi connessi alle TIC rispetto alle giurisdizioni di altri Stati membri, nonché i dettagli delle segnalazioni di incidenti connessi alle TIC da condividere con altre autorità competenti ai sensi dell'articolo 17, paragrafi 5 e 6.

3. Al momento di elaborare il progetto di norme tecniche di regolamentazione comuni di cui al paragrafo 2, le AEV tengono conto delle norme internazionali nonché delle specifiche elaborate e pubblicate dall'ENISA, tra cui, se del caso, le specifiche riguardanti altri settori economici.

Le AEV presentano detti progetti di norme tecniche di regolamentazione comuni alla Commissione entro il [*PO: inserire la data corrispondente a un anno dopo la data di entrata in vigore*].

Alla Commissione è delegato il potere di integrare il presente regolamento, adottando le norme tecniche di regolamentazione di cui al paragrafo 2 in conformità, rispettivamente, degli articoli da 10 a 14 dei regolamenti (UE) n. 1093/2010, (UE) n. 1094/2010 e (UE) n. 1095/2010.

Articolo 17

Segnalazione degli incidenti gravi connessi alle TIC

1. Le entità finanziarie segnalano gli incidenti gravi connessi alle TIC all'autorità competente di cui all'articolo 41 entro i termini fissati al paragrafo 3.

   Ai fini del primo comma, le entità finanziarie redigono, dopo aver raccolto e analizzato tutte le informazioni pertinenti, una relazione sull'incidente utilizzando il modello di cui all'articolo 18 e la trasmettono all'autorità competente.

   La relazione contiene tutte le informazioni necessarie all'autorità competente per determinare la rilevanza dell'incidente grave connesso alle TIC e valutarne i possibili impatti transfrontalieri.

2. Qualora un incidente grave connesso alle TIC eserciti o possa esercitare un impatto sugli interessi finanziari dei clienti e degli utenti del servizio, le entità finanziarie informano, senza indebito ritardo, clienti e utenti del servizio in merito a tale incidente e comunicano loro, il prima possibile, tutte le misure che sono state adottate per attenuare gli effetti avversi dell'incidente.

3. Le entità finanziarie trasmettono all'autorità competente di cui all'articolo 41:

   (a) una notifica iniziale, senza indugio e in ogni caso entro la fine del giorno lavorativo oppure, nel caso di un incidente grave connesso alle TIC che si sia verificato meno di due ore prima della fine del giorno lavorativo, entro quattro ore dall'inizio del giorno lavorativo successivo oppure, qualora non siano disponibili canali di segnalazione, non appena questi diventino disponibili;

   (b) una relazione intermedia, entro una settimana dalla notifica iniziale di cui alla lettera a) seguita, a seconda dei casi, da notifiche aggiornate, ogni qualvolta sia disponibile un aggiornamento della situazione, nonché su specifica richiesta dell'autorità competente;

   (c) una relazione finale, quando l'analisi delle cause di fondo sia stata completata, indipendentemente dal fatto che le misure di attenuazione siano già state attuate, e quando al posto delle stime siano disponibili i dati dell'impatto effettivo, ma in ogni caso entro un mese dall'invio della segnalazione iniziale.

4. Ai sensi del presente articolo, le entità finanziarie possono delegare gli obblighi di segnalazione a un fornitore terzo di servizi soltanto se tale delega è approvata dall'autorità competente di cui all'articolo 41.

5. Dopo aver ricevuto la segnalazione di cui al paragrafo 1, l'autorità competente trasmette senza indebito ritardo i dettagli dell'incidente:

   (a) all'ABE, all'ESMA o all'EIOPA, a seconda dei casi;

(b) alla BCE, se opportuno, qualora siano coinvolte le entità finanziarie di cui all'articolo 2, paragrafo 1, lettere a), b) e c);

(c) al punto di contatto unico designato ai sensi dell'articolo 8 della direttiva (UE) 2016/1148.

6. L'ABE, l'ESMA o l'EIOPA e la BCE valutano la pertinenza dell'incidente grave connesso alle TIC rispetto ad altre autorità pubbliche interessate e inviano loro una notifica al riguardo il prima possibile. La BCE notifica i membri del Sistema europeo di banche centrali in merito a questioni afferenti il sistema di pagamenti. Sulla base di tale notifica, le autorità competenti adottano, se del caso, tutte le misure necessarie per proteggere l'immediata stabilità del sistema finanziario.

Articolo 18

Armonizzazione dei modelli e dei contenuti per la segnalazione

1. Previa consultazione dell'ENISA e della BCE, le AEV, tramite il comitato congiunto, elaborano quanto segue:

(a) progetti di norme tecniche di regolamentazione comuni per:

(1) stabilire il contenuto delle segnalazioni relative agli incidenti gravi connessi alle TIC;

(2) precisare ulteriormente le condizioni alle quali le entità finanziarie possono delegare a un fornitore terzo di servizi, previa approvazione dell'autorità competente, gli obblighi di segnalazione di cui al presente capo;

(b) progetti di norme tecniche di attuazione comuni per stabilire i formati, i modelli e le procedure standard con cui le entità finanziarie devono segnalare un incidente grave connesso alle TIC.

Le AEV trasmettono alla Commissione i progetti di norme tecniche di regolamentazione comuni di cui al paragrafo 1, lettera a), e i progetti di norme tecniche di attuazione comuni di cui al paragrafo 1, lettera b), entro il xx 202x [*PO: inserire la data corrispondente a un anno dopo la data di entrata in vigore*].

Alla Commissione è delegato il potere di integrare il presente regolamento, adottando le norme tecniche di regolamentazione comuni di cui al paragrafo 1, lettera a), in conformità, rispettivamente, degli articoli da 10 a 14 dei regolamenti (UE) n. 1093/2010, (UE) n. 1095/2010 e (UE) n. 1094/2010.

Alla Commissione è conferito il potere di adottare le norme tecniche di attuazione comuni di cui al paragrafo 1, lettera b), in conformità, rispettivamente, dell'articolo 15 dei regolamenti (UE) n. 1093/2010, (UE) n. 1095/2010 e (UE) n. 1094/2010.

Articolo 19

Centralizzazione della segnalazione di incidenti gravi connessi alle TIC

1. In consultazione con la BCE e l'ENISA, le AEV, tramite il comitato congiunto, redigono una relazione congiunta che valuta la fattibilità dell'ulteriore centralizzazione delle segnalazioni degli incidenti mediante l'istituzione di un polo UE unico per la segnalazione degli incidenti gravi connessi alle TIC da parte delle

entità finanziarie. La relazione esamina i criteri per agevolare il flusso delle segnalazioni di incidenti connessi alle TIC, ridurre i costi associati e corroborare le analisi tematiche per migliorare la convergenza della vigilanza.

2. La relazione di cui al paragrafo 1 comprende almeno gli elementi seguenti:

(a) prerequisiti per l'istituzione del polo UE in questione;

(b) benefici, limiti e possibili rischi;

(c) elementi della gestione operativa;

(d) condizioni di adesione;

(e) modalità con cui le entità finanziarie e le autorità nazionali competenti accedono al polo UE;

(f) una valutazione preliminare dei costi finanziari derivanti dall'istituzione della piattaforma operativa su cui dovrà fondarsi il polo UE, comprese le competenze necessarie.

3. Le AEV presentano la relazione di cui al paragrafo 1 alla Commissione, al Parlamento europeo e al Consiglio entro il xx 202x [*GU: inserire la data corrispondente a tre anni dopo la data di entrata in vigore*].

Articolo 20

Riscontri forniti dalle autorità di vigilanza

1. Dopo aver ricevuto la relazione di cui all'articolo 17, paragrafo 1, l'autorità competente accusa ricevuta della notifica e invia il prima possibile all'entità finanziaria tutti i riscontri o gli orientamenti necessari, in particolare allo scopo di discutere rimedi a livello di entità o metodi per ridurre al minimo gli effetti avversi nei diversi settori.

2. Le AEV, tramite il comitato congiunto, riferiscono con frequenza annuale, sulla base di dati anonimizzati e aggregati, in merito alle notifiche di incidenti connessi alle TIC ricevute dalle autorità competenti, indicando almeno il numero degli incidenti gravi connessi alle TIC, la natura, l'impatto sulle operazioni delle entità finanziarie o dei clienti, i costi e le azioni di riparazione intraprese.

Le AEV emanano segnalazioni di allerta e redigono statistiche di alto livello a supporto delle valutazioni della vulnerabilità e delle minacce connesse alle TIC.

CAPO IV

TEST DI RESILIENZA OPERATIVA DIGITALE

Articolo 21

Prescrizioni generali per lo svolgimento dei test di resilienza operativa digitale

1. Allo scopo di valutare la preparazione agli incidenti connessi alle TIC, di identificare punti deboli, carenze o lacune della resilienza operativa digitale e di attuare tempestivamente misure correttive, le entità finanziarie stabiliscono, mantengono e riesaminano, tenendo conto delle proprie dimensioni, nonché del rispettivo profilo commerciale e di rischio, un programma di test di resilienza operativa digitale solido

ed esaustivo quale parte integrante del quadro per la gestione dei rischi relativi alle TIC di cui all'articolo 5.

2. Il programma di test di resilienza operativa digitale comprende una serie di valutazioni, test, metodologie, pratiche e strumenti da applicare conformemente alle disposizioni di cui agli articoli 22 e 23.

3. Le entità finanziarie, nello svolgimento del programma di test di resilienza operativa digitale di cui al paragrafo 1, adottano un approccio basato sul rischio tenendo conto del mutevole contesto dei rischi relativi alle TIC, di eventuali rischi specifici cui l'entità finanziaria è o potrebbe essere esposta, della criticità dei patrimoni di informazioni e dei servizi forniti, nonché di qualsiasi altro fattore giudicato rilevante dall'entità finanziaria stessa.

4. Le entità finanziarie assicurano che i test siano svolti da soggetti indipendenti, interni o esterni.

5. Le entità finanziarie introducono procedure e politiche per dare un ordine di priorità ai problemi evidenziati durante lo svolgimento dei test, per classificarli e porvi rimedio; stabiliscono inoltre metodologie di convalida interne per accertare che tutti i punti deboli, le carenze o le lacune che sono stati individuati siano pienamente affrontati.

6. Le entità finanziarie sottopongono a test tutte le applicazioni e i sistemi di TIC critici con cadenza almeno annuale.

Articolo 22

Test di strumenti e sistemi di TIC

1. Il programma di test di resilienza operativa digitale di cui all'articolo 21 prevede l'esecuzione di una serie completa di test adeguati, tra cui individuazione e valutazione delle vulnerabilità, analisi open source, valutazioni della sicurezza delle reti, analisi delle carenze, esami della sicurezza fisica, questionari e soluzioni di software di scansione, esami del codice sorgente (ove fattibile), test di compatibilità, test basati su scenari, test di compatibilità, test di prestazione, test end-to-end o test di penetrazione.

2. Le entità finanziarie di cui all'articolo 2, paragrafo 1, lettere f) e g), effettuano valutazioni della vulnerabilità prima di ciascuna introduzione o reintroduzione di servizi nuovi o già esistenti a sostegno delle funzioni, delle applicazioni e delle componenti infrastrutturali critiche dell'entità finanziaria.

Articolo 23

Test avanzati di strumenti, sistemi e processi di TIC fondati su test di penetrazione basati su minacce

1. Le entità finanziarie identificate ai sensi del paragrafo 4 effettuano test avanzati sotto forma di test di penetrazione basati su minacce con cadenza almeno triennale.

2. I test di penetrazione basati su minacce riguardano quantomeno le funzioni e i servizi critici dell'entità finanziaria e sono effettuati sui reali sistemi di produzione che sostengono tali funzioni. Il preciso ambito di applicazione dei test di penetrazione basati su minacce, fondato sulla valutazione di funzioni e servizi critici, è determinato dalle entità finanziarie ed è convalidato dalle autorità competenti.

Ai fini del primo comma, le entità finanziarie identificano tutti i processi, i sistemi e le tecnologie TIC sottostanti a supporto delle funzioni e dei servizi critici, comprese le funzioni e i servizi esternalizzati o appaltati a fornitori terzi di servizi di TIC.

Qualora i fornitori terzi di servizi di TIC rientrino nell'ambito dei test di penetrazione basati su minacce, l'entità finanziaria adotta le misure necessarie per garantire la partecipazione di tali fornitori.

Le entità finanziarie applicano efficaci controlli di gestione del rischio per ridurre i rischi di potenziali impatti sui dati, danni alle attività e perturbazioni delle operazioni o dei servizi critici delle entità finanziarie, delle loro controparti o del settore finanziario.

Alla fine dei test, quando relazioni e piani correttivi siano stati concordati, l'entità finanziaria e i tester esterni trasmettono all'autorità competente la documentazione attestante che i test di penetrazione basati su minacce sono stati svolti conformemente alle prescrizioni. Le autorità competenti convalidano la documentazione e rilasciano un attestato.

3. Per l'effettuazione dei test di penetrazione basati su minacce, le entità finanziarie si avvalgono di tester in conformità dell'articolo 24.

Le autorità competenti identificano le entità finanziarie tenute a svolgere test di penetrazione basati su minacce secondo modalità proporzionate alle dimensioni, all'attività e al profilo di rischio complessivo dell'entità finanziaria, sulla base della valutazione degli elementi seguenti:

(a) i fattori correlati all'impatto, in particolare la criticità dei servizi forniti e delle attività svolte dall'entità finanziaria;

(b) i possibili problemi di stabilità finanziaria, tra cui il carattere sistemico dell'entità finanziaria a livello nazionale o di Unione, a seconda dei casi;

(c) lo specifico profilo di rischio relativo alle TIC, il livello di maturità delle TIC dell'entità finanziaria o le caratteristiche tecnologiche in questione.

4. Previa consultazione della BCE e tenendo conto dei pertinenti quadri che, a livello di Unione, si applicano ai test di penetrazione basati su informazioni, l'ABE, l'ESMA e l'EIOPA elaborano progetti di norme tecniche di regolamentazione per specificare ulteriormente quanto segue:

(a) i criteri utilizzati ai fini dell'applicazione del paragrafo 6 del presente articolo;

(b) le prescrizioni concernenti:

(a) l'ambito dei test di penetrazione basati su minacce di cui al paragrafo 2 del presente articolo;

(b) l'approccio e la metodologia da seguire per i test in ciascuna fase del relativo processo;

(c) i risultati, la chiusura e le fasi correttive dei test;

(c) il tipo di cooperazione di vigilanza necessario per svolgere i test di penetrazione basati su minacce nel contesto di entità finanziarie che operano in più di uno Stato membro, per consentire un livello adeguato di partecipazione alla vigilanza, nonché un'attuazione flessibile per tener conto delle specificità dei sottosettori finanziari o dei mercati finanziari locali.

Le AEV presentano detti progetti di norme tecniche di regolamentazione alla Commissione entro il [*GU: inserire la data corrispondente a due mesi prima della data di entrata in vigore*].

Alla Commissione è delegato il potere di integrare il presente regolamento, adottando le norme tecniche di regolamentazione di cui al secondo comma in conformità, rispettivamente, degli articoli da 10 a 14 dei regolamenti (UE) n. 1093/2010, (UE) n. 1095/2010 e (UE) n. 1094/2010.

Articolo 24

Requisiti per i tester

1. Per lo svolgimento dei test di penetrazione basati su minacce le entità finanziarie si avvalgono unicamente di tester che:

   (a) possano vantare il più alto grado di idoneità e reputazione;

   (b) possiedano capacità tecniche e organizzative e dimostrino esperienza specifica nel campo delle informazioni sulle minacce, dei test di penetrazione o dei test red team;

   (c) siano certificati da un ente di accreditamento in uno Stato membro o rispettino codici formali di condotta o quadri etici;

   (d) nel caso di tester esterni, forniscano una garanzia indipendente o una relazione di audit concernente la solida gestione dei rischi derivanti dall'esecuzione di test di penetrazione basati su minacce, comprese un'adeguata protezione delle informazioni riservate dell'entità finanziaria e il risarcimento dei rischi commerciali dell'entità finanziaria;

   (e) nel caso di tester esterni, siano debitamente e pienamente coperti da un'assicurazione di responsabilità professionale, anche contro i rischi di colpa e negligenza.

2. Le entità finanziarie garantiscono che gli accordi conclusi con i tester esterni prevedano una solida gestione dei risultati dei test di penetrazione basati su minacce e che qualsiasi trattamento di tali risultati, comprese la generazione, l'elaborazione, la conservazione, l'aggregazione, la segnalazione, la comunicazione o la distruzione, non comporti rischi per l'entità finanziaria.

CAPO V

GESTIONE DEI RISCHI RELATIVI ALLE TIC DERIVANTI DA TERZI

SEZIONE I

PRINCIPI FONDAMENTALI DI UNA SOLIDA GESTIONE DEI RISCHI RELATIVI ALLE TIC DERIVANTI DA TERZI

Articolo 25

Principi generali

Le entità finanziarie trattano i rischi relativi alle TIC derivanti da terzi quali componenti integranti dei rischi relativi alle TIC nel contesto del proprio quadro per la gestione di detti rischi e conformemente ai principi indicati di seguito.

