Parlamento europeo
2019-2024

Documento di seduta

A9-0341/2021

7.12.2021

***I
RELAZIONE

sulla 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
(COM(2020)0595 – C9-0304/2020 – 2020/0266(COD))

Commissione per i problemi economici e monetari

Relatore: Billy Kelleher

Significato dei simboli utilizzati

*	Procedura di consultazione
***	Procedura di approvazione
***I	Procedura legislativa ordinaria (prima lettura)
***II	Procedura legislativa ordinaria (seconda lettura)
***III	Procedura legislativa ordinaria (terza lettura)

(La procedura indicata dipende dalla base giuridica proposta nel progetto di atto.)

Emendamenti a un progetto di atto

Emendamenti del Parlamento presentati su due colonne

Le soppressioni sono evidenziate in ***corsivo grassetto*** nella colonna di sinistra. Le sostituzioni sono evidenziate in ***corsivo grassetto*** nelle due colonne. Il testo nuovo è evidenziato in ***corsivo grassetto*** nella colonna di destra.

La prima e la seconda riga del blocco d'informazione di ogni emendamento identificano la parte di testo interessata del progetto di atto in esame. Se un emendamento verte su un atto esistente che il progetto di atto intende modificare, il blocco d'informazione comprende anche una terza e una quarta riga che identificano rispettivamente l'atto esistente e la disposizione interessata di quest'ultimo.

Emendamenti del Parlamento presentati in forma di testo consolidato

Le parti di testo nuove sono evidenziate in ***corsivo grassetto***. Le parti di testo soppresse sono indicate con il simbolo ▌ o sono barrate. Le sostituzioni sono segnalate evidenziando in ***corsivo grassetto*** il testo nuovo ed eliminando o barrando il testo sostituito.
A titolo di eccezione, le modifiche di carattere strettamente tecnico apportate dai servizi in vista dell'elaborazione del testo finale non sono evidenziate.

INDICE

Pagina

PROGETTO DI RISOLUZIONE LEGISLATIVA DEL PARLAMENTO EUROPEO 5

PROCEDURA DELLA COMMISSIONE COMPETENTE PER IL MERITO 101

VOTAZIONE FINALE PER APPELLO NOMINALE IN SEDE DI COMMISSIONE COMPETENTE PER IL MERITO.....103

PROGETTO DI RISOLUZIONE LEGISLATIVA DEL PARLAMENTO EUROPEO

sulla 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 (COM(2020)0595 – C9-0304/2020 – 2020/0266(COD))

(Procedura legislativa ordinaria: prima lettura)

Il Parlamento europeo,

– vista la proposta della Commissione al Parlamento europeo e al Consiglio (COM(2020)0595),

– visti l'articolo 294, paragrafo 2, e l'articolo 114 del trattato sul funzionamento dell'Unione europea, a norma dei quali la proposta gli è stata presentata dalla Commissione (C9-0304/2020),

– visto l'articolo 294, paragrafo 3, del trattato sul funzionamento dell'Unione europea,

– visto il parere del Comitato economico e sociale europeo del 24 febbraio 2021[1],

– visto l'articolo 59 del suo regolamento,

– vista la relazione della commissione per i problemi economici e monetari (A9-0341/2021),

1. adotta la posizione in prima lettura figurante in appresso;

2. chiede alla Commissione di presentargli nuovamente la proposta qualora la sostituisca, la modifichi sostanzialmente o intenda modificarla sostanzialmente;

2. incarica il suo Presidente di trasmettere la posizione del Parlamento al Consiglio e alla Commissione nonché ai parlamenti nazionali.

[1] GU L 155 del 30.4.2021, pag. 38.

Emendamento 1

EMENDAMENTI DEL PARLAMENTO EUROPEO*

alla proposta della Commissione

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[2],

visto il parere del Comitato economico e sociale europeo[3],

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 ***deve*** ancora ***essere*** sufficientemente integrata nei loro quadri operativi.

(2) Negli ultimi decenni l'uso delle TIC ha conquistato un ruolo essenziale nella finanza e

---

* Emendamenti: il testo nuovo o modificato è evidenziato in grassetto corsivo il testo nuovo o modificato è evidenziato in grassetto corsivo e le soppressioni sono segnalate con il simbolo ▌.

2 [*aggiungere riferimento*] GU C del , pag. .

3 GU L 155 del 30.4.2021, pag. 38.

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 gestione dei crediti e le operazioni di back-office. ***Anche il settore assicurativo è stato trasformato dall'uso delle TIC, dall'emergere di intermediari assicurativi digitali che operano con specifiche tecnologie TIC (InsurTech) alla sottoscrizione di assicurazioni digitali e alla distribuzione di contratti.*** 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.

(3) In una relazione del 2020 incentrata sul rischio informatico sistemico[4] , 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 all'intero sistema finanziario[5] , 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. ***Di conseguenza, è necessario considerare il rischio relativo alle TIC nel contesto di un sistema finanziario globale altamente interconnesso in cui occorre assegnare priorità alla coerenza della regolamentazione internazionale e alla cooperazione tra le autorità competenti a livello globale.***

(5) Benché a livello nazionale ed europeo siano state adottate iniziative politiche e

---

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

5 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.

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[6] del 2018 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 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, ***rafforzando*** i mandati delle autorità di vigilanza finanziaria ***per gestire i rischi relativi alle TIC nel settore finanziario, proteggere*** l'integrità ***e l'efficienza del*** mercato ***unico ed agevolarne il corretto funzionamento***.

(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

---

[6] 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: P*er un settore finanziario europeo più competitivo e innovativo* COM/2018/0109 final, https://ec.europa.eu/info/publications/180308-action-plan-fintech_en.

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.

(10 bis) Anche la creazione e il mantenimento di reti e infrastrutture informatiche adeguate è una condizione preliminare fondamentale per l'efficace aggregazione dei dati sui rischi e le prassi di segnalazione dei rischi, che rappresentano a loro volta un requisito essenziale per una gestione sana e sostenibile del rischio e per i processi decisionali degli enti creditizi. Nel 2013 il Comitato di Basilea per la vigilanza bancaria (CBVB) ha pubblicato una serie di principi per un'efficace aggregazione e reportistica dei dati di rischio (CBVB 239) sulla base di due principi generali per la governance e l'infrastruttura informatica, da attuare entro l'inizio del 2016. Conformemente al rapporto della Banca centrale europea (BCE) del maggio 2018 sulla revisione tematica sull'efficace aggregazione dei dati sui rischi e la segnalazione dei rischi del maggio 2018 e al rapporto sui progressi compiuti dal CBVB nell'aprile 2020, i progressi in materia di attuazione compiuti da banche di importanza sistemica a livello globale sono stati insoddisfacenti e fonte di preoccupazione. Al fine di agevolare il rispetto e l'allineamento alle norme internazionali, la Commissione, in stretta cooperazione con la BCE e previa consultazione dell'ABE e del CERS, dovrebbe elaborare una relazione per valutare in che modo i principi del CBVB 239 interagiscono con le disposizioni del presente regolamento ed eventualmente in che modo tali principi dovrebbero essere incorporati nel diritto dell'Unione.

(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. ***Con la presente iniziativa si vuole anche accrescere la consapevolezza dei rischi TIC e riconoscere che gli incidenti connessi alle TIC e la mancanza di resilienza operativa potrebbero compromettere la solidità finanziaria delle entità finanziarie.***

(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, ***modulati in funzione delle rispettive dimensioni, caratteristiche, complessità e profili di rischio***. La coerenza contribuisce ad accrescere la fiducia nel sistema finanziario e a preservarne la stabilità, soprattutto in tempi in cui ***l'elevata dipendenza da sistemi di TIC, piattaforme e*** infrastrutture ▌ 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.

(14 bis) Tuttavia, l'attuazione del presente regolamento non dovrebbe ostacolare l'innovazione per quanto riguarda il modo in cui i soggetti finanziari affrontano le

questioni di resilienza operativa digitale nel rispetto delle sue disposizioni, neanche per quanto riguarda i servizi che offrono o i servizi offerti da fornitori terzi di servizi TIC.

(15) Accanto alla legislazione sui servizi finanziari, la direttiva (UE) 2016/1148 del Parlamento europeo e del Consiglio[7] 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***, per le entità finanziarie,*** 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. ***L'organismo congiunto di sorveglianza, le*** autorità ***di vigilanza capofila e le autorità*** competenti ***previsti*** dal presente regolamento dovrebbero anche consultare i CSIRT nazionali designati ai sensi dell'articolo 9 della direttiva (UE) 2016/1148 e collaborare con loro.

Inoltre, il presente regolamento dovrebbe garantire che la rete di CSIRT istituita dalla direttiva (UE) 2016/1148 riceva le informazioni concernenti gli incidenti gravi connessi alle TIC.

(18) È inoltre importante garantire la coerenza ***sia*** con la direttiva sulle infrastrutture critiche europee, di cui attualmente è in corso una revisione volta a migliorare la protezione e la

[7] 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).

resilienza delle infrastrutture critiche rispetto alle minacce non informatiche, ***sia con la direttiva sulla resilienza dei soggetti critici***[8]***,*** con possibili implicazioni per il settore finanziario.

(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 ***e i requisiti sia sostanziali che procedurali applicabili ai fornitori terzi di servizi di TIC critici ai sensi del presente regolamento dovrebbero essere coerenti e senza soluzione di continuità con quelli applicabili ai sensi di tale direttiva***. 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***, nonché*** per la gestione dei rischi relativi alle TIC derivanti da terzi ***e fornitori di servizi di TIC intragruppo***. È opportuno rendere più rigorosi gli obblighi in materia di resilienza operativa digitale per il sistema finanziario, consentendo tuttavia un'applicazione proporzionata delle prescrizioni ***tenendo anche conto delle loro caratteristiche, dimensioni, complessità e profilo generale di rischio***.

(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) e dal gruppo di cooperazione NIS per le entità finanziarie istituito ai sensi della direttiva[9] (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.

(21 bis) Al fine di ridurre l'onere amministrativo ed evitare la complessità e la duplicazione degli obblighi di segnalazione per i fornitori di servizi di pagamento che

---

[8] 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).

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

rientrano nell'ambito di applicazione del presente regolamento, è opportuno che gli obblighi di segnalazione degli incidenti ai sensi della direttiva (UE) 2015/2366 decadano. Pertanto, gli enti creditizi, gli istituti di moneta elettronica e gli istituti di pagamento dovrebbero segnalare, ai sensi del presente regolamento, tutti gli incidenti operativi o quelli relativi alla sicurezza dei pagamenti e non, precedentemente segnalati ai sensi della direttiva (UE) 2015/2366, indipendentemente dal fatto che gli incidenti riguardino le TIC o meno.

(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 ***realizzino un solido*** regime di segnalazione degli incidenti connessi alle TIC con le prescrizioni ***atte a colmare le lacune*** nella legislazione ***settoriale sui servizi finanziari***, 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 alle rispettive autorità competenti ***attraverso il quadro semplificato descritto nel presente regolamento***. 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 ***talvolta*** privi di coordinamento che affrontavano i medesimi problemi in modo differente. Ne è scaturita una duplicazione di costi per le entità finanziarie transfrontaliere ***e potrebbe compromettere*** 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[10], 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 ***forniscono servizi*** critici per le entità finanziarie. ***Poiché la fornitura intragruppo di servizi di TIC non comporta gli stessi rischi, i fornitori di servizi di TIC che appartengono allo stesso gruppo o allo stesso sistema di tutela istituzionale non dovrebbero essere definiti come fornitori terzi di***

[10] 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).

servizi di TIC critici.

(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. ***È quindi importante rafforzare gli accordi di cooperazione e reportistica fra le entità finanziarie e le autorità competenti, nonché condividere le informazioni con il pubblico, al fine di sviluppare un quadro aperto di condivisione dei dati e un approccio "security by design" (sicurezza sin dalla progettazione), essenziali per accrescere la resilienza operativa e la preparazione del settore finanziario nei confronti di rischi connessi alle TIC. Gli accordi di condivisione delle informazioni dovrebbero sempre tenere in debita considerazione i potenziali rischi connessi alla sicurezza informatica, alla protezione dei dati o alla riservatezza commerciale.***

(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 esistono meccanismi di condivisione delle informazioni estesi in maniera omogenea a tutta l'Unione e corrispondenti alle esigenze di un settore finanziario integrato. ***È pertanto importante rafforzare tali canali di comunicazione e disporre dell'apporto da parte di autorità diverse da quelle di vigilanza, ove necessario e pertinente, durante l'intero ciclo di vigilanza.***

(32) È ▌ opportuno incoraggiare le entità finanziarie ***anche*** 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[11] vigenti in materia di concorrenza e operare nel pieno rispetto delle norme dell'UE sulla protezione dei dati, in particolare il regolamento (UE) 2016/679 del Parlamento europeo

[11] 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).

e del Consiglio[12], 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***, compresi i requisiti del quadro per la gestione dei rischi,*** dovrebbe tener conto delle differenze significative che si registrano tra le entità finanziarie in termini di dimensioni, ***caratteristiche, complessità e profili di rischio***. 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***, le caratteristiche, la complessità e il relativo profilo di rischio,*** 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 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 ***le stime di*** tutti i costi e le perdite provocati dalle ***significative*** perturbazioni delle TIC, ***dai gravi incidenti connessi alle TIC,*** nonché i risultati degli esami effettuati dopo l'incidente in occasione di ***tali*** 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

[12] 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).

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[13], 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 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***, valutando se la funzione sia una funzione critica o importante.*** 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,

---

[13] 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

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 ***per la segnalazione di gravi incidenti connessi alle TIC,*** 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***, diverse dalle microimprese,*** 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. ***Inoltre, al fine di rafforzare la cooperazione con paesi terzi affidabili in fatto di resilienza delle entità finanziarie, la Commissione e le autorità competenti dovrebbero cercare di istituire un quadro per il riconoscimento reciproco dei risultati dei test di penetrazione basati su minacce.***

Gli Stati membri dovrebbero designare un'unica autorità pubblica responsabile dei test di penetrazione basati su minacce nel settore finanziario a livello nazionale. L'autorità pubblica unica potrebbe essere, tra l'altro, un'autorità nazionale competente o un'autorità pubblica designata a norma dell'articolo 8 della direttiva (UE) 2016/1148 (NIS). L'autorità pubblica unica dovrebbe essere responsabile del rilascio degli attestati che certifichino che i test di penetrazione basati su minacce sono stati effettuati in conformità ai requisiti. Tali attestati dovrebbero facilitare il reciproco riconoscimento dei test tra le autorità competenti.

Alcuni soggetti finanziari hanno la capacità di effettuare test interni avanzati, mentre altri faranno ricorso a tester esterni provenienti dall'Unione o da un paese terzo. Di conseguenza, è importante che tutti i tester siano soggetti a requisiti precisi identici. Al fine di garantire l'indipendenza dei tester interni, il loro uso dovrebbe essere soggetto all'approvazione dell'autorità competente.

La metodologia concernente i test di penetrazione basati su minacce non dovrebbe essere obbligatoria, ma l'uso del quadro TIBER-EU esistente dovrebbe essere considerato conforme ai requisiti dei test di penetrazione basati su minacce di cui al presente regolamento.

Fino all'entrata in vigore del presente regolamento e all'elaborazione e adozione da parte delle AEV delle previste norme tecniche di regolamentazione in relazione ai test di penetrazione basati su minacce, le entità finanziarie dovrebbero seguire gli orientamenti e i quadri pertinenti dell'Unione applicabili ai test di penetrazione basati su informazioni, giacché essi continueranno ad applicarsi dopo l'entrata in vigore del presente regolamento.

(44 bis) La responsabilità della conduzione del test di penetrazione basati su minacce

— e della gestione della cibersicurezza in generale e della prevenzione degli attacchi informatici — dovrebbe spettare interamente all'entità finanziaria, e gli attestati forniti dalle autorità dovrebbero essere finalizzati esclusivamente al riconoscimento reciproco e non dovrebbero precludere azioni di follow-up sul livello di rischio delle TIC cui l'entità finanziaria è esposta, né essere visti come un avallo delle sue capacità di gestione e mitigazione dei rischi relative alle TIC.

(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 - specie in relazione alla fornitura di funzioni critiche o importanti da parte di 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 ***delle caratteristiche,*** 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***, nonché in funzione del fatto che i servizi di TIC siano forniti da un fornitore intragruppo di servizi o da un fornitore terzo di servizi.***

(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, ***e si dovrebbero adottare misure correttive e rimediative, fra cui*** l'estinzione ***parziale o totale*** dei contratti ***ove si verifichino almeno*** una serie di circostanze che attestino ***gravi*** 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 ▌. 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. ***L'organismo congiunto di sorveglianza che effettua*** la sorveglianza su ciascun fornitore terzo di servizi di TIC critico ***e l'AEV***

designata a effettuare la sorveglianza quotidiana ("l'autorità di sorveglianza capofila") ***dovrebbero, nell'esercizio dei compiti di sorveglianza,*** 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[14].

(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 le garanzie di accesso, ripristino e restituzione in caso di insolvenza, risoluzione, cessazione delle operazioni commerciali del fornitore terzo di servizi di TIC ***o risoluzione degli accordi contrattuali,*** 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 ***attinente ai servizi forniti dal fornitore terzo di servizi di TIC all'entità finanziaria ai livelli di servizio convenuti,*** senza costi supplementari o a un costo stabilito ex ante. ***Non sono coperti dal presente regolamento i servizi TIC accessori da cui le entità finanziarie non sono operativamente dipendenti.***

Inoltre, la definizione di "funzione critica o importante" di cui al presente regolamento dovrebbe comprendere la definizione di "funzioni essenziali" di cui all'articolo 2, paragrafo 1, punto (35), della direttiva 2014/59/UE del Parlamento europeo e del Consiglio, del 15 maggio 2014[15]***. Di conseguenza, le funzioni che sono***

---

14 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.