1. Le entità finanziarie che hanno stipulato accordi contrattuali per l'utilizzo di servizi di TIC per lo svolgimento delle proprie operazioni commerciali rimangono sempre pienamente responsabili del rispetto e dell'adempimento di tutti gli obblighi previsti dal presente regolamento e dalla legislazione applicabile in materia di servizi finanziari.

2. La gestione dei rischi relativi alle TIC derivanti da terzi da parte delle entità finanziarie si svolge nel rispetto del principio di proporzionalità, tenendo conto:

   (a) delle dimensioni, della complessità e dell'importanza delle dipendenze connesse alle TIC;

   (b) dei rischi derivanti dagli accordi contrattuali per l'utilizzo di servizi di TIC conclusi con fornitori terzi di servizi di TIC, tenendo conto della criticità o dell'importanza dei rispettivi servizi, processi o funzioni e del potenziale impatto sulla continuità e la qualità dei servizi finanziari a livello individuale e di gruppo.

3. Nel contesto del quadro per la gestione dei rischi relativi alle TIC, le entità finanziarie adottano e riesaminano periodicamente una strategia per i rischi relativi alle TIC derivanti da terzi, tenendo conto della strategia basata su una varietà di fornitori di cui all'articolo 5, paragrafo 9, lettera g). Tale strategia comprende una politica per l'utilizzo dei servizi di TIC prestati da fornitori terzi e si applica su base individuale e, se del caso, su base subconsolidata e consolidata. L'organo di gestione riesamina periodicamente i rischi identificati in relazione all'esternalizzazione di funzioni critiche o importanti.

4. Nel contesto del quadro per la gestione dei rischi relativi alle TIC, le entità finanziarie mantengono e aggiornano a livello di entità, e su base subconsolidata e consolidata, un registro di informazioni su tutti gli accordi contrattuali per l'utilizzo di servizi di TIC prestati da fornitori terzi.

   Gli accordi contrattuali di cui al primo comma sono opportunamente documentati, distinguendo quelli che si riferiscono a funzioni critiche o importanti dagli altri.

Le entità finanziarie comunicano almeno una volta all'anno alle autorità competenti informazioni sul numero di nuovi accordi per l'utilizzo di servizi di TIC, sulle categorie di fornitori terzi di servizi di TIC, sul tipo di accordi contrattuali e sulle funzioni e i servizi forniti.

Su richiesta, le entità finanziarie mettono a disposizione dell'autorità competente il registro delle informazioni completo o, a seconda della richiesta, determinate sezioni del registro insieme alle informazioni giudicate necessarie per consentire l'efficace vigilanza sull'entità finanziaria.

Le entità finanziarie informano tempestivamente l'autorità competente sui contratti previsti per funzioni critiche o importanti, nonché del momento in cui una funzione diventa critica o importante.

5. Prima di stipulare un accordo contrattuale per l'utilizzo di servizi di TIC, le entità finanziarie:

   (a) valutano se l'accordo contrattuale riguardi una funzione critica o importante;

   (b) verificano se siano soddisfatte le condizioni di vigilanza per la conclusione del contratto;

   (c) identificano e valutano tutti i rischi pertinenti relativi all'accordo contrattuale, compresa la possibilità che tali accordi contrattuali possano aggravare il rischio di concentrazione delle TIC;

   (d) effettuano controlli di dovuta diligenza sui potenziali fornitori terzi di servizi di TIC e ne garantiscono l'idoneità lungo tutto il processo di selezione e valutazione;

   (e) individuano e valutano i conflitti di interesse che possano derivare dall'accordo contrattuale.

6. Le entità finanziarie possono stipulare accordi contrattuali soltanto con fornitori terzi di servizi di TIC che soddisfano standard elevati, appropriati e recenti in materia di sicurezza delle informazioni.

7. Nell'esercizio dei diritti di accesso, ispezione e audit nei confronti del fornitore terzo di servizi di TIC, le entità finanziarie determinano, secondo un approccio basato sul rischio, la frequenza degli audit e delle ispezioni nonché i settori da sottoporre ad audit, aderendo a norme di audit comunemente accettate in conformità di eventuali istruzioni di vigilanza sull'uso e l'integrazione di tali norme di audit.

   Per gli accordi contrattuali che comportano un elevato livello di complessità tecnologica, l'entità finanziaria verifica che i revisori, indipendentemente dal fatto che siano revisori interni, gruppi di revisori, o revisori esterni, possiedano competenze e conoscenze adeguate per svolgere efficacemente gli audit e le valutazioni del caso.

8. Le entità finanziarie stabiliscono clausole che prevedano la risoluzione degli accordi contrattuali per l'utilizzazione di servizi di TIC almeno nelle seguenti circostanze:

   (a) violazione, da parte del fornitore terzo di servizi di TIC, di leggi, regolamenti o condizioni contrattuali applicabili;

   (b) circostanze, identificate nel corso del monitoraggio dei rischi relativi alle TIC derivanti da terzi, ritenute suscettibili di alterare l'esercizio delle funzioni

previsto a norma dell'accordo contrattuale, tra cui modifiche di rilievo che incidano sull'accordo o sulla situazione del fornitore terzo di servizi di TIC;

(c) punti deboli del fornitore terzo di servizi di TIC emersi nella gestione complessiva dei rischi relativi alle TIC e, in particolare, nel modo in cui il fornitore garantisce la sicurezza e l'integrità di dati riservati, personali o altrimenti sensibili, oppure di informazioni non personali;

(d) circostanze in cui l'autorità competente non sia più in grado di vigilare efficacemente sull'entità finanziaria in conseguenza dell'accordo contrattuale in questione.

9. Le entità finanziarie predispongono strategie di uscita per tener conto dei rischi che possono emergere a livello del fornitore terzo di servizi di TIC, in particolare possibili disfunzioni del fornitore, il deterioramento della qualità delle funzioni assolte, una perturbazione dell'attività commerciale conseguente a una fornitura di servizi inadeguata o carente, oppure gravi rischi connessi all'adeguatezza e alla continuità dell'esercizio della funzione.

Le entità finanziarie garantiscono di poter estinguere gli accordi contrattuali senza:

(a) perturbare le proprie attività commerciali;

(b) limitare il rispetto delle prescrizioni normative;

(c) pregiudicare la continuità e la qualità della prestazione dei servizi ai clienti.

I piani di uscita sono esaustivi, documentati e, se del caso, sottoposti a test adeguati.

Le entità finanziarie identificano soluzioni alternative ed elaborano piani di transizione che consentano loro di togliere le funzioni previste dal contratto e i relativi dati al fornitore terzo di servizi di TIC, trasferendoli in maniera sicura e nella loro interezza a fornitori alternativi oppure reintegrandoli al proprio interno.

Le entità finanziarie adottano misure di emergenza idonee per mantenere la continuità operativa in tutte le circostanze di cui al primo comma.

10. Le AEV, tramite il comitato congiunto, elaborano progetti di norme tecniche di attuazione per definire modelli standard ai fini del registro delle informazioni di cui al paragrafo 4.

Le AEV presentano tali progetti di norme tecniche di attuazione alla Commissione entro il [*GU: inserire la data corrispondente a 1 anno dopo la data di entrata in vigore del presente regolamento*].

Alla Commissione è conferito il potere di adottare le norme tecniche di attuazione di cui al primo comma in conformità, rispettivamente, dell'articolo 15 dei regolamenti (UE) n. 1093/2010, (UE) n. 1095/2010 e (UE) n. 1094/2010.

11. Le AEV, tramite il comitato congiunto, elaborano progetti di norme di regolamentazione:

(a) per precisare ulteriormente il contenuto dettagliato della politica di cui al paragrafo 3, in relazione agli accordi contrattuali per l'utilizzo di servizi di TIC prestati da fornitori terzi, con riferimento alle fasi principali del ciclo di vita dei rispettivi accordi per l'utilizzo dei servizi di TIC;

(b) i tipi di informazioni da includere nel registro delle informazioni di cui al paragrafo 4.

Le AEV presentano detti progetti di norme tecniche di regolamentazione alla Commissione entro il [*PO: inserire la data corrispondente a un anno dopo la data di entrata in vigore*].

Alla Commissione è delegato il potere di integrare il presente regolamento, adottando le norme tecniche di regolamentazione di cui al secondo comma in conformità, rispettivamente, degli articoli da 10 a 14 dei regolamenti (UE) n. 1093/2010, (UE) n. 1095/2010 e (UE) n. 1094/2010.

Articolo 26

Valutazione preliminare del rischio di concentrazione delle TIC e ulteriori accordi di subesternalizzazione

1. Al momento di identificare e valutare il rischio di concentrazione delle TIC di cui all'articolo 25, paragrafo 5, lettera c), le entità finanziarie tengono conto dell'eventualità che la conclusione di un accordo contrattuale relativo ai servizi di TIC possa avere una delle seguenti conseguenze:

   (a) la conclusione di un contratto con un fornitore terzo di servizi di TIC non facilmente sostituibile; o

   (b) la presenza di molteplici accordi contrattuali relativi alla prestazione di servizi di TIC con lo stesso fornitore terzo oppure con fornitori terzi strettamente connessi.

   Le entità finanziarie vagliano i benefici e i costi di soluzioni alternative, quali il ricorso a diversi fornitori terzi di servizi di TIC, verificando se e come le soluzioni previste soddisfino le esigenze commerciali e consentano di conseguire gli obiettivi fissati nella propria strategia di resilienza digitale.

2. Qualora l'accordo contrattuale per l'utilizzo di servizi di TIC preveda la possibilità che un fornitore terzo di servizi di TIC subappalti a sua volta una funzione importante o critica ad altri fornitori terzi di servizi di TIC, le entità finanziarie vagliano i benefici e i rischi che possono derivare da tale potenziale subappalto, in particolare nel caso di un subappaltatore di TIC stabilito in un paese terzo.

   Qualora gli accordi contrattuali per l'utilizzo di servizi di TIC siano conclusi con un fornitore terzo stabilito in un paese terzo, le entità finanziarie considerano rilevanti almeno i fattori seguenti:

   (a) il rispetto della protezione dei dati;

   (b) l'effettiva applicazione della legge;

   (c) le disposizioni del diritto fallimentare applicabili in caso di fallimento del fornitore terzo di servizi di TIC;

   (d) eventuali restrizioni relative all'urgente ripristino dei dati dell'entità finanziaria.

   Le entità finanziarie valutano se e come catene di subappalti potenzialmente lunghe e complesse possano incidere sulla loro capacità di monitorare pienamente le funzioni appaltate e sulla capacità dell'autorità competente di vigilare efficacemente, a tal proposito, sull'entità finanziaria.

Articolo 27

Principali disposizioni contrattuali

1. I diritti e gli obblighi dell'entità finanziaria e del fornitore terzo di servizi di TIC sono attribuiti chiaramente e definiti per iscritto. Il testo integrale del contratto, comprendente gli accordi sul livello dei servizi, è contenuto in un documento scritto disponibile alle parti in formato cartaceo o in un formato scaricabile e accessibile.

2. Gli accordi contrattuali per l'utilizzo di servizi di TIC comprendono almeno i seguenti elementi:

   (a) la descrizione chiara e completa di tutte le funzioni che il fornitore terzo di servizi di TIC deve svolgere e tutti i servizi che deve prestare, comprese l'indicazione dell'eventuale autorizzazione a subappaltare una funzione critica o importante o parti significative di essa e, in caso affermativo, le condizioni di tale subappalto;

   (b) le località in cui si devono esercitare le funzioni e prestare i servizi appaltati o subappaltati e in cui si devono trattare i dati, compreso il luogo di conservazione, nonché l'obbligo, per il fornitore terzo di servizi di TIC, di segnalare all'entità finanziaria l'intenzione di cambiare tali località;

   (c) le disposizioni in materia di accessibilità, disponibilità, integrità, sicurezza e protezione dei dati personali, nonché le garanzie di accesso, ripristino e restituzione, in un formato facilmente accessibile, di dati personali e non personali trattati dall'entità finanziaria in caso di insolvenza, risoluzione o interruzione delle operazioni commerciali del fornitore terzo di servizi di TIC;

   (d) la descrizione completa dei livelli di servizio, comprendente i relativi aggiornamenti e revisioni, nonché precisi obiettivi quantitativi e qualitativi, in termini di prestazioni, nell'ambito dei livelli di servizio concordati, in modo da consentire un monitoraggio effettivo da parte dell'entità finanziaria e l'applicazione immediata di opportune azioni correttive qualora i livelli di servizio concordati non siano rispettati;

   (e) termini di preavviso e obblighi di segnalazione per il fornitore terzo di servizi di TIC nei confronti dell'entità finanziaria, tra cui la notifica di eventuali sviluppi che possano esercitare un impatto significativo sulla capacità del fornitore terzo di servizi di TIC di svolgere efficacemente funzioni importanti o critiche conformemente ai livelli di servizio concordati;

   (f) l'obbligo per il fornitore terzo di servizi di TIC di fornire assistenza in caso di incidente connesso alle TIC, senza costi supplementari oppure a un costo stabilito ex ante;

   (g) l'obbligo per il fornitore terzo di servizi di TIC di attuare e testare i piani operativi d'emergenza e di predisporre misure, strumenti e politiche per la sicurezza delle TIC che garantiscano adeguatamente la prestazione sicura dei servizi da parte dell'entità finanziaria, conformemente al proprio quadro normativo;

   (h) il diritto di monitorare costantemente le prestazioni del fornitore terzo di servizi di TIC, tra cui:

      i) diritti di accesso, ispezione e audit da parte dell'entità finanziaria o di un terzo designato a tal fine, nonché il diritto di ottenere copia della

documentazione pertinente, il cui effettivo esercizio non sia impedito o limitato da altri accordi contrattuali o politiche di attuazione;

ii) il diritto di concordare livelli di garanzia alternativi, qualora siano interessati i diritti di altri clienti;

iii) l'impegno a cooperare senza riserve nel corso delle ispezioni in loco svolte dall'entità finanziaria e a fornire dettagli sull'ambito di applicazione, le modalità e la frequenza degli audit a distanza;

(i) l'obbligo per il fornitore terzo di servizi di TIC di cooperare senza riserve con le autorità competenti e con le autorità di risoluzione dell'entità finanziaria, comprese le persone da queste nominate;

(j) i diritti di risoluzione e i relativi termini minimi di preavviso per la risoluzione del contratto, conformemente alle attese delle autorità competenti;

(k) le strategie di uscita, in particolare la definizione di un adeguato periodo di transizione obbligatorio:

(a) durante il quale il fornitore terzo di servizi di TIC continuerà a prestare i suoi servizi e a esercitare le sue funzioni allo scopo di ridurre il rischio di perturbazioni presso l'entità finanziaria;

(b) che permetta all'entità finanziaria di passare a un altro fornitore terzo di servizi di TIC oppure di adottare soluzioni interne coerenti con la complessità del servizio prestato.

3. Al momento di negoziare gli accordi contrattuali, le entità finanziarie e i fornitori terzi di servizi di TIC prendono in considerazione il ricorso a clausole contrattuali standard elaborate per servizi specifici.

4. Le AEV, tramite il comitato congiunto, elaborano progetti di norme tecniche di regolamentazione per specificare ulteriormente gli elementi che l'entità finanziaria deve determinare e valutare quando subappalta funzioni critiche o importanti, in modo da attuare adeguatamente le disposizioni di cui al paragrafo 2, lettera a).

Le AEV presentano detti progetti di norme tecniche di regolamentazione alla Commissione entro il [*GU: inserire la data corrispondente a un anno dopo la data di entrata in vigore*].

Alla Commissione è delegato il potere di integrare il presente regolamento, adottando le norme tecniche di regolamentazione di cui al primo comma in conformità, rispettivamente, degli articoli da 10 a 14 dei regolamenti (UE) n. 1093/2010, (UE) n. 1095/2010 o (UE) n. 1094/2010.

SEZIONE II

QUADRO DI SORVEGLIANZA DEI FORNITORI TERZI DI SERVIZI DI TIC CRITICI

Articolo 28

Designazione dei fornitori terzi di servizi di TIC critici

1. Le AEV, tramite il comitato congiunto e su raccomandazione del forum di sorveglianza istituito ai sensi dell'articolo 29, paragrafo 1:

(a) designano i fornitori terzi di servizi di TIC che sono critici per le entità finanziarie, tenendo conto dei criteri specificati al paragrafo 2;

(b) nominano l'ABE, l'ESMA o l'EIOPA quale autorità di sorveglianza capofila di ciascun fornitore terzo di servizi di TIC critico, a seconda che il valore totale delle attività delle entità finanziarie che utilizzano i servizi di quel determinato fornitore terzo di servizi di TIC critico e che rientrano nell'ambito di applicazione di uno dei regolamenti (UE) n. 1093/2010, (UE) n. 1094/2010 o (UE) n. 1095/2010 rappresenti più della metà del valore delle attività totali di tutte le entità finanziarie che utilizzano i servizi del fornitore terzo di servizi di TIC critico, secondo quanto risulta dai bilanci consolidati (o dai singoli bilanci qualora questi non siano consolidati) di quelle entità finanziarie.