15 ***Direttiva 2014/59/UE del Parlamento europeo e del Consiglio, del 15 maggio 2014, che istituisce un quadro di risanamento e risoluzione degli enti creditizi e delle imprese di investimento e che modifica***

funzioni essenziali ai sensi della direttiva 2014/59/UE dovrebbero essere funzioni critiche o importanti ai sensi del presente regolamento.

(53) ***Nel caso di accordi contrattuali per funzioni critiche o importanti,*** 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'organismo congiunto di sorveglianza e l'autorità di sorveglianza capofila*** dell'entità finanziaria ***dovrebbero*** 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 ***e prestando nel contempo attenzione a non perturbare i servizi forniti ad altri clienti del fornitore terzo di servizi di TIC. L'entità finanziaria e il fornitore terzo di servizi di TIC dovrebbero poter concordare sulla possibilità di delegare i diritti di accesso, ispezione e audit a un terzo indipendente.***

(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. ***Inoltre, gli enti creditizi dovrebbero garantire che i pertinenti contratti TIC siano solidi e pienamente applicabili in caso di risoluzione dell'ente creditizio. In linea con le aspettative delle autorità di risoluzione, gli enti creditizi dovrebbero garantire che i pertinenti contratti di servizi di TIC siano resilienti in caso di risoluzione. Finché continuano a essere svolte funzioni TIC critiche o importanti, tali entità finanziarie dovrebbero garantire che i contratti contengano, tra l'altro, clausole di non estinzione, di non sospensione e di immodificabilità in caso di ristrutturazione o risoluzione.***

(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.

(55 bis) Le AEV dovrebbero essere incaricate di elaborare norme tecniche regolamentari e di attuazione che specifichino le aspettative delle politiche in materia

---

la direttiva 82/891/CEE del Consiglio, e le direttive 2001/24/CE, 2002/47/CE, 2004/25/CE, 2005/56/CE, 2007/36/CE, 2011/35/UE, 2012/30/UE e 2013/36/UE e i regolamenti (UE) n. 1093/2010 e (UE) n. 648/2012, del Parlamento europeo e del Consiglio (GU L 173 del 12.6.2014, pag. 190).

di gestione dei rischi relativi alle TIC derivanti da terzi e in materia di obblighi contrattuali. Fino all'entrata in vigore di tali norme, le entità finanziarie dovrebbero seguire gli orientamenti e le altre misure pertinenti emanati dalle AEV e dalle autorità competenti.

(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 ***nel quadro di*** 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 ***che contribuiscono all'adempimento dei compiti*** a livello dell'Eurosistema ▌di cui all'articolo 127, paragrafo 2, del trattato sul funzionamento dell'Unione europea dovrebbero esserne di conseguenza esentati. ***Analogamente, le imprese che fanno parte di un gruppo finanziario e che forniscono servizi di TIC esclusivamente a entità finanziarie dello stesso gruppo non dovrebbero essere soggette al meccanismo di designazione.***

(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. ***La prescrizione di disporre di un'impresa, come una controllata, costituita nell'Unione a norma del diritto di uno Stato membro, ha lo scopo di fornire un punto di contatto tra, da un lato, il fornitore terzo di servizi di TIC e, dall'altro, l'autorità di sorveglianza capofila e l'organismo congiunto di sorveglianza, nonché di garantire che l'autorità di sorveglianza capofila e l'organismo congiunto di sorveglianza siano in grado di svolgere i propri compiti e di esercitare i propri poteri di sorveglianza e di applicazione secondo quanto previsto dal presente regolamento. I servizi appaltati del fornitore terzo di servizi di TIC non devono necessariamente essere prestati dalla sua entità nell'Unione.***

(58 bis) Visto l'impatto significativo che la designazione come funzione critica può avere sui fornitori terzi di servizi di TIC, i diritti di audizione preventiva dovrebbero configurarsi come obbligo a carico delle AEV e dell'organismo congiunto di sorveglianza di prendere debitamente in considerazione qualsiasi informazione aggiuntiva trasmessa dai fornitori terzi di servizi di TIC nel corso del processo di designazione.

(59) ***Il*** quadro ***di sorveglianza*** 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, ***tramite l'organismo congiunto di sorveglianza di nuova istituzione che adotta*** singole decisioni rivolte a fornitori terzi di servizi di TIC critici ***e*** 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 istituire l'organismo congiunto di sorveglianza per assicurare la sorveglianza diretta dei fornitori terzi di servizi di TIC***. ***Inoltre,*** è opportuno designare una delle AEV come autorità di sorveglianza capofila per ciascun fornitore terzo di servizi di TIC critico ***affinché effettui e coordini le attività quotidiane di sorveglianza e di indagine, funga da punto di contatto unico e assicuri la continuità. L'organismo congiunto di sorveglianza e l'autorità di sorveglianza capofila dovrebbero operare senza soluzione di continuità per garantire una sorveglianza quotidiana efficace nonché un approccio olistico al processo decisionale e alle raccomandazioni.***

(62) Le autorità di sorveglianza capofila dovrebbero detenere i poteri necessari per condurre indagini e ispezioni in loco ▌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.

(62 bis) Affidare all'***organismo congiunto di sorveglianza*** la sorveglianza ***diretta*** 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) ***L'organismo congiunto di sorveglianza dovrebbe*** essere inoltre in grado di ***emettere*** 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 ***dall'organismo congiunto di sorveglianza***. ***Prima di finalizzare tali raccomandazioni, i fornitori terzi di servizi di TIC critici dovrebbero avere l'opportunità di trasmettere le informazioni che ritengano ragionevolmente meritevoli di considerazione, prima che la raccomandazione sia***

finalizzata ed emessa.

(63 bis) Per evitare duplicazioni e incongruenze con le misure tecniche e organizzative applicabili ai fornitori terzi di servizi di TIC critici, nell'esercizio dei loro poteri in conformità del quadro di sorveglianza di cui al presente regolamento le autorità di sorveglianza capofila e l'organismo congiunto di sorveglianza dovrebbero tenere debitamente conto del quadro stabilito dalla direttiva (UE) 2016/1148. Prima di esercitare tali poteri, l'organismo congiunto di sorveglianza e l'autorità di sorveglianza capofila dovrebbero consultare le autorità giuridicamente competenti ai sensi della direttiva (UE) 2016/1148.

(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***, nel condurre indagini generali o ispezioni in loco,*** 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[16], nonché consultazioni con le AEV tramite il reciproco scambio di informazioni e l'offerta di assistenza nel contesto delle attività di vigilanza. ***Il Comitato di risoluzione unico, sebbene non sia un'autorità competente ai fini del presente regolamento, dovrebbe***

[16] 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).

essere comunque coinvolto nei meccanismi di scambio reciproco di informazioni per le entità che rientrano nell'ambito di applicazione del regolamento (UE) n. 806/2014 del Parlamento europeo e del Consiglio[17].

(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 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, nel rispetto dei principi stabiliti nell'accordo interistituzionale "Legiferare meglio" del 13 aprile 2016[18]. In particolare, al fine di garantire la parità di partecipazione 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[19], 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.

Gli orientamenti pertinenti emanati o in corso di elaborazione da parte delle AEV sull'applicazione di tali regolamenti e direttive dovrebbero essere riesaminati e rivisti nel quadro del processo di consolidamento, in modo che la base giuridica delle prescrizioni in materia di rischi relativi alle TIC nel diritto dell'Unione sia rappresentata esclusivamente dal presente regolamento, dai suoi atti di esecuzione e dalle decisioni e raccomandazioni adottate conformemente allo stesso, relativamente alle entità che rientrano nel suo ambito di applicazione.

(69 bis) Le norme tecniche dovrebbero garantire la coerente armonizzazione delle

---

17 ***Regolamento (UE) n. 806/2014 del Parlamento europeo e del Consiglio, del 15 luglio 2014, che fissa norme e una procedura uniformi per la risoluzione degli enti creditizi e di talune imprese di investimento nel quadro del meccanismo di risoluzione unico e del Fondo di risoluzione unico e che modifica il regolamento (UE) n. 1093/2010 (GU L 225 del 30.7.2014, pag. 1).***

18 GU L 123 del 12.5.2016, pag. 1.

19 [*Inserire il riferimento completo*]

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. ***In sede di elaborazione di progetti di norme tecniche di regolamentazione, le AEV dovrebbero tenere debitamente conto del loro mandato in relazione agli aspetti di proporzionalità e ottenere il parere dei rispettivi comitati consultivi sulla proporzionalità, in particolare riguardo all'applicazione del presente regolamento alle PMI e alle imprese a media capitalizzazione.***

(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 parte delle entità finanziarie nonché modelli standardizzati per il registro delle informazioni. Nell'elaborazione di tali norme le AEV dovrebbero tener conto ***della natura,*** delle dimensioni***,*** della complessità ***e del profilo commerciale*** 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;

– ***segnalazione alle autorità competenti, da parte delle entità finanziarie di cui all'articolo 2, paragrafo 1, lettere da a) a c), di gravi incidenti operativi o connessi alla sicurezza dei pagamenti;***

– test di resilienza operativa digitale;

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

– misure relative ***alla*** solida gestione ▌ dei rischi relativi alle TIC derivanti da terzi ***da parte delle entità finanziarie***;

(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.

2 bis. Il presente regolamento lascia impregiudicate le competenze degli Stati membri per quanto riguarda il mantenimento della sicurezza pubblica, della difesa e della sicurezza nazionale.

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 ***e offerenti*** di cripto-attività, emittenti ***e offerenti*** di token collegati ad attività ed emittenti di token collegati ad attività significativi;

(f) depositari centrali di titoli ***e operatori di sistemi di regolamento 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 ***che non siano microimprese, piccole o medie imprese, a meno che tali microimprese, piccole o medie imprese non si affidino esclusivamente a sistemi organizzati di vendita automatizzata;***

(o) enti pensionistici aziendali o professionali ***(EPAP) che non gestiscano regimi pensionistici che contano congiuntamente meno di 15 affiliati;***

(p) agenzie di rating del credito;

(q) revisori legali e imprese di revisione ***che non siano microimprese, piccole o medie imprese, a meno che tali microimprese, piccole o medie imprese non forniscano servizi di revisione contabile alle entità elencate nel presente articolo, ad eccezione delle microimprese, piccole o medie imprese che sono enti senza scopo di lucro che effettuano revisioni a norma dell'articolo 2, paragrafo 3, del regolamento (UE) n. 537/2014, a meno che l'autorità competente non decida che l'eccezione non è valida***;

(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.

1 bis. Il presente regolamento, ad eccezione del capo V, sezione II, si applica anche ai fornitori intragruppo 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".

2 bis. Ai fini del presente regolamento, ad eccezione del capo V, sezione II, i fornitori terzi di servizi di TIC e i fornitori intragruppo di servizi di TIC sono collettivamente denominati "fornitori terzi di servizi di TIC".

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 ▌ garantendo, direttamente o indirettamente, tramite il ricorso ai servizi offerti da fornitori terzi di TIC, ▌ la costante offerta dei servizi finanziari e la loro qualità ***in caso di perturbazioni operative che incidono sulle capacità in materia di TIC dell'entità;***

(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 ▌ che, qualora si concretizzi, potrebbe compromettere la sicurezza della rete e dei sistemi informativi, di eventuali strumenti o processi dipendenti dalle ***TIC***, della continuazione delle operazioni e dei processi, oppure della fornitura dei servizi ▌ ;

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

(6) "incidente connesso alle TIC": un ***incidente*** imprevisto identificato***, o una serie di incidenti collegati,*** che compromette la sicurezza della rete e dei sistemi informativi ▌ o che ha effetti avversi sulla disponibilità, la riservatezza, la continuità***, l'integrità*** o l'autenticità dei servizi finanziari forniti dall'entità finanziaria;

(6 bis) "incidente operativo o connesso alla sicurezza dei pagamenti": un evento o una serie di eventi collegati non previsti dalle entità finanziarie di cui all'articolo 2, paragrafo 1, lettere da a) a c), che ha o avrà verosimilmente un impatto negativo sull'integrità, la disponibilità, la riservatezza, l'autenticità o la continuità dei servizi connessi ai pagamenti;

(7) "incidente grave connesso alle TIC": un incidente connesso alle TIC ***che ha o avrà verosimilmente*** un impatto avverso ▌ elevato sulla rete e sui sistemi informativi che sostengono funzioni critiche dell'entità finanziaria;

(7 bis) "grave incidente operativo o connesso alla sicurezza dei pagamenti": incidente operativo o connesso alla sicurezza dei pagamenti rispondente ai criteri di cui all'articolo 16;

(8) "minaccia informatica": minaccia informatica quale definita all'articolo 2, punto 8, del regolamento (UE) 2019/881 del Parlamento europeo e del Consiglio[20];

(8 bis) "minaccia informatica significativa": una minaccia informatica le cui caratteristiche ne indicano chiaramente la probabilità di dar luogo a un grave incidente connesso

[20] 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).

alle TIC;

(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": un punto debole, una suscettibilità o un difetto di una risorsa, di un sistema, di un processo o di un controllo, di cui una minaccia ***informatica*** 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 ***di TIC***, ***comprese le entità finanziarie che forniscono servizi di TIC e che fanno parte di un'impresa fornitrice di un'ampia gamma di prodotti o servizi,*** 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[21];

(15 bis) "fornitore intragruppo di servizi di TIC": un'impresa che fa parte di un gruppo finanziario e fornisce servizi di TIC esclusivamente a entità finanziarie dello stesso gruppo o a entità finanziarie appartenenti allo stesso sistema di tutela istituzionale, comprese le loro società madri, controllate e succursali o altre entità di proprietà comune o sotto controllo comune;

(16) "servizi di TIC": servizi digitali e di dati forniti attraverso sistemi di TIC a uno o più utenti interni o esterni ***su base continuativa, esclusi i contratti di telecomunicazione;***

(17) "funzione critica o importante": ***un'attività o un servizio essenziale per il funzionamento di un'entità finanziaria la cui perturbazione pregiudicherebbe significativamente la solidità o la continuità dei servizi e delle attività dell'entità finanziaria,*** o 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, ***comprese le "funzioni essenziali"***

---

[21] 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).

quali definite all'articolo 2, paragrafo 1, punto 35, della direttiva 2014/59/UE;

(18) "fornitore terzo di servizi di TIC critico": un fornitore terzo di servizi di TIC designato in conformità dell'articolo ***28*** e soggetto al quadro di sorveglianza di cui agli articoli da ***29*** 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 ▌ 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 ▌ 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 stabilità finanziaria dell'intera Unione o*** la capacità di un'entità finanziaria ▌ di assolvere funzioni critiche ***o importanti*** 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[22], all'articolo 3, paragrafo 1, ***punto 18***, del regolamento (UE) 20xx/xx del Parlamento europeo e del Consiglio[23] [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[24];

(23 bis) "ente creditizio esentato dalla direttiva 2013/36/UE": un ente che beneficia di un'esenzione ai sensi dell'articolo 2, paragrafo 5, punti da 4 a 23, della direttiva 2013/36/UE;

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

(24 bis) "impresa di investimento piccola e non interconnessa": un'impresa di investimento che soddisfa le condizioni di cui all'articolo 12, paragrafo 1, del regolamento (UE) 2019/2033;

(25) "istituto di pagamento": un istituto di pagamento quale definito all'articolo 1, paragrafo

---

22 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).

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

24 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).

1, lettera (d), della direttiva (UE) 2015/2366;

(25 bis) "istituto di pagamento esentato dalla direttiva (UE) 2015/2366": un istituto di pagamento che beneficia di un'esenzione ai sensi dell'articolo 32, paragrafo 1, 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[25];

(26 bis) "istituto di moneta elettronica esentato dalla direttiva 2009/110/CE": un istituto di moneta elettronica; che beneficia di un'esenzione ai sensi dell'articolo 9 della direttiva 2009/110/CE;

(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***, paragrafo 1,*** punto 3, della direttiva (UE) 2016/97;

(37) "intermediario assicurativo a titolo accessorio": un intermediario assicurativo a titolo accessorio quale definito all'articolo 2, ***paragrafo 1,*** punto 4, della direttiva (UE) 2016/97;

(38) "intermediario riassicurativo": un intermediario riassicurativo quale definito all'articolo 2, ***paragrafo 1,*** punto 5, della direttiva (UE) 2016/97;

(39) "ente pensionistico aziendale e professionale": un ente pensionistico aziendale o

---

[25] 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).

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, ***punto 8***, del regolamento (UE) 202x/xx [PO: inserire il riferimento al regolamento MICA];

(44) "emittente di cripto-attività": un emittente di cripto-attività quale definito all'articolo 3, paragrafo 1, ***punto 6***, del [GU: inserire il riferimento al regolamento MICA];

(44 bis) "offerente": un offerente quale definito all'articolo 3, paragrafo 1, punto [(XX)], del [GU: inserire il riferimento al regolamento MICA];

(44 ter) "offerente di cripto-attività": un offerente di cripto-attività quale definito all'articolo 3, paragrafo 1, punto [(XX)], 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];

(45 bis) "offerente di token collegati ad attività": un offerente di token collegati ad attività quale definito all'articolo 3, paragrafo 1, punto [(XX)], 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, ***punto (XX)***, 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 ***3***, punto ***25***, del regolamento ***(UE) 2016/1011*** [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 ***2***, paragrafo ***1***, ***lettera e)***, del regolamento (UE) ***2020/1503*** [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***, piccola e media impresa***": un'entità finanziaria quale definita all'articolo 2 dell'allegato della raccomandazione 2003/361/CE.

(50 bis) "autorità di risoluzione": autorità designata da uno Stato membro a norma dell'articolo 3 della direttiva 2014/59/UE o il Comitato di risoluzione unico istituito a norma dell'articolo 42 del regolamento n. 806/2014.