2. La designazione di cui al paragrafo 1, lettera a), si fonda su tutti i criteri indicati di seguito:

(a) l'impatto sistemico sulla stabilità, la continuità o la qualità della fornitura di servizi finanziari qualora il fornitore terzo di servizi di TIC pertinente sia interessato da una disfunzione operativa su vasta scala che gli impedisca di fornire i suoi servizi, tenendo conto del numero di entità finanziarie cui quel fornitore terzo di servizi di TIC presta servizi;

(b) il carattere sistemico o l'importanza delle entità finanziarie che dipendono da quel fornitore terzo di servizi di TIC, valutati in conformità dei parametri seguenti:

i) il numero di enti a rilevanza sistemica a livello globale (G-SII) o di altri enti a rilevanza sistemica (O-SII) che dipendono dal rispettivo fornitore terzo di servizi di TIC;

ii) l'interdipendenza tra i G-SII o gli O-SII di cui al punto i) e altre entità finanziarie, comprese le situazioni in cui i G-SII o gli O-SII prestano servizi finanziari infrastrutturali ad altre entità finanziarie;

(c) la dipendenza delle entità finanziarie dai servizi prestati dal pertinente fornitore terzo di servizi di TIC in rapporto alle funzioni critiche o importanti delle entità finanziarie che in ultima analisi coinvolgono quel medesimo fornitore terzo di servizi di TIC, indipendentemente dal fatto che le entità finanziarie dipendano da tali servizi direttamente o indirettamente, mediante accordi di subappalto;

(d) il grado di sostituibilità del fornitore terzo di servizi di TIC, prendendo in considerazione i parametri seguenti:

i) la mancanza di alternative reali, anche parziali, dovuta al limitato numero di fornitori terzi di servizi di TIC attivi su un mercato specifico, alla quota di mercato del fornitore terzo di servizi di TIC in questione, o ancora alla complessità tecnica o al grado di sofisticazione, anche in relazione a eventuali tecnologie proprietarie, o alle caratteristiche specifiche dell'organizzazione o dell'attività del fornitore terzo di servizi di TIC;

ii) difficoltà di migrare i dati e i carichi di lavoro, in tutto o in parte, dal fornitore terzo di servizi di TIC in questione a un altro, a causa dei cospicui costi finanziari, del tempo o di altri tipi di risorse che possono essere necessarie per il processo di migrazione, oppure dei maggiori

rischi relativi alle TIC o di altri rischi operativi cui l'entità finanziaria può esporsi a causa di tale migrazione;

(e) il numero di Stati membri in cui il fornitore terzo di servizi di TIC presta i suoi servizi;

(f) il numero di Stati membri in cui operano le entità finanziarie che si avvalgono del fornitore terzo di servizi di TIC in questione.

3. Alla Commissione è conferito il potere di adottare atti delegati conformemente all'articolo 50 per integrare i criteri di cui al paragrafo 2.

4. Il meccanismo di designazione di cui al paragrafo 1, lettera a), non è utilizzato fino a quando la Commissione non abbia adottato un atto delegato in conformità del paragrafo 3.

5. Il meccanismo di designazione di cui al paragrafo 1, lettera a), non si applica in relazione ai fornitori terzi di servizi di TIC che sono soggetti a quadri di sorveglianza istituiti a supporto dei compiti di cui all'articolo 127, paragrafo 2, del trattato sul funzionamento dell'Unione europea.

6. Le AEV, tramite il comitato congiunto, redigono, pubblicano e aggiornano ogni anno l'elenco dei fornitori terzi di servizi di TIC critici a livello di Unione europea.

7. Ai fini del paragrafo 1, lettera a), le autorità competenti trasmettono, con cadenza annuale e in forma aggregata, le relazioni di cui all'articolo 25, paragrafo 4, al forum di sorveglianza istituito ai sensi dell'articolo 29. Il forum di sorveglianza valuta la dipendenza delle entità finanziarie da terzi nel settore delle TIC sulla base delle informazioni ricevute dalle autorità competenti.

8. I fornitori terzi di servizi di TIC che non sono inseriti nell'elenco di cui al paragrafo 6 possono chiedere di esservi inseriti.

Ai fini del primo comma, il fornitore terzo di servizi di TIC presenta una domanda motivata all'ABE, all'ESMA o all'EIOPA; queste ultime, tramite il comitato congiunto, decidono se inserire tale fornitore terzo di servizi di TIC nell'elenco conformemente al paragrafo 1, lettera a).

La decisione di cui al secondo comma è adottata e notificata al fornitore terzo di servizi di TIC entro sei mesi dalla data in cui è stata ricevuta la domanda.

9. Le entità finanziarie non ricorrono a un fornitore terzo di servizi di TIC stabilito in un paese terzo che sarebbe designato come critico ai sensi del paragrafo 1, lettera a), se fosse stabilito all'interno dell'Unione.

Articolo 29

Struttura del quadro di sorveglianza

1. Il comitato congiunto, in conformità dell'articolo 57 dei regolamenti (UE) n. 1093/2010, (UE) n. 1094/2010 o (UE) n. 1095/2010, istituisce il forum di sorveglianza come sottocomitato incaricato di coadiuvare il lavoro del comitato congiunto e dell'autorità di sorveglianza capofila di cui all'articolo 28, paragrafo 1, lettera b), per quanto concerne i rischi relativi alle TIC derivanti da terzi in tutti i settori finanziari. Il forum di sorveglianza prepara i progetti di posizioni comuni e atti comuni del comitato congiunto in questo campo.

Il forum di sorveglianza discute periodicamente gli sviluppi rilevanti in materia di vulnerabilità e rischi relativi alle TIC e promuove un approccio coerente al monitoraggio dei rischi relativi alle TIC derivanti da terzi su scala dell'Unione.

2. Il forum di sorveglianza intraprende, con cadenza annuale, una valutazione collettiva degli esiti e delle risultanze delle attività di sorveglianza condotte su tutti i fornitori terzi di servizi di TIC critici e promuove misure di coordinamento per potenziare la resilienza operativa digitale delle entità finanziarie, favorire le migliori pratiche per contrastare il rischio di concentrazione delle TIC e studiare metodi per attenuare il trasferimento intersettoriale dei rischi.

3. Il forum di sorveglianza sottopone al comitato congiunto parametri di riferimento globali per i fornitori terzi di servizi di TIC critici affinché siano adottati come posizioni congiunte delle AEV ai sensi dell'articolo 56, paragrafo 1, dei regolamenti (UE) n. 1093/2010, (UE) n. 1094/2010 e (UE) n. 1095/2010.

4. Il forum di sorveglianza è composto dai presidenti delle AEV e da un rappresentante di alto livello del personale in servizio dell'autorità competente interessata di ciascuno Stato membro. I direttori esecutivi di ciascuna AEV e un rappresentante della Commissione europea, del CERS, della BCE e dell'ENISA partecipano al forum di sorveglianza in qualità di osservatori.

5. Ai sensi dell'articolo 16 dei regolamenti (UE) n. 1093/2010, (UE) n. 1094/2010 e (UE) n. 1095/2010, le AEV formulano orientamenti sulla cooperazione tra le AEV e le autorità competenti, ai fini della presente sezione, sulle procedure e le condizioni dettagliate relative alla ripartizione dei compiti tra le autorità competenti e le AEV, nonché forniscono dettagli sullo scambio di informazioni necessario alle autorità competenti per garantire il seguito da dare alle raccomandazioni inviate dall'autorità di sorveglianza capofila ai fornitori terzi di servizi di TIC critici a norma dell'articolo 31, paragrafo 1, lettera d).

6. Le prescrizioni di cui alla presente sezione non pregiudicano l'applicazione della direttiva (UE) 2016/1148 né di altre norme dell'Unione in materia di sorveglianza applicabili ai fornitori di servizi di cloud computing.

7. Sulla base di un lavoro preparatorio svolto dal forum di sorveglianza, le AEV, tramite il comitato congiunto, presentano ogni anno una relazione sull'applicazione della presente sezione al Parlamento europeo, al Consiglio e alla Commissione.

Articolo 30

Compiti dell'autorità di sorveglianza capofila

1. L'autorità di sorveglianza capofila valuta se ciascun fornitore terzo di servizi di TIC critico abbia predisposto norme, procedure, meccanismi e accordi esaustivi, solidi ed efficaci per gestire i rischi relativi alle TIC cui esso può esporre le entità finanziarie.

2. La valutazione di cui al paragrafo 1 include almeno:

(a) prescrizioni in materia di TIC atte a garantire, in particolare, la sicurezza, la disponibilità, la continuità, la scalabilità e la qualità dei servizi che il fornitore terzo di servizi di TIC critico presta alle entità finanziarie, nonché la capacità di mantenere standard di sicurezza, riservatezza e integrità dei dati costantemente elevati;

(b) la sicurezza fisica che contribuisce a mantenere la sicurezza delle TIC, compresa la sicurezza dei locali, delle attrezzature e dei centri dati;

(c) i processi di gestione del rischio, comprese le politiche di gestione dei rischi relativi alle TIC, i piani per la continuità operativa delle TIC e per il piano di ripristino in caso di disastro relativo alle TIC;

(d) le disposizioni di governance, compresa una struttura organizzativa dotata di linee e norme in materia di responsabilità chiare, trasparenti e coerenti che consentano un'efficace gestione dei rischi relativi alle TIC;

(e) l'identificazione, il monitoraggio e la tempestiva segnalazione alle entità finanziarie degli incidenti connessi alle TIC, la gestione e la risoluzione di tali incidenti, in particolare degli attacchi informatici;

(f) i meccanismi per la portabilità dei dati, la portabilità delle applicazioni e l'interoperabilità, per assicurare un effettivo esercizio dei diritti di risoluzione da parte delle entità finanziarie;

(g) i test dei sistemi, delle infrastrutture e dei controlli relativi alle TIC;

(h) gli audit in materia di TIC;

(i) l'utilizzo delle pertinenti norme nazionali e internazionali applicabili alla fornitura dei servizi di TIC alle entità finanziarie.

3. Sulla base della valutazione di cui al paragrafo 1, l'autorità di sorveglianza capofila adotta un piano di sorveglianza individuale, chiaro, dettagliato e motivato per ciascun fornitore terzo di servizi di TIC critico. Tale piano è comunicato ogni anno al fornitore terzo di servizi di TIC critico.

4. Allorché i piani di sorveglianza annuali di cui al paragrafo 3 sono stati concordati e notificati ai fornitori terzi di servizi di TIC critici, le autorità competenti possono adottare misure concernenti i fornitori terzi di servizi di TIC critici soltanto in accordo con l'autorità di sorveglianza capofila.

Articolo 31

Poteri dell'autorità di sorveglianza capofila

1. Ai fini dello svolgimento dei compiti previsti dalla presente sezione, all'autorità di sorveglianza capofila sono conferiti i poteri indicati di seguito:

(a) richiedere tutte le informazioni e la documentazione pertinenti ai sensi dell'articolo 32;

(b) condurre indagini e ispezioni di carattere generale ai sensi degli articoli 33 e 34;

(c) richiedere relazioni dopo il completamento delle attività di sorveglianza, in cui si specifichino le azioni adottate o i rimedi applicati da parte dei fornitori terzi di servizi di TIC critici in relazione alle raccomandazioni di cui alla lettera d) del presente paragrafo;

(d) formulare raccomandazioni concernenti i settori di cui all'articolo 30, paragrafo 2, in particolare per quanto riguarda gli elementi indicati di seguito:

i) l'impiego di specifici processi o requisiti di sicurezza e qualità delle TIC, soprattutto per l'introduzione di correzioni, aggiornamenti, cifratura e

altre misure di sicurezza che l'autorità di sorveglianza capofila giudichi pertinenti per garantire la sicurezza a livello di TIC dei servizi forniti alle entità finanziarie;

ii) l'uso di termini e condizioni, compresa la relativa attuazione tecnica, in base ai quali i fornitori terzi di servizi di TIC critici prestano servizi alle entità finanziarie, che l'autorità di sorveglianza capofila giudichi importanti per prevenire il prodursi di singoli punti di guasto o l'amplificazione degli stessi, oppure per ridurre al minimo il possibile impatto sistemico in tutto il settore finanziario dell'Unione in caso di rischio di concentrazione delle TIC;

iii) al momento dell'esame degli accordi di subappalto, intrapreso conformemente agli articoli 32 e 33, compresi gli accordi di subesternalizzazione che i fornitori terzi di servizi di TIC critici intendano stipulare con altri fornitori terzi di servizi di TIC o con subappaltatori di TIC stabiliti in un paese terzo, eventuali subappalti previsti, compresa la subesternalizzazione, ove l'autorità di sorveglianza capofila ritenga che ulteriori subappalti possano produrre rischi per la fornitura di servizi da parte dell'entità finanziaria o rischi per la stabilità finanziaria;

iv) la rinuncia a stipulare un ulteriore accordo di subappalto qualora siano soddisfatte le condizioni cumulative seguenti:

– il subappaltatore designato è un fornitore terzo di servizi di TIC oppure un subappaltatore di TIC stabilito in un paese terzo;

– il subappalto riguarda una funzione critica o importante dell'entità finanziaria.

2. L'autorità di sorveglianza capofila consulta il forum di sorveglianza prima di esercitare i poteri di cui al paragrafo 1.

3. I fornitori terzi di servizi di TIC critici cooperano in buona fede con l'autorità di sorveglianza capofila e la coadiuvano nell'adempimento dei suoi compiti.

4. L'autorità di sorveglianza capofila può imporre una penalità di mora, al fine di costringere il fornitore terzo di servizi di TIC critico a rispettare il paragrafo 1, lettere a), b) e c).

5. La penalità di mora, di cui al paragrafo 4, è imposta su base giornaliera fino al conseguimento della conformità e per un periodo non superiore a sei mesi dalla notifica al fornitore terzo di servizi di TIC critico.

6. L'importo della penalità di mora, calcolato a partire dalla data indicata nella decisione che la impone, è pari all'1 % del fatturato medio quotidiano realizzato a livello mondiale dal fornitore terzo di servizi di TIC critico nel precedente esercizio.

7. Le penalità sono di natura amministrativa e sono esecutive. L'applicazione delle penalità è regolata dalle norme di procedura civile vigenti nello Stato membro sul cui territorio si svolgono le ispezioni e l'accesso. I giudici dello Stato membro interessato esercitano la giurisdizione sui reclami concernenti l'irregolarità dell'applicazione delle penalità. Gli importi delle penalità sono assegnati al bilancio generale dell'Unione europea.

8. Le AEV comunicano al pubblico ogni penalità di mora inflitta, salvo il caso in cui tale comunicazione possa mettere gravemente a rischio i mercati finanziari o possa arrecare un danno sproporzionato alle parti coinvolte.

9. Prima di imporre una penalità di mora ai sensi del paragrafo 4, l'autorità di sorveglianza capofila concede ai rappresentanti del fornitore terzo di servizi di TIC critico oggetto del procedimento l'opportunità di essere sentito in merito alle risultanze, e fonda le proprie decisioni unicamente sulle risultanze in merito alle quali il fornitore terzo di servizi di TIC critico oggetto del procedimento ha avuto la possibilità di esporre le proprie osservazioni. Nel corso del procedimento sono pienamente garantiti i diritti della difesa delle persone interessate dal procedimento. Tali persone hanno diritto di accesso al fascicolo, fermo restando il legittimo interesse di altre persone alla tutela dei propri segreti aziendali. Il diritto di accesso al fascicolo non si estende alle informazioni riservate o ai documenti preparatori interni dell'autorità di sorveglianza capofila.

Articolo 32
Richiesta di informazioni

1. L'autorità di sorveglianza capofila può, con semplice richiesta o mediante decisione, imporre ai fornitori terzi di servizi di TIC critici di trasmettere tutte le informazioni necessarie all'autorità di sorveglianza capofila per adempiere i propri compiti ai sensi del presente regolamento, tra cui tutti i pertinenti documenti aziendali od operativi, contratti, documentazione strategica, relazioni di audit sulla sicurezza delle TIC, segnalazioni di incidenti connessi alle TIC, nonché qualsiasi informazione relativa ai soggetti cui il fornitore terzo di servizi di TIC critico ha esternalizzato attività o funzioni operative.

2. Quando invia una semplice richiesta di informazioni a norma del paragrafo 1, l'autorità di sorveglianza capofila:

   (a) fa riferimento al presente articolo quale base giuridica della richiesta;

   (b) dichiara la finalità della richiesta;

   (c) specifica le informazioni richieste;

   (d) stabilisce un termine entro il quale tali informazioni devono pervenirle;

   (e) informa il rappresentante del fornitore terzo di servizi di TIC critico cui sono richieste le informazioni che non è tenuto a fornirle, ma che in caso di risposta volontaria alla richiesta di informazioni, tali informazioni non devono essere inesatte né fuorvianti.

3. Quando impone la comunicazione di informazioni a norma del paragrafo 1, l'autorità di sorveglianza capofila:

   (a) fa riferimento al presente articolo quale base giuridica della richiesta;

   (b) dichiara la finalità della richiesta;

   (c) specifica le informazioni richieste;

   (d) stabilisce un termine entro il quale tali informazioni devono pervenirle;

   (e) indica le penalità di mora di cui all'articolo 31, paragrafo 4, laddove le informazioni fornite siano incomplete;

(f) indica il diritto di presentare ricorso contro la decisione dinanzi alla commissione di ricorso dell'AEV e di adire la Corte di giustizia dell'Unione europea ("Corte di giustizia") conformemente agli articoli 60 e 61 dei regolamenti (UE) n. 1093/2010, (UE) n. 1094/2010 o (UE) n. 1095/2010.

4. I rappresentanti dei fornitori terzi di servizi di TIC critici forniscono le informazioni richieste. Gli avvocati debitamente incaricati possono fornire le informazioni richieste a nome dei loro clienti. I fornitori terzi di servizi di TIC critici sono pienamente responsabili qualora le informazioni fornite siano incomplete, inesatte o fuorvianti.

5. L'autorità di sorveglianza capofila invia senza indugio copia della decisione di fornire informazioni alle autorità competenti delle entità finanziarie che utilizzano i servizi dei fornitori terzi di servizi di TIC critici.

Articolo 33
Indagini generali

1. Per adempiere i propri compiti ai sensi del presente regolamento, l'autorità di sorveglianza capofila, coadiuvata dal gruppo di esaminatori di cui all'articolo 34, paragrafo 1, può svolgere le necessarie indagini sui fornitori terzi di servizi di TIC.

2. All'autorità di sorveglianza capofila sono conferiti i poteri di:

(a) esaminare registri, dati, procedure e qualsiasi altro materiale pertinente per l'esecuzione dei compiti di sua competenza, su qualsiasi forma di supporto;

(b) fare od ottenere copie certificate o estratti di tali registri, dati, procedure e altro materiale;

(c) convocare rappresentanti del fornitore terzo di servizi di TIC e chiedere loro spiegazioni scritte od orali su fatti o documenti relativi all'oggetto e alle finalità dell'indagine e registrarne le risposte;

(d) interpellare persone fisiche o giuridiche consenzienti allo scopo di raccogliere informazioni pertinenti all'oggetto dell'indagine;

(e) richiedere la documentazione relativa al traffico telefonico e al traffico dati.

3. I funzionari e altre persone autorizzate dall'autorità di sorveglianza capofila allo svolgimento dell'indagine di cui al paragrafo 1 esercitano i loro poteri dietro esibizione di un'autorizzazione scritta che specifichi l'oggetto e le finalità dell'indagine.

Tale autorizzazione indica anche la penalità di mora, di cui all'articolo 31, paragrafo 4, qualora i registri, i dati, le procedure o qualsiasi altro materiale richiesto, oppure le risposte alle domande poste ai rappresentanti del fornitore terzo di servizi di TIC, siano incompleti o non siano forniti affatto.

4. I rappresentanti dei fornitori terzi di servizi di TIC sono tenuti a sottoporsi alle indagini sulla base di una decisione dell'autorità di sorveglianza capofila. La decisione specifica l'oggetto e le finalità dell'indagine nonché le penalità di mora di cui all'articolo 31, paragrafo 4, i mezzi di ricorso disponibili ai sensi dei regolamenti (UE) n. 1093/2010, (UE) n. 1094/2010 o (UE) n. 1095/2010 e il diritto di ricorso dinanzi alla Corte di giustizia.

5. In tempo utile prima dell'indagine, le autorità di sorveglianza capofila informano le autorità competenti delle entità finanziarie che si avvalgono del fornitore terzo di

servizi di TIC in questione in merito all'indagine e all'identità delle persone autorizzate.

Articolo 34
Ispezioni in loco

1. Per adempiere i propri compiti ai sensi del presente regolamento, l'autorità di sorveglianza capofila può, coadiuvata dai gruppi di esaminatori di cui all'articolo 35, paragrafo 1, accedere a locali commerciali, immobili o proprietà dei fornitori terzi di servizi di TIC, come sedi centrali, centri operativi, sedi secondarie, per condurvi tutte le necessarie ispezioni in loco; può inoltre effettuare ispezioni off-line.

2. I funzionari e altre persone autorizzate dall'autorità di sorveglianza capofila a effettuare l'ispezione in loco possono accedere ai predetti locali commerciali, immobili o proprietà e dispongono del completo potere di sigillare locali e libri o registri per il periodo dell'ispezione e nella misura necessaria per effettuarla.

   Esercitano i loro poteri dietro esibizione di un'autorizzazione scritta che specifichi l'oggetto e le finalità dell'ispezione nonché le penalità di mora di cui all'articolo 31, paragrafo 4, qualora i rappresentanti dei fornitori terzi di servizi di TIC interessati non si sottopongano all'indagine.

3. In tempo utile prima dell'ispezione, l'autorità di sorveglianza capofila informa le autorità competenti delle entità finanziarie che si avvalgono di quel fornitore terzo di servizi di TIC.

4. Le ispezioni si estendono all'intera gamma di sistemi, reti, dispositivi, informazioni e dati in materia di TIC utilizzati per la fornitura dei servizi alle entità finanziarie, o che vi contribuiscono.

5. Prima di qualsiasi visita in loco programmata, l'autorità di sorveglianza capofila concede un ragionevole preavviso ai fornitori terzi di servizi di TIC critici, a meno che tale preavviso si riveli impossibile per una situazione di emergenza o di crisi, o qualora il preavviso rischi di provocare una situazione in cui l'ispezione o l'audit non sarebbero più efficaci.

6. Il fornitore terzo di servizi di TIC critico si sottopone alle ispezioni in loco ordinate con decisione dell'autorità di sorveglianza capofila. La decisione specifica l'oggetto e le finalità dell'ispezione, precisa la data d'inizio e indica le penalità di mora di cui all'articolo 31, paragrafo 4, i mezzi di ricorso disponibili a norma dei regolamenti (UE) n. 1093/2010, (UE) n. 1094/2010 o (UE) n. 1095/2010, nonché il diritto di adire la Corte di giustizia.

7. Qualora i funzionari e altre persone autorizzate dall'autorità di sorveglianza capofila constatino che il fornitore terzo di servizi di TIC critico si oppone all'ispezione ordinata ai sensi del presente articolo, l'autorità di sorveglianza capofila informa il fornitore terzo di servizi di TIC critico delle conseguenze di tale opposizione, compresa la possibilità per le autorità competenti delle entità finanziarie interessate di risolvere gli accordi contrattuali stipulati con il fornitore terzo di servizi di TIC critico.

Articolo 35

Sorveglianza costante

1. Nello svolgimento di indagini generali o di ispezioni in loco, le autorità di sorveglianza capofila sono coadiuvate da un gruppo di esaminatori istituito per ciascun fornitore terzo di servizi di TIC critico.

2. Il gruppo di esaminatori congiunto di cui al paragrafo 1 è composto da membri del personale dell'autorità di sorveglianza capofila e delle autorità competenti che vigilano sulle entità finanziarie cui il fornitore terzo di servizi di TIC critico presta servizi, che parteciperanno alla preparazione e allo svolgimento delle attività di sorveglianza, con un massimo di 10 membri. Tutti i membri del gruppo di esaminatori congiunto possiedono competenze in materia di TIC e rischi operativi. Il gruppo di esaminatori congiunto è coordinato da un membro del personale dell'AEV designato a tale scopo (il "coordinatore dell'autorità di sorveglianza capofila").

3. Le AEV, tramite il comitato congiunto, elaborano un progetto di norme tecniche di regolamentazione comuni per specificare ulteriormente la nomina dei membri del gruppo di esaminatori congiunto provenienti dalle autorità competenti, nonché i compiti e le modalità di lavoro del gruppo di esaminatori. Le AEV presentano detti progetti di norme tecniche di regolamentazione alla Commissione entro il [*GU: inserire la data corrispondente a un anno dopo la data di entrata in vigore*].

   Alla Commissione è delegato il potere di adottare le norme tecniche di regolamentazione di cui al primo comma conformemente agli articoli da 10 a 14 dei regolamenti (UE) n. 1093/2010, (UE)n. 1094/2010 e (UE) n. 1095/2010.

4. Entro tre mesi dal completamento dell'indagine o dell'ispezione in loco, l'autorità di sorveglianza capofila, dopo essersi consultata con il forum di sorveglianza, adotta le raccomandazioni da inviare al fornitore terzo di servizi di TIC critico in forza dei poteri che le sono stati conferiti ai sensi dell'articolo 31.

5. Le raccomandazioni di cui al paragrafo 4 sono comunicate immediatamente al fornitore terzo di servizi di TIC critico e alle autorità competenti delle entità finanziarie cui il fornitore in questione presta i suoi servizi.

   Per l'adempimento delle attività di sorveglianza, le autorità di sorveglianza capofila possono tener conto di qualsiasi certificazione fornita da terzi e di relazioni di audit interni o esterni effettuati da terzi in materia di TIC messe a disposizione dal fornitore terzo di servizi di TIC critico.

Articolo 36

Armonizzazione delle condizioni che consentono lo svolgimento della sorveglianza

1. Le AEV, tramite il comitato congiunto, elaborano progetti di norme tecniche di regolamentazione per specificare:

   (a) le informazioni che il fornitore terzo di servizi di TIC critico deve fornire nella domanda di adesione volontaria di cui all'articolo 28, paragrafo 8;

   (b) il contenuto e il formato delle relazioni che possono essere richieste ai fini dell'articolo 31, paragrafo 1, lettera c);

(c) la presentazione delle informazioni, compresi la struttura, i formati e i metodi, che un fornitore terzo di servizi di TIC critico è tenuto a trasmettere, comunicare o segnalare ai sensi dell'articolo 31, paragrafo 1;

(d) i dettagli della valutazione, da parte delle autorità competenti, delle misure adottate dai fornitori terzi di servizi di TIC critici sulla base delle raccomandazioni delle autorità di sorveglianza capofila ai sensi dell'articolo 37, paragrafo 2.

2. Le AEV presentano detti progetti di norme tecniche di regolamentazione alla Commissione entro il 1° gennaio 20xx [*GU: inserire la data corrispondente a un anno dopo la data di entrata in vigore*].

Alla Commissione è delegato il potere di integrare il presente regolamento, adottando le norme tecniche di regolamentazione di cui al primo comma, in conformità, rispettivamente, della procedura sancita agli articoli da 10 a 14 dei regolamenti (UE) n. 1093/2010, (UE) n. 1094/2010 e (UE) n. 1095/2010.

Articolo 37

Seguito dato dalle autorità competenti

1. Entro 30 giorni di calendario dalla ricezione delle raccomandazioni formulate dall'autorità di sorveglianza capofila ai sensi dell'articolo 31, paragrafo 1, lettera d), i fornitori terzi di servizi di TIC critici comunicano all'autorità di sorveglianza capofila se hanno intenzione di attenersi alle raccomandazioni. Le autorità di sorveglianza capofila trasmettono immediatamente le informazioni alle autorità competenti.

2. Le autorità competenti verificano se le entità finanziarie tengono conto dei rischi individuati nelle raccomandazioni inviate ai fornitori terzi di servizi di TIC critici da parte dell'autorità di sorveglianza capofila ai sensi dell'articolo 31, paragrafo 1, lettera d).

3. A norma dell'articolo 44, le autorità competenti possono chiedere alle entità finanziarie di sospendere temporaneamente, in tutto o in parte, l'utilizzo o l'introduzione di un servizio prestato dal fornitore terzo di servizi di TIC critico, fino a quando non siano stati affrontati i rischi identificati nelle raccomandazioni trasmesse al fornitore terzo di servizi di TIC critico. Laddove si renda necessario, le autorità competenti possono chiedere alle entità finanziarie di risolvere, in tutto o in parte, gli accordi contrattuali pertinenti stipulati con i fornitori terzi di servizi di TIC critici.

4. Al momento di adottare le decisioni di cui al paragrafo 3, le autorità competenti tengono conto del tipo e delle dimensioni del rischio che non è stato affrontato dal fornitore terzo di servizi di TIC critico, nonché della gravità dell'inosservanza, in considerazione dei criteri seguenti:

(a) la gravità e la durata dell'inosservanza;

(b) se l'inosservanza abbia portato alla luce gravi carenze nelle procedure, nei sistemi di gestione, nella gestione dei rischi e nei controlli interni del fornitore terzo di servizi di TIC critico;

(c) se l'inadempienza abbia favorito o generato un reato finanziario o se tale reato sia in qualche misura attribuibile all'inadempienza;

(d) se l'inosservanza sia stata commessa intenzionalmente o per negligenza.

5. Le autorità competenti informano l'autorità di sorveglianza capofila in merito alle misure e agli approcci adottati nell'ambito dei propri compiti di vigilanza in relazione alle entità finanziarie, nonché in merito alle misure contrattuali adottate da queste ultime qualora i fornitori terzi di servizi di TIC critici non abbiano accolto, in tutto o in parte, le raccomandazioni formulate dall'autorità di sorveglianza capofila.

Articolo 38

Commissioni per le attività di sorveglianza

1. Le AEV addebitano ai fornitori terzi di servizi di TIC critici commissioni che coprono completamente le spese necessarie sostenute dalle AEV in relazione allo svolgimento dei compiti di sorveglianza ai sensi del presente regolamento, compreso il rimborso dei costi eventualmente sostenuti in seguito al lavoro svolto dalle autorità competenti che hanno partecipato alle attività di sorveglianza in conformità dell'articolo 35.

   L'importo della commissione addebitata al fornitore di servizi di TIC critico copre tutti i costi amministrativi ed è proporzionato al fatturato del fornitore.

2. Alla Commissione è conferito il potere di adottare un atto delegato, conformemente all'articolo 50, per integrare il presente regolamento determinando l'importo delle commissioni e le relative modalità di pagamento.

Articolo 39

Cooperazione internazionale

1. Ai sensi, rispettivamente, dell'articolo 33 dei regolamenti (UE) n. 1093/2010, (UE) n. 1094/2010 e (UE) n. 1095/2010, l'ABE, l'ESMA e l'EIOPA possono concludere accordi amministrativi con le autorità di vigilanza e di regolamentazione di paesi terzi per promuovere la cooperazione internazionale in materia di rischi relativi alle TIC derivanti da terzi tra i diversi settori finanziari, in particolare definendo migliori prassi per il riesame delle pratiche e dei controlli per la gestione dei rischi relativi alle TIC nonché per le misure di attenuazione e risposta agli incidenti.

2. Le AEV, tramite il comitato congiunto, presentano ogni cinque anni al Parlamento europeo, al Consiglio e alla Commissione una relazione congiunta riservata in cui sintetizzano le conclusioni delle discussioni tenute con le autorità dei paesi terzi di cui al paragrafo 1, con particolare attenzione all'evoluzione dei rischi relativi alle TIC derivanti da terzi e alle implicazioni per la stabilità finanziaria, l'integrità del mercato, la protezione degli investitori o il funzionamento del mercato unico.

CAPO VI

MECCANISMI DI CONDIVISIONE DELLE INFORMAZIONI

Articolo 40

Meccanismi di condivisione delle informazioni e dei dati sulle minacce informatiche

1. Le entità finanziarie possono scambiarsi reciprocamente informazioni e dati sulle minacce informatiche, tra cui indicatori di compromissione, tattiche, tecniche e procedure, segnali di allarme per la cibersicurezza e strumenti di configurazione, nella misura in cui tale condivisione di informazioni e dati:

(a) mira a potenziare la resilienza operativa digitale delle entità finanziarie, in particolare svolgendo opera di sensibilizzazione in merito alle minacce informatiche, contenendo o inibendo la capacità di diffusione delle minacce informatiche e rafforzando la gamma di capacità di difesa, tecniche di individuazione delle minacce, strategie di attenuazione o fasi di risposta e ripristino delle entità finanziarie;

(b) si svolge entro comunità fidate di entità finanziarie;

(c) si realizza mediante meccanismi di condivisione delle informazioni che tutelano la natura potenzialmente sensibile delle informazioni condivise e sono disciplinati da norme di condotta pienamente rispettose della riservatezza dell'attività economica, della protezione dei dati personali[48] e delle linee direttrici sulla politica in materia di concorrenza[49].

2. Ai fini del paragrafo 1, lettera c), i meccanismi di condivisione delle informazioni definiscono le condizioni per la partecipazione e, se del caso, definiscono i dettagli del coinvolgimento delle autorità pubbliche e la veste in cui queste ultime possono partecipare ai meccanismi di condivisione delle informazioni, nonché gli elementi operativi tra cui l'utilizzo di piattaforme informatiche apposite.

3. Le entità finanziarie notificano alle autorità competenti la propria partecipazione ai meccanismi di condivisione delle informazioni di cui al paragrafo 1, al momento della convalida della propria adesione o, se del caso, della cessazione dell'adesione, quando quest'ultima abbia effetto.

CAPO VII

AUTORITÀ COMPETENTI

Articolo 41

Autorità competenti

Fatte salve le disposizioni sul quadro di sorveglianza per i fornitori terzi di servizi di TIC critici di cui al capo V, sezione II, il rispetto degli obblighi sanciti dal presente regolamento è assicurato dalle seguenti autorità competenti conformemente ai poteri conferiti dai rispettivi atti giuridici:

(a) per gli enti creditizi, l'autorità competente designata in conformità dell'articolo 4 della direttiva 2013/36/UE, fatti salvi i compiti specifici conferiti alla BCE dal regolamento (UE) n. 1024/2013;

(b) per i prestatori di servizi di pagamento, l'autorità competente designata in conformità dell'articolo 22 della direttiva (UE) 2015/2366;

[48] Ai sensi del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati) (GU L 119 del 4.5.2016, pag. 1).