Articolo 3 bis

Principio di proporzionalità

1. *Le entità finanziarie attuano le norme introdotte dai capi II, III e IV conformemente al principio di proporzionalità, tenendo conto delle loro dimensioni, della natura, portata e complessità dei loro servizi, delle loro attività e delle loro operazioni, nonché del loro profilo di rischio complessivo.*

2. *In virtù del principio di proporzionalità, gli articoli da 4 a 14 del presente regolamento non si applicano:*

   (a) alle piccole imprese di investimento non interconnesse o agli istituti di pagamento esentati dalla direttiva (UE) 2015/2366;

   (b) agli enti creditizi esentati dalla direttiva 2013/36/UE;

   (c) agli istituti di moneta elettronica esentati dalla direttiva 2009/110/CE; o

   (d) ai piccoli enti pensionistici aziendali o professionali;

3. *Sulla base della relazione annuale sul riesame del quadro per la gestione dei rischi relativi alle TIC, di cui all'articolo 5, paragrafo 6, e all'articolo 14 bis, paragrafo 2, le autorità competenti esaminano e valutano l'applicazione della proporzionalità da parte di un'entità finanziaria e stabiliscono se il quadro per la gestione dei rischi relativi alle TIC dell'entità finanziaria garantisca una sana gestione, la resilienza operativa digitale e la copertura del rischio relativo alle ICT. A tal fine, le autorità competenti tengono conto delle dimensioni dell'entità finanziaria, della natura, della portata e della complessità dei suoi servizi, delle sue attività e delle sue operazioni, nonché del suo profilo di rischio globale.*

4. *Qualora ritenga che il quadro per la gestione dei rischi relativi alle TIC dell'entità finanziaria sia insufficiente e sproporzionato, l'autorità competente avvia un dialogo con l'entità finanziaria per porre rimedio alle carenze e garantire la piena conformità al capo II.*

5. *Le AEV elaborano progetti di norme tecniche di regolamentazione per quanto riguarda:*

   (a) la determinazione della misura in cui le prescrizioni in materia di gestione dei rischi relativi alle TIC sono applicabili a ciascuna delle entità finanziarie di cui al paragrafo 1;

   (b) l'ulteriore specificazione del contenuto e del formato della relazione annuale sul riesame del quadro per la gestione dei rischi relativi alle TIC di cui al paragrafo 3;

   (c) l'ulteriore specificazione delle norme e delle procedure che le autorità competenti e le entità finanziarie devono seguire nell'ambito del dialogo di cui al paragrafo 4.

6. *Le AEV trasmettono alla Commissione i progetti di norme tecniche di regolamentazione di cui al paragrafo 5 entro il [GU: inserire la data corrispondente a 1 anno dopo la data di entrata in vigore].*

   Alla Commissione è delegato il potere di adottare le norme tecniche di regolamentazione di cui al paragrafo 5 del presente articolo in conformità,

rispettivamente, degli articoli da 10 a 14 dei regolamenti (UE) n. 1093/2010, (UE) n. 1094/2010 e (UE) n. 1095/2010.

CAPO II

GESTIONE DEI RISCHI RELATIVI ALLE TIC

SEZIONE I

Articolo 4

Governance e organizzazione

1. Le entità finanziarie predispongono ***un quadro*** di gestione e di controllo interni che ***garantisca*** una gestione efficace e prudente di tutti i rischi relativi alle TIC***, al fine di pervenire a un elevato livello di resilienza operativa digitale***.

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 ***in ultima istanza*** per la gestione dei rischi relativi alle TIC dell'entità finanziaria;

   (a bis) predispone politiche e procedure miranti a garantire il mantenimento di standard elevati di sicurezza, riservatezza e integrità dei dati;

   (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***, che possono essere adottati come una politica specifica distinta e come parte integrante della più ampia politica di continuità operativa e del più ampio piano di ripristino in caso di disastro,*** 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 ***pertinente*** formazione sui rischi relativi alle TIC e sulle relative competenze per tutto il personale ▌;

   (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 ***regolarmente*** informato in merito ***ad almeno gli*** incidenti ***gravi*** 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 ***in seno all'entità finanziaria per*** l'uso di ▌servizi ***di TIC, in particolare quelli conclusi con i fornitori terzi di servizi di TIC***, 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 ***dell'entità finanziaria mantengono*** aggiornate conoscenze e competenze adeguate per comprendere e valutare i rischi relativi alle TIC e il loro impatto sulle operazioni dell'entità finanziaria***, anche seguendo una formazione specifica su base regolare, commisurata ai rischi relativi alle TIC gestiti.***

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 ▌.

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 ***e sul proprio quadro per la gestione dei 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***, ove già disponibili e del caso, compresi gli orientamenti stabiliti nelle pertinenti linee guida definite dalle AEV,*** e lo riesaminano

periodicamente.

5. Le entità finanziarie diverse dalle microimprese ***attribuiscono la responsabilità della gestione e della sorveglianza dei rischi relativi alle TIC a una funzione di controllo, di cui assicurano l'indipendenza per evitare conflitti di interesse.*** Le entità finanziarie ▌garantiscono un'opportuna ***indipendenza*** 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.

Ogni anno è presentata all'autorità competente una relazione sul riesame del quadro per la gestione dei rischi relativi alle TIC.

7. ***Per quanto riguarda le entità finanziarie diverse dalle microimprese,*** 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 ▌delle conclusioni dell'audit ▌.

9. Il quadro per la gestione dei rischi relativi alle TIC di cui al paragrafo 1 comprende una strategia di resilienza ***operativa*** 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 ▌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) ***individuando*** le principali dipendenze da fornitori terzi di servizi di TIC ***e illustrando le strategie di uscita in relazione a tali dipendenze;***

(h) attuando test di resilienza operativa digitale***, conformemente al capo IV del presente regolamento***;

(i) delineando una strategia di comunicazione in caso di incidenti connessi alle TIC ***che vanno divulgati ai sensi dell'articolo 13***.

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

Previa comunicazione alle autorità competenti, le entità finanziarie possono delegare a imprese intragruppo i compiti di verifica della conformità alle prescrizioni in materia di gestione dei rischi relativi alle TIC.

Laddove venga concessa la delega di cui al secondo comma, l'entità finanziaria rimane pienamente responsabile della verifica della conformità alle prescrizioni in materia di gestione dei rischi relativi alle TIC.

Articolo 6

Sistemi, protocolli e strumenti di TIC

1. ***Per affrontare e gestire i rischi relativi alle TIC*** 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 ▌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 ***critiche o importanti*** 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, ***la criticità o l'importanza delle funzioni commerciali connesse alle TIC, nonché*** 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 ***critiche o importanti*** 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. ***Se del caso,*** 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 ***critici o importanti*** a livello di TIC ***tenuto conto delle loro finalità***, nonché dei collegamenti e delle interdipendenze tra i diversi beni a livello di TIC.

5. Le entità finanziarie identificano e documentano tutti i processi ***critici o importanti*** dipendenti da fornitori terzi di servizi di TIC e identificano le interconnessioni con detti fornitori ***che supportano funzioni critiche o importanti***.

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, ***compresi i sistemi che sono ancora in uso e svolgono le loro funzioni ma:***

   (a) sono vecchi o a fine vita, nel caso dell'hardware;

   (b) non sono più in grado di ricevere assistenza o manutenzione dal loro fornitore; o

   (c) è impossibile o antieconomico procedere a un loro aggiornamento. I sistemi di TIC esistenti sono oggetto di una valutazione annuale dei rischi legati alle TIC, soprattutto prima e dopo la connessione fra tecnologie, applicazioni o sistemi ▌.

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***, a sostenere funzioni critiche o importanti***, 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 ▌che:

   (a) ***massimizzano*** 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 ***i rischi interni relativi alle TIC, compresi*** la cattiva amministrazione***, i*** rischi relativi al trattamento dei dati ***e l'errore umano***.

4. All'interno del quadro per la gestione dei rischi relativi alle TIC di cui all'articolo 5, paragrafo 1, ***e secondo il proprio profilo di rischio,*** 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 ***delle proprie risorse, dati e patrimoni di informazioni a livello di TIC e assicura al tempo stesso la piena protezione di*** risorse, dati e patrimoni di informazioni a livello di TIC dei propri clienti ***quando questi fanno parte dei sistemi di TIC propri dell'entità finanziaria***;

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

   (c) attuano politiche***, procedure e controlli*** 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 ▌;

   (d) attuano politiche e protocolli riguardanti robusti meccanismi di autenticazione ***e la protezione di chiavi crittografiche,*** basati su norme pertinenti e sistemi di controllo dedicati ▌;

   (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 ***il più rapidamente possibile*** 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***, laddove sia tecnologicamente possibile,*** per individuare ***e monitorare*** 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 ***avviano*** processi di individuazione degli incidenti connessi alle TIC e di risposta agli stessi***, fra cui*** meccanismi di allarme automatico per il personale incaricato della risposta agli incidenti connessi alle TIC.

3. Le entità finanziarie dedicano risorse e capacità sufficienti ▌al monitoraggio dell'attività degli utenti e al verificarsi di anomalie e incidenti connessi alle TIC, in particolare attacchi informatici.

3 bis. Le entità finanziarie registrano tutti gli incidenti connessi alle TIC che hanno un impatto sulla stabilità, la continuità o la qualità dei servizi finanziari, compresi i casi in cui l'incidente ha avuto o può avere un impatto su questi servizi.