[49] Comunicazione della Commissione, Linee direttrici sull'applicabilità dell'articolo 101 del trattato sul funzionamento dell'Unione europea agli accordi di cooperazione orizzontale (GU C 11 del 14.1.2011, pag. 1).

(c) per gli istituti di moneta elettronica, l'autorità competente designata in conformità dell'articolo 37 della direttiva 2009/110/CE;

(d) per le imprese di investimento, l'autorità competente designata in conformità dell'articolo 4 della direttiva (UE) 2019/2034;

(e) per i fornitori di servizi per le cripto-attività, gli emittenti di cripto-attività, gli emittenti di token collegati ad attività e gli emittenti di token collegati ad attività significativi, l'autorità competente designata in conformità dell'articolo 3, paragrafo 1, lettera e), primo trattino, del [*regolamento (UE) 20xx, regolamento MICA*];

(f) per i depositari centrali di titoli, l'autorità competente designata in conformità dell'articolo 11 del regolamento (UE) n. 909/2014;

(g) per le controparti centrali, l'autorità competente designata in conformità dell'articolo 22 del regolamento (UE) n. 648/2012;

(h) per le sedi di negoziazione e i fornitori di servizi di comunicazione dati, l'autorità competente designata in conformità dell'articolo 67 della direttiva 2014/65/UE;

(i) per i repertori di dati sulle negoziazioni, l'autorità competente designata in conformità dell'articolo 55 del regolamento (UE) n. 648/2012;

(j) per i gestori di fondi di investimento alternativi, l'autorità competente designata in conformità dell'articolo 44 della direttiva 2011/61/UE;

(k) per le società di gestione, l'autorità competente designata in conformità dell'articolo 97 della direttiva 2009/65/CE;

(l) per le imprese di assicurazione e di riassicurazione, l'autorità competente designata in conformità dell'articolo 30 della direttiva 2009/138/CE;

(m) per gli intermediari assicurativi, gli intermediari riassicurativi e gli intermediari assicurativi a titolo accessorio, l'autorità competente designata in conformità dell'articolo 12 della direttiva (UE) 2016/97;

(n) per gli enti pensionistici aziendali o professionali, l'autorità competente designata a norma dell'articolo 47 della direttiva (UE) 2016/2341;

(o) per le agenzie di rating del credito, l'autorità competente designata in conformità dell'articolo 21 del regolamento (CE) n. 1060/2009;

(p) per i revisori legali e le imprese di revisione, l'autorità competente designata in conformità dell'articolo 3, paragrafo 2, e dell'articolo 32 della direttiva 2006/43/CE;

(q) per gli amministratori degli indici di riferimento critici, l'autorità competente designata in conformità degli articoli 40 e 41 del *regolamento xx/202x*;

(r) per i fornitori di servizi di crowdfunding, l'autorità competente designata in conformità dell'*articolo x del regolamento xx/202x*;

(s) per i repertori di dati sulle cartolarizzazioni, l'autorità competente designata in conformità dell'articolo 10 e dell'articolo 14, paragrafo 1, del regolamento (UE) 2017/2402.

Articolo 42

Cooperazione con le strutture e le autorità istituite dalla direttiva (UE) 2016/1148

1. Per promuovere la cooperazione e consentire lo scambio di pratiche di vigilanza tra le autorità competenti designate a norma del presente regolamento e il gruppo di cooperazione istituito dall'articolo 11 della direttiva (UE) 2016/1148, le AEV e le autorità competenti possono chiedere di essere invitate ai lavori del gruppo di cooperazione.

2. Le autorità competenti possono consultare, se del caso, il punto di contatto unico e i gruppi di intervento per la sicurezza informatica in caso di incidente istituiti rispettivamente ai sensi degli articoli 8 e 9 della direttiva (UE) 2016/1148.

Articolo 43

Comunicazione, cooperazione e attività finanziarie intersettoriali

1. Le AEV, tramite il comitato congiunto e in collaborazione con le autorità competenti, la BCE e il CERS, possono istituire meccanismi che consentano la condivisione di pratiche efficaci tra i vari settori finanziari per migliorare la consapevolezza situazionale e identificare i rischi e le vulnerabilità informatiche comuni a tutti i settori.

   Le AEV possono elaborare esercitazioni di gestione delle crisi e delle emergenze comprendenti scenari di attacchi informatici al fine di sviluppare canali di comunicazione e promuovere gradualmente una risposta efficace coordinata a livello dell'UE nel caso di grave incidente transfrontaliero connesso alle TIC o relativa minaccia aventi un impatto sistemico sull'intero settore finanziario dell'Unione.

   A seconda dei casi queste esercitazioni possono anche servire come test delle dipendenze del settore finanziario da altri settori economici.

2. Le autorità competenti, l'ABE, l'ESMA o l'EIOPA e la BCE cooperano strettamente tra loro e si scambiano informazioni per svolgere i compiti di cui agli articoli da 42 a 48. Realizzano uno stretto coordinamento dell'attività di vigilanza per rilevare e correggere le violazioni del presente regolamento, sviluppare e promuovere migliori pratiche, agevolare la collaborazione, promuovere la coerenza dell'interpretazione e formulare valutazioni transgiurisdizioni in caso di disaccordo.

Articolo 44

Sanzioni amministrative e misure di riparazione

1. Alle autorità competenti sono conferiti tutti i poteri di vigilanza, di indagine e sanzionatori necessari per adempiere i propri compiti ai sensi del presente regolamento.

2. I poteri di cui al paragrafo 1 includono almeno il potere di:

   (a) accedere a qualsiasi documento o dato, detenuto in qualsiasi forma, che l'autorità competente consideri pertinente per lo svolgimento dei propri compiti e riceverne o farne una copia;

   (b) effettuare indagini o ispezioni in loco;

   (c) richiedere l'applicazione di misure correttive e di riparazione per le violazioni delle prescrizioni del presente regolamento.

3. Fatto salvo il diritto degli Stati membri di imporre sanzioni penali ai sensi dell'articolo 46, gli Stati membri stabiliscono norme che prevedano adeguate sanzioni amministrative e misure di riparazione per le violazioni del presente regolamento e ne garantiscono l'effettiva applicazione.

   Tali sanzioni e misure sono efficaci, proporzionate e dissuasive.

4. Gli Stati membri conferiscono alle autorità competenti il potere di applicare almeno le sanzioni amministrative o misure di riparazione seguenti per le violazioni del presente regolamento:

   (a) emanare un ordine che imponga alla persona fisica o giuridica di porre termine al comportamento in questione e di astenersi dal ripeterlo;

   (b) richiedere la cessazione temporanea o permanente di qualsiasi pratica o comportamento che le autorità competenti considerino contrari alle disposizioni del presente regolamento e prevenirne la reiterazione;

   (c) adottare qualsiasi tipo di misura, anche di natura pecuniaria, per assicurare che le entità finanziarie continuino a rispettare le prescrizioni di legge;

   (d) chiedere, nella misura in cui ciò sia consentito dal diritto nazionale, le registrazioni esistenti di traffico dati detenute dagli operatori di telecomunicazioni, qualora vi sia il ragionevole sospetto di violazioni del presente regolamento e qualora si ritenga che le registrazioni possano essere pertinenti ai fini delle rispettive indagini; e

   (e) pubblicare comunicazioni pubbliche, comprese dichiarazioni pubbliche, indicanti l'identità della persona fisica o giuridica e la natura della violazione.

5. Qualora le disposizioni di cui al paragrafo 2, lettera c), e al paragrafo 4 si applichino a persone giuridiche, gli Stati membri conferiscono alle autorità competenti il potere di imporre sanzioni amministrative e misure di riparazione, alle condizioni previste dal diritto nazionale, nei confronti di membri dell'organo di gestione e di altre persone che, ai sensi del diritto nazionale, siano responsabili della violazione.

6. Gli Stati membri garantiscono che qualsiasi decisione di imporre sanzioni amministrative o misure di riparazione adottata ai sensi del paragrafo 2, lettera c), sia adeguatamente motivata e preveda il diritto di ricorso.

Articolo 45

Esercizio del potere di imporre sanzioni amministrative e misure di riparazione

1. Le autorità competenti esercitano il potere di imporre sanzioni amministrative e misure di riparazione di cui all'articolo 44 in conformità del proprio quadro giuridico nazionale, a seconda dei casi:

   (a) direttamente;

   (b) in collaborazione con altre autorità;

   (c) sotto la propria responsabilità mediante delega ad altre autorità;

   (d) rivolgendosi alle competenti autorità giudiziarie.

2. Per stabilire il tipo e il livello della sanzione amministrativa o della misura di riparazione da imporre a norma dell'articolo 44, le autorità competenti tengono conto

della misura in cui la violazione è intenzionale o è dovuta a negligenza e di tutte le altre circostanze pertinenti, tra cui, secondo il caso:

(a) la rilevanza, la gravità e la durata della violazione;

(b) il grado di responsabilità della persona fisica o giuridica responsabile della violazione;

(c) la solidità finanziaria della persona fisica o giuridica responsabile;

(d) l'importanza degli utili realizzati e delle perdite evitate da parte della persona fisica o giuridica responsabile, nella misura in cui possano essere determinati;

(e) le perdite subite da terzi a causa della violazione, nella misura in cui possano essere determinate;

(f) il livello di cooperazione che la persona fisica o giuridica responsabile ha dimostrato nei confronti dell'autorità competente, ferma restando la necessità di garantire la restituzione degli utili realizzati o delle perdite evitate da tale soggetto;

(g) le precedenti violazioni commesse dalla persona fisica o giuridica responsabile.

Articolo 46

Sanzioni penali

1. Gli Stati membri possono decidere di non emanare norme relative a sanzioni amministrative o misure di riparazione per violazioni che, ai sensi del rispettivo diritto nazionale, siano passibili di sanzioni penali.

2. Qualora abbiano deciso di imporre sanzioni penali per violazioni del presente regolamento, gli Stati membri provvedono affinché siano messe in atto misure adeguate per far sì che le autorità competenti dispongano di tutti i poteri necessari per stabilire contatti con le autorità giudiziarie, le autorità inquirenti o le autorità di giustizia penale della loro giurisdizione, al fine di ricevere informazioni specifiche sulle indagini o i procedimenti penali avviati per violazioni del presente regolamento, e di trasmetterle alle altre autorità competenti, nonché all'ABE, all'ESMA o all'EIOPA in modo tale che possano adempiere l'obbligo di cooperazione ai fini del presente regolamento.

Articolo 47

Obblighi di notifica

Gli Stati membri notificano alla Commissione, all'ABE, all'ESMA e all'EIOPA le disposizioni legislative, regolamentari ed amministrative adottate in attuazione del presente capo, incluse le eventuali norme di diritto penale applicabili, entro il [*GU: inserire la data corrispondente a un anno dopo la data di entrata in vigore*]. Gli Stati membri notificano senza indebito ritardo alla Commissione, all'ESMA, all'ABE e all'EIOPA tutte le successive modifiche.

Articolo 48

Pubblicazione delle sanzioni amministrative

1. Le autorità competenti pubblicano senza indebito ritardo sul proprio sito web ufficiale qualsiasi decisione di imporre sanzioni amministrative contro la quale non vi sia diritto di ricorso, dopo la notifica al destinatario.

2. La pubblicazione di cui al paragrafo 1 comprende informazioni sul tipo e la natura della violazione, l'identità delle persone responsabili e le sanzioni imposte.

3. Qualora, in seguito a una valutazione caso per caso, ritenga che la pubblicazione dell'identità, nel caso di persone giuridiche, o dell'identità e dei dati personali, nel caso di persone fisiche, sarebbe sproporzionata, metterebbe a repentaglio la stabilità dei mercati finanziari o lo svolgimento di un'indagine penale in corso, oppure potrebbe provocare, nella misura in cui possano essere determinati, danni sproporzionati alla persona coinvolta, l'autorità competente adotta una delle soluzioni seguenti in merito alla decisione di imporre una sanzione amministrativa:

   (a) rinvia la pubblicazione fino al momento in cui cesseranno di esistere tutti i motivi che giustificano la non pubblicazione;

   (b) pubblica la sanzione in forma anonima in maniera conforme al diritto nazionale; o

   (c) si astiene dalla pubblicazione, qualora le opzioni di cui alle lettere a) e b) siano ritenute insufficienti per scongiurare ogni pericolo per la stabilità dei mercati finanziari, oppure quando tale pubblicazione non sarebbe proporzionata alla mitezza della sanzione imposta.

4. Qualora si decida di pubblicare una sanzione amministrativa in forma anonima, ai sensi del paragrafo 3, lettera b), la pubblicazione dei dati pertinenti può essere rinviata.

5. Qualora l'autorità competente pubblichi una decisione che impone una sanzione amministrativa che è oggetto di ricorso dinanzi alle pertinenti autorità giudiziarie, le autorità competenti aggiungono immediatamente sul proprio sito web ufficiale tale informazione e, nelle fasi successive, eventuali informazioni correlate all'esito del ricorso. È pubblicata anche ogni decisione giudiziaria che annulli una decisione di imporre una sanzione amministrativa.

6. Le autorità competenti provvedono affinché le informazioni pubblicate ai sensi dei paragrafi da 1 a 4 restino sul loro sito web ufficiale per cinque anni almeno dalla pubblicazione. I dati personali contenuti nella pubblicazione sono conservati sul sito web ufficiale dell'autorità competente unicamente per il periodo necessario conformemente alle norme applicabili in materia di protezione dei dati.

Articolo 49

Segreto professionale

1. Le informazioni riservate ricevute, scambiate o trasmesse a norma del presente regolamento sono soggette alle condizioni in materia di segreto professionale di cui al paragrafo 2.

2. L'obbligo del segreto professionale si applica a tutte le persone che prestano o hanno prestato la loro attività per le autorità competenti ai sensi del presente regolamento o per qualsiasi autorità, impresa che opera sul mercato o persona fisica o giuridica cui tali autorità competenti hanno delegato i propri poteri, compresi i revisori e gli esperti incaricati da dette autorità.

3. Le informazioni coperte dal segreto professionale non possono essere divulgate ad alcuna altra persona o autorità se non in forza di disposizioni del diritto dell'Unione o del diritto nazionale.

4. Tutte le informazioni scambiate tra le autorità competenti in applicazione del presente regolamento relativamente ad aspetti commerciali od operativi e ad altre questioni di natura economica o personale sono considerate riservate e sono soggette all'obbligo del segreto professionale, salvo quando l'autorità competente dichiara al momento della loro comunicazione che è consentita la divulgazione di tali informazioni o che la stessa è necessaria a fini di procedimenti giudiziari.

CAPO VIII

ATTI DELEGATI

Articolo 50

Esercizio della delega

1. Il potere di adottare atti delegati è conferito alla Commissione alle condizioni stabilite nel presente articolo.

2. Il potere di adottare atti delegati di cui all'articolo 28, paragrafo 3, e all'articolo 38, paragrafo 2, è conferito alla Commissione per un periodo di cinque anni a decorrere da [PO: inserire la data corrispondente a cinque anni dopo la data di entrata in vigore del presente regolamento].

3. La delega di potere di cui all'articolo 28, paragrafo 3, e all'articolo 38, paragrafo 2, può essere revocata in qualsiasi momento dal Parlamento europeo o dal Consiglio. La decisione di revoca pone fine alla delega di potere ivi specificata. Gli effetti della decisione decorrono dal giorno successivo alla pubblicazione della decisione nella Gazzetta ufficiale dell'Unione europea o da una data successiva ivi specificata. Essa non pregiudica la validità degli atti delegati già in vigore.

4. Prima dell'adozione dell'atto delegato la Commissione consulta gli esperti designati da ciascuno Stato membro nel rispetto dei principi stabiliti nell'accordo interistituzionale "Legiferare meglio" del 13 aprile 2016.

5. Non appena adotta un atto delegato, la Commissione ne dà contestualmente notifica al Parlamento europeo e al Consiglio.

6. L'atto delegato adottato ai sensi dell'articolo 28, paragrafo 3, e dell'articolo 38, paragrafo 2, entra in vigore solo se né il Parlamento europeo né il Consiglio hanno sollevato obiezioni entro il termine di due mesi dalla data in cui esso è stato loro notificato o se, prima della scadenza di tale termine, sia il Parlamento europeo che il Consiglio hanno informato la Commissione che non intendono sollevare obiezioni. Tale termine è prorogato di due mesi su iniziativa del Parlamento europeo o del Consiglio.

CAPO IX

DISPOSIZIONI TRANSITORIE E FINALI

SEZIONE I

Articolo 51

Clausola di riesame

Entro il [*PO: inserire la data corrispondente a cinque anni dopo la data di entrata in vigore del presente regolamento*], la Commissione, dopo aver consultato l'ABE, l'ESMA, l'EIOPA e il CERS, a seconda dei casi, effettua un riesame e presenta al Parlamento europeo e al Consiglio una relazione accompagnata, se del caso, da una proposta legislativa concernente i criteri per la designazione dei fornitori terzi di servizi di TIC critici, di cui all'articolo 28, paragrafo 2.