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 ▌esaustiva***, che può essere adottata come una politica specifica distinta e*** come parte integrante della ***più ampia*** politica di continuità operativa ***dell'entità***.

La politica di continuità operativa delle TIC mira a gestire e attenuare i rischi che potrebbero avere un impatto avverso sui sistemi e servizi TIC delle entità finanziarie e ad agevolarne la rapida ripresa, se necessario. Nel redigere la politica di continuità operativa delle TIC, le entità finanziarie considerano specificamente i rischi che potrebbero avere un impatto avverso sui servizi e sistemi di TIC.

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:

   (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 ***critici o importanti***;

   (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 potrà essere una funzione dedicata o far parte integrante delle funzioni adibite alla risposta e gestione degli incidenti. La funzione di gestione delle crisi fissa***, in caso di attivazione della politica di continuità operativa delle TIC o del piano di ripristino in caso di disastro relativo alle TIC, ▌procedure chiare per la gestione della comunicazione interna ed esterna delle crisi, in conformità dell'articolo 13.

7. Le entità finanziarie registrano le attività ***pertinenti*** 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 ***le stime di*** tutti i costi e le perdite ***sul piano finanziario*** causati dalle perturbazioni ***significative*** a livello di TIC e agli incidenti ***gravi*** connessi alle TIC.

9 bis. Le AEV, tramite il comitato congiunto, elaborano orientamenti comuni sulla metodologia di calcolo dei costi e di quantificazione delle perdite di cui al paragrafo 9.

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. ***In linea con la politica di backup di cui al paragrafo 1, lettera a),*** 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 ***fisicamente o logicamente segregati dal sistema di TIC principale, che sono protetti*** 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 ***valutano la necessità di mantenere*** capacità di TIC ridondanti, dotate di risorse e funzionalità sufficienti e idonee a soddisfare le esigenze commerciali ***e a rispettare i requisiti di resilienza operativa digitale stabiliti nel presente regolamento***.

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) ▌accessibile al personale dell'entità finanziaria per garantire la continuità ***delle funzioni critiche o importanti*** 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 fatto che si tratti di una funzione critica o importante e 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 ***assicurano il più elevato livello di integrità dei dati, ad esempio effettuando*** molteplici verifiche, compresi i controlli incrociati. ***Tali*** 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 ▌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 ***a un grave*** 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 ***volte a rispondere ai rischi relativi alle TIC identificati in sede di riesame successivo a un grave incidente connesso alle TIC,*** le

entità finanziarie diverse dalle microimprese comunicano tali modifiche alle autorità competenti ***specificando i miglioramenti che è necessario apportare e le modalità con cui mirano a prevenire o a mitigare le perturbazioni future***. ***La notifica delle modifiche alle autorità competenti può avvenire prima o dopo la loro attuazione***.

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***, compresa la prossimità di tali rischi a funzioni critiche o importanti,*** 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. ***I programmi di sensibilizzazione sulla sicurezza delle TIC si applicano a tutto il personale. Le attività di formazione sulla resilienza operativa si applicano ad almeno*** tutti i dipendenti ***con diritti di accesso diretto ai sistemi di TIC*** e ***agli*** alti dirigenti. ***La complessità dei moduli di formazione è commisurata al livello di accesso diretto ai sistemi di TIC del membro del personale e, in particolare, tiene conto del suo accesso a funzioni essenziali o importanti.***

Le entità finanziarie ***diverse dalle microimprese*** 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 ***almeno sugli*** incidenti ***gravi*** connessi alle TIC o sulle vulnerabilità più rilevanti ai clienti e alle controparti nonché al pubblico, a seconda dei casi.

   I piani di comunicazione di cui al primo comma garantiscono inoltre la divulgazione ai clienti e alle controparti, su base annuale, di una sintesi di tutti gli incidenti connessi alle TIC. Tale divulgazione rispetta pienamente la riservatezza commerciale dell'entità finanziaria e dei suoi clienti e controparti e non compromette il quadro per la gestione dei rischi relativi alle TIC di cui all'articolo 5, paragrafo 1.

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 ***almeno i gravi*** 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 ***e indebiti ritardi***;

(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.

Articolo 14 bis

Quadro di gestione dei rischi relativi alle TIC per le entità di piccole dimensioni, non interconnesse ed esenti

1. A norma dell'articolo 3 bis, le piccole imprese di investimento non interconnesse, gli istituti di pagamento esentati dalla direttiva (UE) 2015/2366, gli enti creditizi esentati dalla direttiva 2013/36/UE, gli istituti di moneta elettronica esentati dalla direttiva 2009/110/CE e i piccoli enti pensionistici aziendali o professionali pongono in essere e mantengono un solido e documentato quadro per la gestione dei rischi relativi alle TIC che:

(a) precisi i meccanismi e le misure finalizzate a una gestione rapida, efficiente e organica di tutti i rischi relativi alle TIC, anche ai fini della protezione delle relative componenti fisiche e infrastrutture;

(b) monitori costantemente la sicurezza e il funzionamento di tutti i sistemi di TIC;

(c) riduca al minimo l'impatto dei rischi relativi alle TIC attraverso l'uso di sistemi, protocolli e strumenti TIC solidi, resilienti e aggiornati e atti a supportare lo svolgimento delle loro attività e la fornitura di servizi;

(d) tuteli adeguatamente la riservatezza, l'integrità e la disponibilità della rete di dati e dei sistemi informativi;

(e) provveda a che le fonti di rischio e le anomalie di rete e dei sistemi

informativi siano prontamente identificate e rilevate e che gli incidenti connessi alle TIC siano gestiti con rapidità.

2. 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.

Ogni anno è presentata all'autorità competente una relazione sul riesame del quadro per la gestione dei rischi relativi alle TIC.

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 ***procedure e*** 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 affrontare*** le cause di fondo ***al fine di*** 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 ***almeno*** degli incidenti gravi connessi alle TIC agli alti dirigenti interessati e informa l'organo di gestione in merito a detti ***gravi*** 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 ▌;

(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. ***In coordinamento con*** la Banca centrale europea (BCE) e ***l'***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 ***gravi*** 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 tengono inoltre conto del fatto che la gestione tempestiva ed efficiente di un incidente da parte delle piccole e microimprese non deve subire restrizioni legate alla necessità di rispettare i criteri di classificazione di cui al presente articolo. Le AEV tengono anche conto delle dimensioni delle entità finanziarie, della natura, della portata e della complessità dei loro servizi, attività e operazioni, nonché del loro profilo di rischio globale.***

Le AEV presentano detti progetti di norme tecniche di regolamentazione comuni alla Commissione entro il [PO: inserire la data corrispondente a ***due anni*** 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.

1 bis. Le entità finanziarie possono, su base volontaria, notificare le minacce informatiche significative all'autorità competente pertinente qualora ritengano che la minaccia sia rilevante per il sistema finanziario, gli utenti dei servizi o i clienti. L'autorità competente interessata può fornire tali informazioni ad altre autorità pertinenti conformemente al paragrafo 5.

2. Qualora ***si verifichi*** un incidente grave connesso alle TIC ***avente*** un impatto ***rilevante*** sugli interessi finanziari dei clienti e degli utenti del servizio, le entità finanziarie informano, senza indebito ritardo ***dopo esserne venute a conoscenza***, clienti e utenti del servizio in merito a tale incidente e comunicano loro ▌le ***pertinenti*** misure che sono state adottate per attenuare gli effetti avversi dell'incidente. ***L'obbligo di informare gli utenti e i clienti del servizio non si applica se le contromisure adottate dall'entità finanziaria evitano danni agli utenti e ai clienti del servizio.***

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

   (a) una notifica iniziale ▌***dell'***incidente grave connesso alle TIC***, che deve contenere le informazioni di cui dispone il soggetto che effettua la notifica con la massima diligenza, nel modo seguente:***

      i) per quanto riguarda gli incidenti che perturbano in modo significativo la disponibilità dei servizi forniti dall'entità finanziaria, l'autorità competente è informata senza indebito ritardo e in ogni caso entro 24 ore dal momento in cui è stata presa conoscenza dell'incidente;

      ii) per quanto riguarda gli incidenti che hanno un impatto significativo sull'entità finanziaria, ma non sulla disponibilità dei servizi da essa forniti, l'autorità competente è informata senza indebito ritardo e in ogni caso entro 72 ore dal momento in cui è stata presa conoscenza dell'incidente;

   iii) per quanto riguarda gli incidenti che perturbano l'integrità, la riservatezza o la sicurezza dei dati personali conservati dall'entità finanziaria, l'autorità competente è informata senza indebito ritardo e in ogni caso entro 24 ore dal momento in cui è stata presa conoscenza dell'incidente;

   (b) una relazione intermedia***, non appena lo stato originario dell'incidente sia notevolmente cambiato o dopo che siano venute alla luce nuove informazioni suscettibili di influire notevolmente sul modo di affrontare l'incidente da parte dell'autorità competente, dopo*** la 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 ***dalla data di*** invio della segnalazione iniziale.

(c bis) in caso di incidente ancora in corso al momento della presentazione della relazione definitiva di cui alla lettera c), una relazione finale è presentata un mese dopo la risoluzione dell'incidente.

L'autorità competente di cui all'articolo 41 dispone che, in casi debitamente giustificati, un'entità finanziaria sia autorizzata a discostarsi dai termini di cui alle lettere a), b), c) e c bis) del presente paragrafo, tenendo debitamente conto della capacità delle entità finanziarie di fornire informazioni accurate e significative in relazione a incidenti gravi connessi alle TIC.

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. ***In caso di delega, l'entità finanziaria rimane pienamente responsabile dell'adempimento degli obblighi di segnalazione dell'incidente.***

5. Dopo aver ricevuto la segnalazione di cui al paragrafo 1, l'autorità competente trasmette senza indebito ritardo i dettagli ***del grave*** incidente ***connesso alle TIC***:

(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 ***o al CSIRT designato ai sensi dell'articolo 9 della direttiva (UE) 2016/1149;***

(c bis) all'autorità di risoluzione responsabile dell'entità finanziaria pertinente; al comitato di risoluzione unico (SRB) per le entità di cui all'articolo 7, paragrafo 2, del regolamento (UE) n. 806/2014 e per le entità e i gruppi di cui all'articolo 7, paragrafo 4, lettera b), e paragrafo 5, del regolamento (UE) n. 806/2014, qualora siano soddisfatte le condizioni per l'applicazione di tali paragrafi;

(c ter) alle autorità nazionali di risoluzione per le entità e i gruppi di cui all'articolo 7, paragrafo 3, del regolamento (UE) n. 806/2014. Le autorità nazionali di risoluzione forniscono all'SRB, su base trimestrale, una sintesi delle relazioni ricevute a norma della presente lettera in relazione alle entità e ai gruppi di cui all'articolo 7, paragrafo 3, del regolamento (UE) n. 806/2014;

(c quater) ad altre autorità pubbliche pertinenti, comprese quelle di altri Stati membri.

6. L'ABE, l'ESMA o l'EIOPA e la BCE***, in cooperazione con l'ENISA,*** 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;

(3) specificare ulteriormente i criteri per determinare l'impatto di un incidente grave connesso alle TIC su un'entità finanziaria ai fini dell'articolo 17, paragrafo 3, lettera a).

(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 primo paragrafo, lettera a), e i progetti di norme tecniche di attuazione comuni di cui al primo paragrafo, lettera b), entro il xx 202x [PO: inserire la data corrispondente ***a due anni*** 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 primo paragrafo, 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 primo paragrafo, lettera b), in conformità, rispettivamente, dell'articolo 15 dei regolamenti (UE) n. 1093/2010, (UE) n. 1095/2010 e (UE) n. 1094/2010.

2. In attesa dell'esito della relazione di fattibilità di cui all'articolo 19 sull'ulteriore centralizzazione delle segnalazioni degli incidenti, le AEV, tramite il comitato congiunto e in collaborazione con le autorità competenti, la BCE, l'SRB e l'ENISA, elaborano orientamenti per lo scambio di informazioni sulle segnalazioni di incidenti gravi connessi alle TIC a norma dell'articolo 17, paragrafo 5.

Gli orientamenti di cui al primo comma prendono in considerazione almeno i seguenti elementi:

(a) i canali di comunicazione più efficienti;

(b) la tutela della sicurezza, della riservatezza e dell'integrità dei dati scambiati;

(c) l'eventuale coinvolgimento di entità finanziarie per integrare lo scambio di informazioni di cui all'articolo 40.

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 ***di un*** polo ***unico*** UE ;

   (b) benefici, limiti e possibili rischi;

   (b bis) la possibilità di stabilire l'interoperabilità valutandone il valore aggiunto rispetto ad altri pertinenti sistemi di segnalazione, quali previsti dalla direttiva (UE) 2016/1148;

   (c) elementi della gestione operativa;

   (d) condizioni di adesione;

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

   (f) una valutazione preliminare dei costi finanziari derivanti dall'istituzione della piattaforma operativa su cui dovrà fondarsi il polo ***unico*** 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, paragrafi 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 ***nonché di fornire feedback, approfondimenti e informazioni adeguatamente anonimizzate a tutte le entità finanziarie che potrebbero avvalersene, sulla scorta di eventuali segnalazioni di incidenti gravi connessi alle TIC pervenute***.

2. Le AEV, tramite il comitato congiunto, riferiscono con frequenza annuale, sulla base di dati anonimizzati e aggregati, in merito alle notifiche di incidenti ***gravi*** 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 ***stimati*** 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.

Articolo 20 bis

Incidenti operativi o relativi alla sicurezza dei pagamenti riguardanti determinate entità finanziarie

Le prescrizioni contenute nel presente capo si applicano anche agli incidenti operativi o relativi alla sicurezza dei pagamenti e ai gravi incidenti operativi o relativi alla sicurezza dei pagamenti, quando riguardano le entità finanziarie di cui all'articolo 2, paragrafo 1, lettere a), b) e c).

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 ***diverse dalle microimprese*** stabiliscono, mantengono e riesaminano ▌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. ***Se i test sono svolti da un tester interno, le entità finanziarie dedicano risorse sufficienti e garantiscono che siano evitati conflitti di interesse durante le fasi di progettazione ed esecuzione del test.***

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 ***affrontarli***; 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 ***provvedono a eseguire opportuni test su*** 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 questi figurano 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 ***3, secondo comma,*** 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 ***o importanti*** dell'entità finanziaria e sono effettuati sui reali sistemi di produzione che sostengono tali funzioni***, ove possibile, o sui sistemi di pre-produzione con la stessa configurazione di sicurezza***. Il preciso ambito di applicazione dei test di penetrazione basati su minacce, fondato sulla valutazione di funzioni e servizi critici ***o importanti***, è determinato dalle entità finanziarie ed è convalidato dalle autorità competenti. ***Un singolo test di penetrazione basato su minacce non riguarda obbligatoriamente tutte le funzioni critiche o importanti.***

   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 ***o importanti***, comprese le funzioni e i servizi ***critici o importanti*** esternalizzati o appaltati a fornitori terzi di servizi di TIC.

   Qualora i fornitori terzi di servizi di TIC ***critici e, se del caso, i fornitori terzi di servizi di TIC non critici*** rientrino nell'ambito dei test di penetrazione basati su minacce, l'entità finanziaria adotta le misure necessarie per garantire la partecipazione di tali fornitori ***Tali fornitori terzi di servizi di TIC non sono tenuti a comunicare informazioni o a fornire particolari in relazione a elementi non rilevanti ai fini dei controlli di gestione del rischio delle pertinenti funzioni critiche o importanti delle entità finanziarie interessate. Tali test non si ripercuotono negativamente su altri clienti dei fornitori terzi di servizi di TIC.***

   Qualora il coinvolgimento di un fornitore terzo di servizi di TIC nei test di penetrazione basati su minacce sia potenzialmente in grado di influire sulla qualità, sulla riservatezza o sulla sicurezza dei servizi di TIC prestati dal fornitore terzo ad altri clienti che non rientrano nell'ambito di applicazione del presente regolamento, o sull'integrità generale delle operazioni del fornitore terzo di servizi di TIC, l'entità finanziaria e il fornitore terzo di servizi di TIC possono concordare contrattualmente che il fornitore terzo di servizi di TIC sia autorizzato a stipulare accordi contrattuali direttamente con un tester esterno. I fornitori terzi di servizi di TIC possono stipulare tali accordi per conto di tutte le entità finanziarie che ricorrono ai loro servizi al fine di condurre test congiunti.

   Le entità finanziarie applicano efficaci controlli di gestione del rischio per ***mitigare*** i rischi di potenziali impatti sui dati, danni alle attività e perturbazioni delle ***funzioni o delle*** operazioni ***critiche o importanti*** 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 ***pubblica unica designata a norma***

del paragrafo 3 bis o, nel caso di fornitori terzi di servizi di TIC che stipulano direttamente accordi contrattuali con tester esterni, all'ENISA una sintesi riservata dei risultati dei test e la documentazione attestante che i test di penetrazione basati su minacce sono stati svolti conformemente alle prescrizioni. ***L'autorità pubblica unica o l'ENISA rilascia, se del caso,*** un attestato ***che confermi che i test sono stati svolti conformemente alle prescrizioni definite nella documentazione, in modo da consentire il riconoscimento reciproco dei test di penetrazione basati su minacce tra le autorità competenti***. ***L'attestato è condiviso con l'autorità competente dell'entità finanziaria e, se del caso, con l'autorità di sorveglianza capofila del fornitore terzo di servizi di TIC critico.***

3. Per l'effettuazione dei test di penetrazione basati su minacce, le entità finanziarie ***o i fornitori terzi di servizi di TIC autorizzati a stipulare accordi contrattuali direttamente con un tester esterno a norma del paragrafo 2 del presente articolo*** si avvalgono di tester in conformità dell'articolo 24.