SEZIONE II

MODIFICHE

Articolo 52

Modifiche del regolamento (CE) n. 1060/2009

Nell'allegato I del regolamento (CE) n. 1060/2009, il punto 4, primo comma, della sezione A è sostituito dal testo seguente:

> "Un'agenzia di rating del credito dispone di procedure amministrative e contabili solide, di meccanismi di controllo interno, di procedure efficaci per la valutazione del rischio e di meccanismi efficaci di controllo e protezione per la gestione dei sistemi di TIC in conformità del regolamento (UE) 2021/xx del Parlamento europeo e del Consiglio* [DORA].
>
> * Regolamento (UE) 2021/xx del Parlamento europeo e del Consiglio […] (GU L XX del GG.MM.AAAA, pag. X)."

Articolo 53

Modifiche del regolamento (UE) n. 648/2012

Il regolamento (UE) n. 648/2012 è così modificato:

(1) l'articolo 26 è così modificato:

(a) il paragrafo 3 è sostituito dal seguente:

> "3. Le CCP mantengono e gestiscono una struttura organizzativa che assicuri la continuità e il regolare funzionamento della prestazione dei servizi e dell'esercizio delle attività. Esse utilizzano sistemi, risorse e procedure adeguati e proporzionati, compresi sistemi di TIC gestiti in

conformità del regolamento (UE) 2021/xx del Parlamento europeo e del Consiglio* [DORA].

* Regolamento (UE) 2021/xx del Parlamento europeo e del Consiglio […](GU L XX, GG.MM.AAAA, pag. X).";

(b) il paragrafo 6 è soppresso;

(2) l'articolo 34 è così modificato:

(a) il paragrafo 1 è sostituito dal seguente:

"1. Le CCP adottano, attuano e mantengono una politica adeguata di continuità operativa e un piano di ripristino in caso di disastro, comprendenti piani di continuità operativa e di ripristino in caso di disastro relativi alle TIC istituiti in conformità del regolamento (UE) 2021/xx [DORA], miranti a preservare le funzioni, ad assicurare la ripresa tempestiva delle attività e l'adempimento delle obbligazioni della CCP.";

(b) al paragrafo 3, il primo comma è sostituito dal seguente:

"Al fine di garantire l'applicazione coerente del presente articolo, l'ESMA, previa consultazione dei membri del SEBC, elabora progetti di norme tecniche di regolamentazione per specificare il contenuto minimo e i requisiti della politica di continuità operativa e del piano di ripristino in caso di disastro, con l'esclusione dei piani di continuità operativa e di ripristino in caso di disastro relativi alle TIC.";

(3) all'articolo 56, il primo comma del paragrafo 3 è sostituito dal seguente:

"3. Per assicurare l'applicazione uniforme del presente articolo, l'ESMA elabora progetti di norme tecniche di regolamentazione che specifichino, tranne che per le prescrizioni in materia di gestione dei rischi relativi alle TIC, i dettagli della domanda di registrazione di cui al paragrafo 1.";

(4) all'articolo 79, i paragrafi 1 e 2 sono sostituiti dai seguenti:

"1. I repertori di dati sulle negoziazioni individuano le fonti di rischio operativo e le riducono anche sviluppando sistemi, controlli e procedure adeguati, tra cui sistemi di TIC gestiti ai sensi del regolamento (UE) 2021/xx *[DORA*].

2. I repertori di dati sulle negoziazioni stabiliscono, attuano e mantengono una politica adeguata di continuità operativa e un piano di ripristino in caso di disastro, comprendenti piani di continuità operativa e di ripristino in caso di disastro relativi alle TIC istituiti in conformità del regolamento (UE) 2021/xx *[DORA]*, miranti a preservare le loro funzioni, ad assicurare la ripresa tempestiva delle attività e l'adempimento degli obblighi assunti.";

(5) all'articolo 80, il paragrafo 1 è soppresso.

Articolo 54

Modifiche del regolamento (UE) n. 909/2014

L'articolo 45 del regolamento (UE) n. 909/2014 è così modificato:

(1) il paragrafo 1 è sostituito dal seguente:

"1. I CSD individuano le fonti di rischio operativo, interne ed esterne, e ne riducono al minimo l'impatto avvalendosi di strumenti, processi e politiche in materia di TIC adeguati, istituiti e gestiti ai sensi del regolamento (UE) 2021/xx del Parlamento europeo e del Consiglio*[*DORA*], nonché mediante qualsiasi altro tipo adeguato di strumenti, controlli e procedure per altri tipi di rischi operativi, anche per tutti i sistemi di regolamento titoli da essi operati.

* Regolamento (UE) 2021/xx del Parlamento europeo e del Consiglio […] (GU L XX, GG.MM.AAAA, pag. X).";

(2) il paragrafo 2 è soppresso;

(3) i paragrafi 3 e 4 sono sostituiti dai seguenti:

"3. Per i servizi che forniscono nonché per ciascun sistema di regolamento titoli da essi operati, i CSD stabiliscono, attuano e mantengono una politica di continuità operativa ed un piano di ripristino in caso di disastro relativi alle TIC adeguati, istituiti ai sensi del regolamento (UE) 2021/xx [DORA], allo scopo di preservare i servizi, assicurare la ripresa tempestiva delle attività e l'adempimento degli obblighi del CSD in caso di eventi che comportino un rischio significativo di perturbare le attività.

4. Il piano di cui al paragrafo 3 prevede il ripristino di tutte le operazioni e posizioni dei partecipanti al momento della perturbazione, in modo da permettere ai partecipanti al CSD di continuare ad operare con certezza e di completare il regolamento alla data prevista, anche assicurando che i sistemi informatici critici possano riprendere a funzionare dal momento della perturbazione, come previsto dall'articolo 11, paragrafi 5 e 7, del regolamento (UE) 2021/xx [DORA].";

(4) al paragrafo 6, il primo comma è sostituito dal seguente*:*

"I CSD individuano, controllano e gestiscono i rischi ai quali i principali partecipanti ai sistemi di regolamento titoli da essi operati nonché i fornitori di servizi e utenze, e altri CSD o altre infrastrutture di mercato possono esporre le loro attività. Su richiesta, forniscono alle autorità competenti e rilevanti informazioni su ogni rischio siffatto individuato. Informano inoltre senza indugio l'autorità competente e le autorità interessate in merito a eventuali incidenti operativi causati da tali rischi, tranne che in relazione ai rischi relativi alle TIC.";

(5) al paragrafo 7, il primo comma è sostituito dal seguente*:*

"L'ESMA, in stretta cooperazione con i membri del SEBC, elabora progetti di norme tecniche di regolamentazione per specificare i rischi operativi di cui ai paragrafi 1 e 6, tranne che in relazione ai rischi relativi alle TIC, i metodi per testare, gestire o ridurre al minimo tali rischi, compresi una politica adeguata di continuità operativa e un piano di ripristino in caso di disastro di cui ai paragrafi 3 e 4 e i metodi di valutazione degli stessi.".

Articolo 55

Modifiche del regolamento (UE) n. 600/2014

Il regolamento (UE) n. 600/2014 è così modificato:

(1) l'articolo 27 octies è così modificato:

(a) il paragrafo 4 è soppresso;

(b) al paragrafo 8, la lettera c) è sostituita dalla seguente:

"c) i requisiti organizzativi concreti di cui ai paragrafi 3 e 5.";

(2) l'articolo 27 nonies è così modificato:

(a) il paragrafo 5 è soppresso;

(b) al paragrafo 8, la lettera e) è sostituita dalla seguente:

"e) i requisiti organizzativi concreti di cui al paragrafo 4.";

(3) l'articolo 27 decies è così modificato:

(a) Il paragrafo 3 è soppresso;

(b) al paragrafo 5, la lettera b) è sostituita dalla seguente:

"b) i requisiti organizzativi concreti di cui ai paragrafi 2 e 4.".

Articolo 56

Entrata in vigore e applicazione

Il presente regolamento entra in vigore il ventesimo giorno successivo alla pubblicazione nella *Gazzetta ufficiale dell'Unione europea*.

Esso si applica a decorrere dal [*PO: inserire la data corrispondente a 12 mesi dopo la data di entrata in vigore*].

Gli articoli 23 e 24 si applicano tuttavia a decorrere dal [*PO: inserire la data corrispondente a 36 mesi dopo la data di entrata in vigore del presente regolamento*].

Il presente regolamento è obbligatorio in tutti i suoi elementi e direttamente applicabile in ciascuno degli Stati membri.

Fatto a Bruxelles, il

Per il Parlamento europeo	*Per il Consiglio*
Il presidente	*Il presidente*

SCHEDA FINANZIARIA LEGISLATIVA

1. CONTESTO DELLA PROPOSTA/INIZIATIVA

1.1. Titolo della proposta/iniziativa

1.2. Settore/settori interessati

1.3. Natura della proposta/iniziativa

1.4. Obiettivi

1.5. Motivazione della proposta/iniziativa

1.6. Durata e incidenza finanziaria della proposta/iniziativa

1.7. Modalità di gestione previste

2. MISURE DI GESTIONE

2.1. Disposizioni in materia di monitoraggio e di relazioni

2.2. Sistemi di gestione e di controllo

2.3. Misure di prevenzione delle frodi e delle irregolarità

3. INCIDENZA FINANZIARIA PREVISTA DELLA PROPOSTA/INIZIATIVA

3.1. Rubrica/rubriche del quadro finanziario pluriennale e linea/linee di bilancio di spesa interessate

3.2. Incidenza prevista sulle spese

3.2.1. Sintesi dell'incidenza prevista sulle spese

3.2.2. Incidenza prevista sugli stanziamenti

3.2.3. Incidenza prevista sulle risorse umane

3.2.4. Compatibilità con il quadro finanziario pluriennale attuale

3.2.5. Partecipazione di terzi al finanziamento

3.3. Incidenza prevista sulle entrate

Allegato

Ipotesi generali

Poteri di sorveglianza

SCHEDA FINANZIARIA LEGISLATIVA "AGENZIE"

1. CONTESTO DELLA PROPOSTA/INIZIATIVA

1.1. Titolo della proposta/iniziativa

Proposta di regolamento del Parlamento europeo e del Consiglio relativo alla resilienza operativa digitale per il settore finanziario.

1.2. Settore/settori interessati

Settore: stabilità finanziaria, servizi finanziari e Unione dei mercati dei capitali

Attività: resilienza operativa digitale

1.3. La proposta riguarda

☑ **una nuova azione**

☐ **una nuova azione a seguito di un progetto pilota/un'azione preparatoria**[50]

☐ **la proroga di un'azione esistente**

☐ **la fusione di una o più azioni verso un'altra/una nuova azione**

1.4. Obiettivi

1.4.1. Obiettivi generali

L'obiettivo generale dell'iniziativa consiste nel rafforzare la resilienza operativa digitale delle entità del settore finanziario dell'UE, razionalizzando e aggiornando le norme vigenti e introducendo nuove prescrizioni laddove si riscontrino lacune. Ne risulterebbe anche un miglioramento della dimensione digitale del codice unico.

L'obiettivo complessivo può articolarsi in tre obiettivi generali: 1) ridurre il rischio di instabilità e perturbazioni finanziarie, 2) ridurre gli oneri amministrativi e accrescere l'efficacia della vigilanza e 3) rafforzare la protezione dei consumatori e degli investitori.

1.4.2. Obiettivi specifici

La proposta ha gli obiettivi specifici seguenti:

affrontare i rischi relativi alle tecnologie dell'informazione e della comunicazione ("TIC") in maniera più esaustiva e potenziare il livello complessivo di resilienza digitale del settore finanziario;

razionalizzare le segnalazioni di incidenti connessi alle TIC e affrontare il problema delle sovrapposizioni fra prescrizioni in materia di segnalazioni;

consentire alle autorità di vigilanza finanziaria di accedere alle informazioni relative agli incidenti connessi alle TIC;

garantire alle entità finanziarie interessate dalla presente proposta di valutare l'efficacia delle proprie misure di prevenzione e resilienza e di identificare le vulnerabilità connesse alle TIC;

[50] A norma dell'articolo 58, paragrafo 2, lettera a) o b), del regolamento finanziario.

ridurre la frammentazione del mercato unico e far sì che i risultati dei test siano accettati su scala transfrontaliera;

potenziare le salvaguardie contrattuali a favore delle entità finanziarie che fruiscono di servizi di TIC, anche per quanto riguarda le norme sull'esternalizzazione (disciplinando il monitoraggio di fornitori terzi di servizi di TIC);

attivare la sorveglianza delle attività dei fornitori terzi di servizi di TIC critici;

incoraggiare lo scambio di dati sulle minacce nel settore finanziario.

1.4.3. Risultati e incidenza previsti

Precisare gli effetti che la proposta/iniziativa dovrebbe avere sui beneficiari/gruppi interessati.

Un atto sulla resilienza operativa digitale per il settore finanziario offrirebbe un quadro generale per tutti gli aspetti della resilienza operativa digitale e costituirebbe uno strumento efficace per migliorare la resilienza operativa complessiva del settore finanziario. Garantirebbe chiarezza e coerenza all'interno del codice unico.

Renderebbe inoltre più chiara e coerente l'interazione con la direttiva NIS e il riesame di quest'ultima. Renderebbe più chiare alle entità finanziarie le diverse norme che esse devono rispettare in materia di resilienza operativa digitale, in particolare per quelle entità finanziarie che detengono più autorizzazioni e operano in diversi mercati dell'UE.

1.4.4. Indicatori di prestazione

Precisare gli indicatori con cui monitorare progressi e risultati.

Possibili indicatori

Numero di incidenti connessi alle TIC nel settore finanziario dell'UE e relativo impatto

Numero di incidenti gravi connessi alle TIC segnalati alle autorità di vigilanza prudenziale

Numero di entità finanziarie che sarebbero tenute a svolgere test di penetrazione basati su minacce

Numero di entità finanziarie che utilizzano clausole contrattuali standard per stipulare accordi contrattuali con fornitori terzi di servizi di TIC

Numero di fornitori terzi di servizi di TIC critici su cui le AEV/autorità di vigilanza prudenziale esercitano attività di vigilanza

Numero di entità finanziarie che partecipano a soluzioni di condivisione di dati sulle minacce

Numero di autorità che devono ricevere relazioni sullo stesso incidente connesso alle TIC

Numero di test di penetrazione basati su minacce transfrontalieri

1.5. Motivazione della proposta/iniziativa

1.5.1. Necessità nel breve e lungo termine, compreso un calendario dettagliato per fasi di attuazione dell'iniziativa

Il settore finanziario dipende in larga misura dalle tecnologie dell'informazione e della comunicazione (TIC). Nonostante i notevoli progressi compiuti grazie all'adozione, a livello nazionale ed europeo, di iniziative legislative e politiche mirate, i rischi relativi alle TIC continuano a rappresentare una sfida per la resilienza operativa, le prestazioni e la stabilità del sistema finanziario dell'Unione. La riforma che è stata introdotta sulla scia della crisi finanziaria del 2008 ha rafforzato in primo luogo la resilienza finanziaria del settore finanziario dell'UE, mirando a salvaguardare la competitività e la stabilità dell'UE in una prospettica economica, prudenziale e di condotta sul mercato. Benché si inseriscano nel quadro del rischio operativo, la sicurezza delle TIC e la resilienza operativa digitale complessiva hanno occupato un posto meno rilevante nell'agenda normativa che è seguita alla crisi e sono state sviluppate solo in alcuni settori delle politiche e della normativa dell'Unione in materia di mercati finanziari, o soltanto in alcuni Stati membri. Ciò si traduce nelle sfide indicate di seguito, che la proposta si propone di affrontare.

Il quadro giuridico dell'UE in materia di rischi relativi alle TIC e resilienza operativa nel settore finanziario è frammentato e non del tutto coerente.

A causa della mancanza di prescrizioni coerenti per la segnalazione di incidenti connessi alle TIC, le autorità di vigilanza possono disporre solo di un quadro incompleto della natura, della frequenza, della rilevanza e dell'impatto degli incidenti.

Alcune entità finanziarie devono rispettare, per lo stesso incidente, prescrizioni in materia di segnalazione complesse, sovrapposte e potenzialmente incoerenti.

Le carenze nelle attività di condivisione delle informazioni e nella cooperazione relative ai dati sulle minacce informatiche, a livello strategico, tattico e operativo, impediscono alle singole entità finanziarie di valutare e monitorare adeguatamente le minacce informatiche, difendersi dai loro effetti e rispondervi.

In alcuni sottosettori finanziari possono esservi più quadri di test di penetrazione e resilienza, privi di coordinamento oltre che di riconoscimento transfrontaliero dei risultati, mentre in altri sottosettori non esiste alcun quadro in materia.

Le scarse indicazioni che la vigilanza offre sulle attività delle entità finanziarie svolte tramite i fornitori terzi di servizi di TIC espongono a rischi operativi sia le singole entità finanziarie, sia l'intero sistema finanziario.

Le autorità di vigilanza finanziaria non detengono un mandato sufficiente né gli strumenti per monitorare e gestire i rischi sistemici e di concentrazione derivanti dalla dipendenza delle entità finanziarie da terzi attivi nel settore delle TIC.

1.5.2. Valore aggiunto dell'intervento dell'Unione (che può derivare da diversi fattori, ad esempio un miglior coordinamento, la certezza del diritto o un'efficacia e una complementarità maggiori). Ai fini del presente punto, per "valore aggiunto dell'intervento dell'Unione" si intende il valore derivante dall'intervento dell'Unione che va ad aggiungersi al valore che avrebbero altrimenti generato gli Stati membri se avessero agito da soli.

Motivi dell'azione a livello europeo (ex ante)

La resilienza operativa digitale è una questione di interesse comune per i mercati finanziari dell'UE. Un'azione intrapresa a livello dell'Unione recherebbe maggiori vantaggi e un valore più elevato rispetto a un'azione intrapresa separatamente a livello nazionale. Se non si aggiungessero queste disposizioni operative in materia di rischi relativi alle TIC, il codice unico offrirebbe bensì gli strumenti per affrontare tutti gli altri tipi di rischi a livello europeo,

ma trascurerebbe gli aspetti della resilienza operativa digitale o li assoggetterebbe a iniziative frammentarie e prive di coordinamento adottate a livello nazionale. La proposta intende introdurre chiarezza giuridica sulla possibilità e le modalità di applicazione delle disposizioni operative digitali, in particolare per le entità finanziarie transfrontaliere, ed eliminerebbe la necessità per gli Stati membri di migliorare individualmente norme, standard e aspettative in materia di resilienza operativa e cibersicurezza in risposta all'attuale limitatezza della portata delle norme dell'UE e alla natura generale della direttiva NIS.

Valore aggiunto dell'Unione previsto (ex post)

L'intervento dell'Unione accrescerebbe sensibilmente l'efficacia della politica, riducendo d'altra parte la complessità e alleviando gli oneri finanziari e amministrativi che gravano su tutte le entità finanziarie. Armonizzerebbe un settore dell'economia che è profondamente interconnesso e integrato e già beneficia di un unico insieme di norme e vigilanza. Per quanto riguarda la segnalazione di incidenti connessi alle TIC, la proposta ridurrebbe gli oneri di segnalazione - e i costi impliciti - derivanti dalla necessità di segnalare lo stesso incidente connesso alle TIC a diverse autorità dell'UE e/o nazionali. Favorirà inoltre il riconoscimento/l'accettazione reciproci dei risultati dei test di entità che operano a livello transfrontaliero e sono soggette a molteplici quadri in materia di test nei diversi Stati membri.

1.5.3. Insegnamenti tratti da esperienze analoghe

Nuova iniziativa

1.5.4. Compatibilità con il quadro finanziario pluriennale ed eventuali sinergie con altri strumenti pertinenti

L'obiettivo di questa proposta è coerente con una serie di altre iniziative in corso e politiche dell'UE, in particolare con la direttiva sulla sicurezza delle reti e dei sistemi informativi (NIS) e la direttiva sulle infrastrutture critiche europee (ECI). La proposta intende preservare i benefici associati al quadro orizzontale sulla cibersicurezza, mantenendo i tre sottosettori finanziari nell'ambito di applicazione della direttiva NIS. Rimanendo associate all'ecosistema NIS, le autorità di vigilanza finanziaria sarebbero in grado di scambiare informazioni pertinenti con le autorità NIS e di partecipare al gruppo di cooperazione NIS. La proposta non inciderebbe sulla direttiva NIS ma ne costituirebbe uno sviluppo e affronterebbe il problema di possibili sovrapposizioni mediante un'esenzione del tipo lex specialis. L'interazione tra il regolamento sui servizi finanziari e la direttiva NIS sarebbe sempre disciplinata da una clausola lex specialis, esentando in tal modo le entità finanziarie da prescrizioni sostanziali contenute nella direttiva NIS ed evitando sovrapposizioni tra i due strumenti. Inoltre la proposta è coerente con la direttiva sulle infrastrutture critiche europee (ECI), di cui attualmente è in corso una revisione volta a migliorare la protezione e la resilienza delle infrastrutture critiche rispetto alle minacce non informatiche.

La proposta non inciderebbe sul quadro finanziario pluriennale (QFP). In primo luogo, il quadro di sorveglianza dei fornitori terzi di servizi di TIC critici sarà interamente finanziato dalle commissioni addebitate a tali fornitori; in secondo luogo, le funzioni regolamentari supplementari concernenti la resilienza operativa digitale attribuite alle AEV saranno assolte per mezzo di una ridistribuzione interna del personale attuale.

Ciò si tradurrà in una proposta di aumento del personale autorizzato dell'agenzia nel corso della futura procedura annuale di bilancio. L'agenzia continuerà ad adoperarsi per massimizzare le sinergie e gli incrementi di efficienza (anche attraverso sistemi informatici) e a monitorare attentamente il carico di lavoro supplementare associato alla presente proposta,

che si rifletterà nel livello di personale autorizzato richiesto dall'agenzia nella procedura annuale di bilancio.

1.5.5. Valutazione delle varie opzioni di finanziamento disponibili, comprese le possibilità di riassegnazione

Sono state prese in considerazione varie opzioni di finanziamento.

In primo luogo, i costi supplementari potrebbero essere finanziati tramite il consueto meccanismo di finanziamento delle AEV. Ciò comporterebbe tuttavia un notevole incremento del contributo dell'UE alle risorse finanziarie delle AEV.

Quest'opzione viene scelta per i costi relativi alle funzioni regolamentari connessi alla proposta. Di fatto le AEV dovranno ridistribuire il personale esistente per elaborare una serie di norme tecniche. Inoltre non sarebbe possibile sostenere i costi supplementari connessi alla sorveglianza dei fornitori terzi di servizi di TIC critici ridistribuendo le risorse all'interno delle AEV, che devono svolgere anche altri compiti oltre a quelli previsti ai sensi della presente proposta nonché ai sensi di altri provvedimenti legislativi dell'Unione. Per giunta le funzioni di vigilanza connesse alla resilienza operativa digitale richiedono conoscenze e competenze tecniche specifiche. Dal momento che il livello di queste risorse attualmente disponibile presso le AEV è insufficiente, occorrono risorse supplementari.

Infine, secondo la proposta, ai fornitori terzi di servizi di TIC critici oggetto della sorveglianza saranno addebitate commissioni. In tal modo si prevede di coprire tutte le risorse supplementari necessarie alle AEV per lo svolgimento dei nuovi compiti e l'esercizio dei nuovi poteri.

1.6. Durata e incidenza finanziaria della proposta/iniziativa

☐ **durata limitata**

☐ Proposta/iniziativa in vigore a decorrere dal [GG/MM]AAAA fino al [GG/MM]AAAA

☐ Incidenza finanziaria dal AAAA al AAAA

☑ **durata illimitata**

Attuazione con un periodo di avviamento dal 2021

e successivo funzionamento a pieno ritmo.

1.7. Modalità di gestione previste[51]

Gestione diretta a opera della Commissione

☐ agenzie esecutive

☐ **Gestione concorrente** con gli Stati membri

☑ **Gestione indiretta** con compiti di esecuzione del bilancio affidati:

☐ a organizzazioni internazionali e loro agenzie (specificare);

☐alla BEI e al Fondo europeo per gli investimenti;

☑ agli organismi di cui agli articoli 70 e 71;

[51] Le spiegazioni sulle modalità di gestione e i riferimenti al regolamento finanziario sono disponibili sul sito BudgWeb: https://myintracomm.ec.europa.eu/budgweb/IT/man/budgmanag/Pages/budgmanag.aspx.

☐ a organismi di diritto pubblico;

☐ a organismi di diritto privato investiti di attribuzioni di servizio pubblico nella misura in cui sono dotati di sufficienti garanzie finanziarie;

☐ a organismi di diritto privato di uno Stato membro preposti all'attuazione di un partenariato pubblico-privato e che sono dotati di sufficienti garanzie finanziarie;

☐ alle persone incaricate di attuare azioni specifiche nel settore della PESC a norma del titolo V TUE, che devono essere indicate nel pertinente atto di base.

Osservazioni

Non pertinente

2. MISURE DI GESTIONE

2.1. Disposizioni in materia di monitoraggio e di relazioni

Precisare frequenza e condizioni.

In conformità degli accordi già vigenti, le AEV redigono periodicamente relazioni sulla propria attività (comprese relazioni interne ai dirigenti di grado più elevato, relazioni ai consigli di amministrazione e relazioni annuali) e sono sottoposte ad audit da parte della Corte dei conti e del servizio di audit interno della Commissione per quanto riguarda l'impiego di risorse e le prestazioni. Il monitoraggio e la comunicazione delle azioni incluse nella proposta soddisferanno le prescrizioni vigenti, nonché eventuali nuove prescrizioni derivanti dalla presente proposta.

2.2. Sistemi di gestione e di controllo

2.2.1. Giustificazione delle modalità di gestione, dei meccanismi di attuazione del finanziamento, delle modalità di pagamento e della strategia di controllo proposti

La gestione sarà indiretta tramite le AEV. Il meccanismo di finanziamento opererebbe tramite commissioni versate dai fornitori terzi di servizi di TIC critici interessati.

2.2.2. Informazioni concernenti i rischi individuati e il sistema o i sistemi di controllo interno per attenuarli

Per quanto riguarda l'uso giuridico, economico, efficiente ed efficace degli stanziamenti derivanti dalla proposta, si prevede che questa non determini nuovi rischi rilevanti che non siano già coperti da un quadro di controllo interno esistente. Potrebbe tuttavia profilarsi una nuova sfida connessa alla garanzia di una tempestiva riscossione delle commissioni dai fornitori terzi di servizi di TIC critici interessati.

2.2.3. Stima e giustificazione del rapporto costo/efficacia dei controlli (rapporto "costi del controllo ÷ valore dei fondi gestiti") e valutazione dei livelli di rischio di errore previsti (al pagamento e alla chiusura)

I sistemi di gestione e controllo previsti dai regolamenti delle AEV sono già operanti. Le AEV collaborano strettamente con il servizio di audit interno della Commissione per garantire il rispetto delle norme del caso sotto tutti gli aspetti del quadro di controllo interno. Questi accordi si applicheranno anche al ruolo attribuito alle AEV ai sensi della presente proposta. Inoltre in ogni esercizio finanziario, su raccomandazione del Consiglio, il Parlamento europeo dà a ciascuna AEV il discarico per l'esecuzione del suo bilancio.

2.3. Misure di prevenzione delle frodi e delle irregolarità

Precisare le misure di prevenzione e tutela in vigore o previste, ad esempio strategia antifrode.

Ai fini della lotta contro le frodi, la corruzione e qualsiasi altra attività illegale, alle AEV saranno applicate senza restrizioni le disposizioni del regolamento (UE, Euratom) n. 883/2013 del Parlamento europeo e del Consiglio, dell'11 settembre 2013, relativo alle indagini svolte dall'Ufficio europeo per la lotta antifrode (OLAF).

Le AEV dispongono di un'apposita strategia antifrode e del relativo piano d'azione. Le azioni rafforzate delle AEV nel settore della lotta contro le frodi rispetteranno le norme e gli orientamenti contenuti nel regolamento finanziario (misure antifrode nel quadro di una sana gestione finanziaria), le politiche dell'OLAF per la prevenzione delle frodi, le disposizioni previste dalla strategia antifrode della Commissione (COM(2011) 376), nonché quelle delineate dall'orientamento comune sulle agenzie decentrate dell'UE (luglio 2012) e dalla relativa tabella di marcia.

Inoltre i regolamenti che istituiscono le AEV e i regolamenti finanziari delle AEV fissano disposizioni per l'esecuzione e il controllo dei bilanci delle AEV insieme alle norme finanziarie applicabili, comprese quelle miranti a prevenire frodi e irregolarità.

3. INCIDENZA FINANZIARIA PREVISTA DELLA PROPOSTA/INIZIATIVA

3.1. Rubrica/rubriche del quadro finanziario pluriennale e linea/linee di bilancio di spesa interessate

Linee di bilancio esistenti

Secondo l'ordine delle rubriche del quadro finanziario pluriennale e delle linee di bilancio.

Rubrica del quadro finanziario pluriennale	Linea di bilancio	Tipo di spesa	Contributo			
	Numero	Diss./Non diss[52].	di paesi EFTA[53]	di paesi candidati[54]	di paesi terzi	ai sensi dell'articolo 21, paragrafo 2, lettera b), del regolamento finanziario

Nuove linee di bilancio di cui è chiesta la creazione

Secondo l'ordine delle rubriche del quadro finanziario pluriennale e delle linee di bilancio.

Rubrica del quadro finanziario pluriennale	Linea di bilancio	Tipo di spesa	Contributo			
	Numero	Diss./Non diss.	di paesi EFTA	di paesi candidati	di paesi terzi	ai sensi dell'articolo 21, paragrafo 2, lettera b), del regolamento finanziario

[52] Diss. = stanziamenti dissociati / Non diss. = stanziamenti non dissociati.

[53] EFTA: Associazione europea di libero scambio.

[54] Paesi candidati e, se del caso, potenziali candidati dei Balcani occidentali.

3.2. Incidenza prevista sulle spese

3.3. Sintesi dell'incidenza prevista sulle spese

Mio EUR (al terzo decimale)

Rubrica del quadro finanziario pluriennale	Numero	Rubrica

DG: <..>			2020	2021	2022	2023	2024	2025	2026	2027	**TOTALE**
	Impegni	(1)									
	Pagamenti	(2)									
TOTALE degli stanziamenti per DG <>	Impegni										
	Pagamenti										

Rubrica del quadro finanziario pluriennale		

Mio EUR (al terzo decimale)

		2022	2023	2024	2025	2026	2027	**TOTALE**
DG:								
• Risorse umane								
• Altre spese amministrative <>								
TOTALE DG	Stanziamenti							

TOTALE degli stanziamenti sotto la RUBRICA del quadro finanziario pluriennale	(Totale impegni = Totale pagamenti)							

Mio EUR (al terzo decimale) in prezzi costanti

		2022	**2023**	**2024**	**2025**	**2026**	**2027**	**TOTALE**
TOTALE degli stanziamenti sotto la RUBRICA 1 del quadro finanziario pluriennale	Impegni							
	Pagamenti							

3.3.1. Incidenza prevista sugli stanziamenti

☑ La proposta/iniziativa non comporta l'utilizzo di stanziamenti operativi.

☐ La proposta/iniziativa comporta l'utilizzo di stanziamenti operativi, come spiegato di seguito:

Stanziamenti di impegno in Mio EUR (al terzo decimale) in prezzi costanti

Specificare gli obiettivi e i risultati ⇩			2022		2023		2024		2025		2026		2027		**TOTALE**	
	RISULTATI															
	Tipo[55]	Costo medio	N.	Costo	N.	Costo	N.	Costo	N.	Costo	N.	Costo	N.	Costo	N. totale	Costo totale
OBIETTIVO SPECIFICO 1[56] …																
- Risultato																
Totale parziale dell'obiettivo specifico 1																
OBIETTIVO SPECIFICO 2...																
- Risultato																
Totale parziale dell'obiettivo specifico 2																
COSTO TOTALE																

[55] I risultati sono prodotti e servizi da fornire (ad esempio: numero di scambi di studenti finanziati, numero di km di strade costruiti, ecc.).

[56] Come descritto nella sezione 1.4.2. "Obiettivi specifici...".

3.3.2. Incidenza prevista sulle risorse umane

3.3.2.1. Sintesi

☐ La proposta/iniziativa non comporta l'utilizzo di stanziamenti amministrativi.

☑ La proposta/iniziativa comporta l'utilizzo di stanziamenti amministrativi, come spiegato di seguito:

Mio EUR (al terzo decimale) in prezzi costanti

ABE, EIOPA, ESMA	2022	2023	2024	2025	2026	2027	**TOTALE**
Agenti temporanei (gradi AD)	1,188	2,381	2,381	2,381	2,381	2,381	13,093
Agenti temporanei (gradi AST)	0,238	0,476	0,476	0,476	0,476	0,476	2,618
Agenti contrattuali							
Esperti nazionali distaccati							
TOTALE	1,426	2,857	2,857	2,857	2,857	2,857	15,711

Fabbisogno di personale (lavoratori dipendenti a tempo pieno):

ABE, EIOPA, ESMA e SEE	2022	2023	2024	2025	2026	2027	**TOTALE**
Agenti temporanei (gradi AD) ABE = 5, EIOPA = 5, ESMA = 5	15	15	15	15	15	15	15
Agenti temporanei (gradi AST) ABE = 1, EIOPA = 1, SEE = 1	3	3	3	3	3	3	3
Agenti contrattuali							
Esperti nazionali distaccati							
TOTALE	**18**	**18**	**18**	**18**	**18**	**18**	**18**

3.3.2.2. Fabbisogno previsto di risorse umane per la DG di riferimento

☑ La proposta/iniziativa non comporta l'utilizzo di risorse umane.

☐ La proposta/iniziativa comporta l'utilizzo di risorse umane, come spiegato di seguito:

Stima da esprimere in numeri interi (o, al massimo, con un decimale)

		2022	2023	2024	2025	2026	2027
• **Posti della tabella dell'organico (funzionari e agenti temporanei)**							
• **Personale esterno (in equivalenti a tempo pieno, ETP)**[57]							
XX 01 02 01 (AC, END e INT della dotazione globale)							
XX 01 02 02 (AC, AL, END, INT e JPD nelle delegazioni)							
XX 01 04 *yy*[58]	- in sede[59]						
	- nelle delegazioni						
XX 01 05 02 (AC, END, INT - ricerca indiretta)							
10 01 05 02 (AC, END, INT - ricerca diretta)							
Altre linee di bilancio (specificare)							
TOTALE							

XX è il settore o il titolo di bilancio interessato.

Il fabbisogno di risorse umane è coperto dal personale della DG già assegnato alla gestione dell'azione e/o riassegnato all'interno della stessa DG, integrato dall'eventuale dotazione supplementare concessa alla DG responsabile nell'ambito della procedura annuale di assegnazione, tenendo conto dei vincoli di bilancio.

Descrizione dei compiti da svolgere:

Funzionari e agenti temporanei	
Personale esterno	

La descrizione del calcolo dei costi per equivalente a tempo pieno deve figurare nell'allegato V, sezione 3.

[57] AC = agente contrattuale; AL = agente locale; END = esperto nazionale distaccato; INT = personale interinale; JPD = giovane professionista in delegazione.

[58] Sottomassimale per il personale esterno previsto dagli stanziamenti operativi (ex linee "BA").

[59] Principalmente per i fondi strutturali, il Fondo europeo agricolo per lo sviluppo rurale (FEASR) e il Fondo europeo per la pesca (FEP).

3.3.3. Compatibilità con il quadro finanziario pluriennale attuale

☑ La proposta/iniziativa è compatibile con il quadro finanziario pluriennale attuale.

☐ La proposta/iniziativa richiederà una riprogrammazione della pertinente rubrica del quadro finanziario pluriennale.

☐ La proposta/iniziativa richiede l'applicazione dello strumento di flessibilità o la revisione del quadro finanziario pluriennale[60].

Spiegare la necessità, precisando le rubriche e le linee di bilancio interessate e gli importi corrispondenti. […]

3.3.4. Partecipazione di terzi al finanziamento

☐ La proposta/iniziativa non prevede cofinanziamenti da terzi.

☑ La proposta/iniziativa prevede il cofinanziamento indicato di seguito:

Mio EUR (al terzo decimale)

ABE

	2022	2023	2024	2025	2026	2027	Totale
I costi sono coperti al 100 % da commissioni pagate dalle entità sottoposte a vigilanza[61]	1,373	1,948	1,748	1,748	1,748	1,748	10,313
TOTALE degli stanziamenti cofinanziati	1,373	1,948	1,748	1,748	1,748	1,748	10,313

EIOPA

	2022	2023	2024	2025	2026	2027	Totale
I costi sono coperti al 100 % da commissioni pagate dalle entità sottoposte a vigilanza[62]	1,305	1,811	1,611	1,611	1,611	1,611	9,560
TOTALE degli stanziamenti cofinanziati	1,305	1,811	1,611	1,611	1,611	1,611	9,560

60 Cfr. articoli 11 e 17 del regolamento (UE, Euratom) n. 1311/2013 del Consiglio, che stabilisce il quadro finanziario pluriennale per il periodo 2014-2020.

61 100 % dei costi totali stimati più gli interi contributi pensionistici dei datori di lavoro.

62 100 % dei costi totali stimati più gli interi contributi pensionistici dei datori di lavoro.

ESMA

	2022	2023	2024	2025	2026	2027	Totale
I costi sono coperti al 100 % da commissioni pagate dalle entità sottoposte a vigilanza[63]	1,373	1,948	1,748	1,748	1,748	1,748	10,313
TOTALE degli stanziamenti cofinanziati	1,373	1,948	1,748	1,748	1,748	1,748	10,313

3.4. Incidenza prevista sulle entrate

☑ La proposta/iniziativa non ha incidenza finanziaria sulle entrate.

☐ La proposta/iniziativa ha l'incidenza finanziaria seguente:

☐ sulle risorse proprie

☐ su altre entrate

☐ indicare se le entrate sono destinate a linee di spesa specifiche

Mio EUR (al terzo decimale)

Linea di bilancio delle entrate:	Stanziamenti disponibili per l'esercizio in corso	Incidenza della proposta/iniziativa[64]						
		Anno **N**	Anno **N+1**	Anno **N+2**	Anno **N+3**	Inserire gli anni necessari per evidenziare la durata dell'incidenza (cfr. punto 1.6)		
Articolo								

Per quanto riguarda le entrate varie con destinazione specifica, precisare le linee di spesa interessate.

[…]

Precisare il metodo di calcolo dell'incidenza sulle entrate.

[…]

63 100 % dei costi totali stimati più gli interi contributi pensionistici dei datori di lavoro.

64 Per le risorse proprie tradizionali (dazi doganali, contributi zucchero), indicare gli importi netti, cioè gli importi lordi al netto del 20 % per spese di riscossione.

ALLEGATO

Ipotesi generali

Titolo I – Spese relative al personale

Nel calcolo delle spese relative al personale sono state applicate le ipotesi specifiche seguenti, basate sul fabbisogno di personale individuato illustrato di seguito:

- il costo del personale supplementare assunto nel 2022 è calcolato su sei mesi, dato il tempo che si presume sarà necessario per l'assunzione;
- il costo medio annuo è di 150 000 EUR, di cui 25 000 EUR di costi di "habillage" (edifici, sistemi e dispositivi informatici, ecc.);
- I coefficienti correttori applicabili alle retribuzioni del personale a Parigi (ABE ed ESMA) e a Francoforte (EIOPA) sono pari rispettivamente a 117,7 e 99,4;
- I contributi pensionistici del datore di lavoro per gli agenti temporanei sono stati calcolati sulla base degli stipendi base standard inclusi nei costi medi annuali standard, ossia 95 660 EUR;
- tutti gli altri agenti temporanei sono AD5 e AST.

Titolo II – Spese per infrastrutture e di funzionamento

I costi si basano sulla moltiplicazione del numero di dipendenti per la parte dell'anno impiegato per il costo standard di "habillage", pari a 25 000 EUR.

Titolo III – Spese operative

I costi sono stimati sulla base delle ipotesi seguenti:

- I costi di traduzione per ciascuna AEV sono fissati a 350 000 EUR all'anno;
- Si ipotizza che i costi informatici una tantum per AEV, pari a 500 000 EUR, saranno sostenuti nel corso dei due anni 2022 e 2023 sulla base di una ripartizione del 50 % - 50 %. I costi di manutenzione annuale fino al 2024 sono stimati a 50 000 EUR per AEV;
- I costi annuali di vigilanza in loco sono stimati a 200 000 EUR per AEV.

Le stime sopra riportate comportano i costi annui seguenti:

Rubrica del quadro finanziario pluriennale	Numero	

Prezzi costanti

ABE:			2022	2023	2024	2025	2026	2027	**TOTALE**
Titolo 1:	Impegni	(1)	0,498	0,998	0,998	0,998	0,998	0,998	5,488
	Pagamenti	(2)	0,498	0,998	0,998	0,998	0,998	0,998	5,488
Titolo 2:	Impegni	(1a)	0,075	0,150	0,150	0,150	0,150	0,150	0,825
	Pagamenti	(2a)	0,075	0,150	0,150	0,150	0,150	0,150	0,825
Titolo 3:	Impegni	(3a)	0,800	0,800	0,600	0,600	0,600	0,600	4,000
	Pagamenti	(3b)	0,800	0,800	0,600	0,600	0,600	0,600	4,000
TOTALE degli stanziamenti per l'ABE	Impegni	=1+1a+3a	1,373	1,948	1,748	1,748	1,748	1,748	10,313
	Pagamenti	=2+2a +3b	1,373	1,948	1,748	1,748	1,748	1,748	10,313

EIOPA:			2022	2023	2024	2025	2026	2027	**TOTALE**
Titolo 1:	Impegni	(1)	0,430	0,861	0,861	0,861	0,861	0,861	4,735
	Pagamenti	(2)	0,430	0,861	0,861	0,861	0,861	0,861	4,735
Titolo 2:	Impegni	(1a)	0,075	0,150	0,150	0,150	0,150	0,150	0,825
	Pagamenti	(2a)	0,075	0,150	0,150	0,150	0,150	0,150	0,825
Titolo 3:	Impegni	(3a)	0,800	0,800	0,600	0,600	0,600	0,600	4,000
	Pagamenti	(3b)	0,800	0,800	0,600	0,600	0,600	0,600	4,000
TOTALE degli stanziamenti per l'EIOPA	Impegni	=1+1a+3a	1,305	1,811	1,611	1,611	1,611	1,611	9,560
	Pagamenti	=2+2a +3b	1,305	1,811	1,611	1,611	1,611	1,611	9,560

ESMA:			2022	2023	2024	2025	2026	2027	**TOTALE**
Titolo 1:	Impegni	(1)	0,498	0,998	0,998	0,998	0,998	0,998	5,488
	Pagamenti	(2)	0,498	0,998	0,998	0,998	0,998	0,998	5,488
Titolo 2:	Impegni	(1a)	0,075	0,150	0,150	0,150	0,150	0,150	0,825
	Pagamenti	(2a)	0,075	0,150	0,150	0,150	0,150	0,150	0,825
Titolo 3:	Impegni	(3a)	0,800	0,800	0,600	0,600	0,600	0,600	4,000
	Pagamenti	(3b)	0,800	0,800	0,600	0,600	0,600	0,600	4,000
TOTALE degli stanziamenti per l'ESMA	Impegni	=1+1a+3a	1,373	1,948	1,748	1,748	1,748	1,748	10,313
	Pagamenti	=2+2a +3b	1,373	1,948	1,748	1,748	1,748	1,748	10,313

La proposta comporta l'utilizzo di stanziamenti operativi, come spiegato di seguito:

Stanziamenti di impegno in Mio EUR (al terzo decimale) in prezzi costanti

ABE

Specificare gli obiettivi e i risultati ⇩			2022		2023		2024		2025		2026		2027			
	RISULTATI															
	Tipo[65]	Costo medio	N.	Costo	N.	Costo	N.	Costo	N.	Costo	N.	Costo	N.	Costo	N. totale	Costo totale
OBIETTIVO SPECIFICO 1[66] Sorveglianza diretta dei fornitori terzi di servizi di TIC critici																
- Risultato				0,800		0,800		0,600		0,600		0,600		0,600		4,000
Totale parziale dell'obiettivo specifico 1																
OBIETTIVO SPECIFICO 2...																
- Risultato																
Totale parziale dell'obiettivo specifico 2																
COSTO TOTALE				**0,800**		**0,800**		**0,600**		**0,600**		**0,600**		**0,600**		**4,000**

EIOPA

Specificare gli obiettivi e i risultati ⇩			2022		2023		2024		2025		2026		2027			
	RISULTATI															
	Tipo[67]	Costo medio	N.	Costo	N.	Costo	N.	Costo	N.	Costo	N.	Costo	N.	Costo	N. totale	Costo totale
OBIETTIVO SPECIFICO 1[68] Sorveglianza diretta dei fornitori terzi di servizi di TIC critici																
- Risultato				0,800		0,800		0,600		0,600		0,600		0,600		4,000

[65] I risultati sono prodotti e servizi da fornire (ad esempio: numero di scambi di studenti finanziati, numero di km di strade costruiti, ecc.).

[66] Come descritto nella sezione 1.4.2. "Obiettivi specifici...".

[67] I risultati sono prodotti e servizi da fornire (ad esempio: numero di scambi di studenti finanziati, numero di km di strade costruiti, ecc.).

[68] Come descritto nella sezione 1.4.2. "Obiettivi specifici...".

Totale parziale dell'obiettivo specifico 1															
OBIETTIVO SPECIFICO 2...															
- Risultato															
Totale parziale dell'obiettivo specifico 2															
COSTO TOTALE		**0,800**		**0,800**		**0,600**		**0,600**		**0,600**		**0,600**		**4,000**	

ESMA

Specificare gli obiettivi e i risultati ⇩			2022		2023		2024		2025		2026		2027			
	RISULTATI															
	Tipo[69]	Costo medio	N.	Costo	N.	Costo	N.	Costo	N.	Costo	N.	Costo	N.	Costo	N. totale	Costo totale
OBIETTIVO SPECIFICO 1[70] Sorveglianza diretta dei fornitori terzi di servizi di TIC critici																
- Risultato				0,800		0,800		0,600		0,600		0,600		0,600		4,000
Totale parziale dell'obiettivo specifico 1																
OBIETTIVO SPECIFICO 2...																
- Risultato																
Totale parziale dell'obiettivo specifico 2																
COSTO TOTALE				**0,800**		**0,800**		**0,600**		**0,600**		**0,600**		**0,600**		**4,000**

[69] I risultati sono prodotti e servizi da fornire (ad esempio: numero di scambi di studenti finanziati, numero di km di strade costruiti, ecc.).

[70] Come descritto nella sezione 1.4.2. "Obiettivi specifici...".

Le attività di sorveglianza sono interamente finanziate da commissioni pagate dalle entità sottoposte a sorveglianza, come segue:

ABE

	2022	2023	2024	2025	2026	2027	Totale
I costi sono coperti al 100 % da commissioni pagate dalle entità sottoposte a sorveglianza[71]	1,373	1,948	1,748	1,748	1,748	1,748	10,313
TOTALE degli stanziamenti cofinanziati	1,373	1,948	1,748	1,748	1,748	1,748	10,313

EIOPA

	2022	2023	2024	2025	2026	2027	Totale
I costi sono coperti al 100 % da commissioni pagate dalle entità sottoposte a sorveglianza[72]	1,305	1,811	1,611	1,611	1,611	1,611	9,560
TOTALE degli stanziamenti cofinanziati	1,305	1,811	1,611	1,611	1,611	1,611	9,560

ESMA

	2022	2023	2024	2025	2026	2027	Totale
I costi sono coperti al 100 % da commissioni pagate dalle entità sottoposte a sorveglianza[73]	1,373	1,948	1,748	1,748	1,748	1,748	10,313
TOTALE degli stanziamenti cofinanziati	1,373	1,948	1,748	1,748	1,748	1,748	10,313

[71] 100 % dei costi totali stimati più gli interi contributi pensionistici dei datori di lavoro.
[72] 100 % dei costi totali stimati più gli interi contributi pensionistici dei datori di lavoro.
[73] 100 % dei costi totali stimati più gli interi contributi pensionistici dei datori di lavoro.

INFORMAZIONI SPECIFICHE

Poteri di sorveglianza diretta

Si rilevi, anzitutto, che i soggetti su cui l'ESMA esercita la vigilanza diretta dovrebbero versarle una commissione (costo una tantum di registrazione e costi ricorrenti della vigilanza). È il caso delle agenzie di rating del credito (cfr. il regolamento delegato (UE) n. 272/2012 della Commissione) e dei repertori di dati sulle negoziazioni (regolamento delegato (UE) n. 1003/2013 della Commissione).

Ai sensi della presente proposta legislativa, alle AEV saranno affidati nuovi compiti volti a promuovere la convergenza per quanto riguarda gli approcci di vigilanza ai rischi relativi alle TIC derivanti da terzi nel settore finanziario, sottoponendo i fornitori terzi di servizi di TIC critici al quadro di sorveglianza dell'Unione.

Il quadro di sorveglianza previsto dalla presente proposta si fonda sull'architettura istituzionale esistente nel settore dei servizi finanziari, per cui il comitato congiunto delle AEV garantisce il coordinamento intersettoriale in tutte le questioni concernenti i rischi relativi alle TIC, conformemente ai propri compiti in materia di cibersicurezza, coadiuvato dal sottocomitato pertinente (forum di sorveglianza) che svolge il lavoro preparatorio per decisioni individuali e raccomandazioni collettive rivolte ai fornitori terzi di servizi di TIC critici.

Tramite questo quadro, l'AEV designata come autorità di sorveglianza capofila per ciascun fornitore terzo di servizi di TIC critico riceve poteri idonei a garantire l'adeguato monitoraggio su scala paneuropea dei fornitori di servizi tecnologici che assolvono una funzione critica per il funzionamento del settore finanziario. I compiti di sorveglianza sono delineati nella proposta e ulteriormente chiariti nella relazione. Comprendono il diritto di richiedere tutta la documentazione e le informazioni pertinenti per svolgere indagini e ispezioni di carattere generale, per formulare raccomandazioni e successivamente presentare relazioni sulle azioni intraprese o i rimedi attuati per rispondere a tali raccomandazioni.

Per assolvere i nuovi compiti previsti dalla presente proposta, le AEV assumono pertanto altro personale specializzato nei rischi relativi alle TIC e destinato a valutare le dipendenze da terzi.

Il fabbisogno di risorse umane può esser stimato a sei dipendenti a tempo pieno per ciascuna autorità (cinque AD e un AST che coadiuvi gli AD). Le AEV sostengono anche ulteriori costi informatici, stimati a 500 000 EUR (una tantum) oltre a 50 000 EUR all'anno per ciascuna delle tre AEV come costi di manutenzione. Un elemento importante per l'assolvimento dei nuovi compiti è costituito dalle missioni per lo svolgimento di ispezioni e audit in loco, che si può stimare a 200 000 EUR all'anno per ciascuna AEV. Anche i costi di traduzione per i diversi documenti che le AEV riceveranno dai fornitori terzi di servizi di TIC critici sono inclusi tra i costi operativi e ammontano a 350 000 EUR all'anno.

Tutti i costi amministrativi di cui sopra saranno finanziati per intero con i contributi annuali versati alle AEV dai fornitori terzi di servizi di TIC critici (senza alcuna incidenza sul bilancio dell'UE).