Fatta salva la loro facoltà di delegare compiti e competenze a norma del presente articolo ad altre autorità competenti incaricate dei test di penetrazione basati su minacce, le autorità competenti identificano le entità finanziarie tenute a svolgere test di penetrazione basati su minacce ***in modo proporzionato*** 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.

3 bis. Gli Stati membri designano un'autorità pubblica unica responsabile dei testi di penetrazione basati su minacce nel settore finanziario a livello nazionale, fatta eccezione per l'identificazione delle entità finanziarie a norma del paragrafo 3, inclusi i testi di penetrazione basati su minacce svolti da entità finanziarie e da fornitori terzi di servizi di TIC che stipulano direttamente accordi contrattuali con tester esterni. All'autorità pubblica unica designata sono affidati tutti i compiti e le competenze a tal fine.

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 ***e su minacce, incuso il quadro TIBER-EU***, ***le AEV*** elaborano***, in coordinamento con l'ENISA, una serie di*** progetti di norme tecniche di regolamentazione per specificare ulteriormente quanto segue:

(a) i criteri utilizzati ai fini dell'applicazione del paragrafo ***3, secondo comma,*** 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 test di penetrazione basati su minacce nel contesto di entità finanziarie che operano in più di uno Stato membro ***e per facilitare il pieno riconoscimento reciproco dei test stessi, anche per quanto riguarda i test svolti da tester esterni che abbiano stipulato accordi contrattuali direttamente con fornitori terzi di servizi di TIC a norma del paragrafo 2 del presente articolo***, 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 ***sei*** 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 ***e i fornitori terzi di servizi di TIC autorizzati a stipulare accordi contrattuali direttamente con tester esterni a norma dell'articolo 23, paragrafo 2,*** 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***, indipendentemente dal fatto che provengano dall'Unione o da un paese terzo***;

(d) ▌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) ▌siano debitamente e pienamente coperti da un'assicurazione di responsabilità professionale, anche contro i rischi di colpa e negligenza.

(e bis) nel caso di tester esterni, siano stati approvati dalla pertinente autorità competente e dall'autorità pubblica unica designata a norma dell'articolo 23, paragrafo 3 bis, una volta che tali autorità abbiano verificato che l'entità finanziaria ha destinato risorse sufficienti e garantito che si evitassero conflitti

di interessi durante le fasi di progettazione e svolgimento dei test.

2. Le entità finanziarie ***e i fornitori terzi di servizi di TIC autorizzati a stipulare accordi contrattuali direttamente con tester esterni a norma dell'articolo 23, paragrafo 2,*** 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) ***della natura,*** 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;

   (b bis) del fatto che un fornitore di servizi di TIC sia, o meno, un fornitore intragruppo di tali servizi.

3. Nel contesto del quadro per la gestione dei rischi relativi alle TIC, le entità finanziarie ***diverse dalle microimprese*** adottano e riesaminano periodicamente una strategia per i rischi relativi alle TIC derivanti da terzi ▌. 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 ***a sostegno di funzioni critiche o importanti*** prestati da fornitori terzi.

   Gli accordi contrattuali di cui al primo comma sono opportunamente documentati ▌.

   Le entità finanziarie seguono gli orientamenti e le altre misure eventualmente disponibili adottati dalle AEV e dalle autorità competenti fino all'entrata in vigore delle norme tecniche di attuazione di cui al paragrafo 10.

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 ***a sostegno di funzioni critiche o importanti***, 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 ***aggiornati*** in materia di sicurezza ▌. ***Gli standard più recenti sono altresì presi in considerazione per determinare se gli standard in vigore in materia di sicurezza sono appropriati.***

7. Nell'esercizio dei diritti di accesso, ispezione e audit nei confronti del fornitore terzo di servizi di TIC ***in relazione a funzioni critiche o importanti***, 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 ***una*** complessità tecnologica ***sofisticata***, 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 ***garantiscono*** che ***gli*** accordi contrattuali per l'utilizzazione di servizi di TIC ***consentano alle entità finanziarie di adottare adeguate misure correttive o di riparazione, che potrebbero includere la totale risoluzione degli accordi, laddove non sia possibile una rettifica, o la risoluzione parziale degli accordi, laddove sia invece possibile una rettifica, conformemente al diritto applicabile,*** almeno nelle

seguenti circostanze:

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

(a bis) raccomandazione formulata dall'organismo congiunto di sorveglianza a norma dell'articolo 37 e destinata a un fornitore terzo di servizi di TIC critico;

(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 ***per quanto riguarda il suo contratto con l'entità finanziaria*** 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 ***manifestamente*** in grado di vigilare efficacemente sull'entità finanziaria in conseguenza dell'accordo contrattuale in questione.

8 bis. Al fine di ridurre il rischio di perturbazioni a livello dell'entità finanziaria, in circostanze debitamente giustificate e in accordo con le rispettive autorità competenti, l'entità finanziaria può decidere di non risolvere gli accordi contrattuali con il fornitore terzo di servizi di TIC finché non sia in grado di rivolgersi a un altro fornitore terzo di servizi di TIC o di passare a soluzioni interne adatte alla complessità del servizio fornito, in conformità con la strategia di uscita di cui al paragrafo 9.

8 ter. In caso di risoluzione di accordi contrattuali con fornitori terzi di servizi di TIC in una delle circostanze di cui al paragrafo 8, lettere da a) a d), le entità finanziarie non sostengono i costi di trasferimento dei dati da un fornitore terzo di servizi di TIC se il costo di tale trasferimento è superiore a quello del trasferimento di dati previsto nel contratto iniziale.

9. ***Per i servizi di TIC relativi a funzioni critiche o importanti,*** le entità finanziarie predispongono strategie di uscita ***soggette a riesame periodico. Tali strategie di uscita tengono*** 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***, o in caso di risoluzione di accordi contrattuali con fornitori terzi di servizi di TIC in una delle circostanze di cui al paragrafo 8, lettere da a) a d)***.

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 ***18 mesi*** 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 ***subappalto***

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 ***a*** servizi di TIC ***a sostegno di funzioni critiche o importanti*** 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 ***a sostegno di funzioni critiche o importanti*** 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 ***a sostegno di funzioni critiche o importanti*** 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 ▌.

Qualora gli accordi contrattuali per l'utilizzo di servizi di TIC ***a sostegno di funzioni critiche o importanti*** siano conclusi con un fornitore terzo ▌, le entità finanziarie considerano rilevanti almeno i fattori seguenti:

(a) ▌

(b) ▌

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

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

Qualora gli accordi contrattuali per l'utilizzo di servizi di TIC a sostegno di funzioni critiche o importanti siano conclusi con un fornitore terzo di servizi di TIC stabilito in un paese terzo, le entità finanziarie, in aggiunta alle considerazioni di cui al primo e al secondo comma, tengono altresì conto:

(a) del rispetto delle norme dell'Unione in materia di protezione dei dati; e

(b) dell'effettiva applicazione delle norme stabilite nel presente regolamento.

Qualora tali accordi contrattuali includano il subappalto di funzioni critiche o importanti, le entità finanziarie valutano se e come catene di subappalti potenzialmente lunghe e complesse possano incidere sulla loro capacità di ***valutare appieno i fattori elencati al primo e al secondo comma al fine*** di monitorare ▌ le funzioni appaltate e la 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 ***documentato per iscritto e reso*** disponibile alle parti in formato cartaceo o in un formato scaricabile e accessibile.

2. ***Le entità finanziarie e i fornitori terzi di servizi di TIC provvedono a che*** 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, ***segnatamente le regioni o i paesi,*** in cui si devono esercitare le funzioni ***di TIC*** e prestare i servizi ***di TIC*** 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 ***anticipatamente*** all'entità finanziaria l'intenzione di cambiare tali località;

(c) le disposizioni in materia di accessibilità, disponibilità, integrità, sicurezza***, riservatezza*** e protezione dei dati***, incusi i dati*** personali***;***

(c bis) le disposizioni relative alle 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***, o in caso di risoluzione degli accordi contrattuali***;

(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) ▌

(f) l'obbligo per il fornitore terzo di servizi di TIC di fornire assistenza in caso di incidente connesso alle TIC ***relativo al servizio fornito***, 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 ***offrano un adeguato livello di*** prestazione sicura dei servizi da parte dell'entità finanziaria, conformemente al proprio quadro normativo;

(h) ▌

(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 ***e di risoluzione, e, laddove tale accordo contrattuale abbia un impatto su un fornitore intragruppo di servizi di TIC dello stesso gruppo, un'analisi che segua un approccio basato sul rischio***;

(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 ***o di garantire la sua efficace risoluzione e ristrutturazione***;

(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;

(b bis) qualora tale accordo contrattuale abbia un impatto su un fornitore intragruppo di servizi TIC dello stesso gruppo, esso è analizzato seguendo un approccio basato sul rischio;

(k bis) una disposizione sul trattamento di dati personali da parte del fornitore terzo di servizi di TIC in conformità del regolamento (UE) 2016/679.

2 bis. Gli accordi contrattuali per la fornitura di funzioni critiche o importanti includono, in aggiunta al paragrafo 2, almeno quanto segue:

(a) 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;

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

(a) diritti di accesso, ispezione e audit da parte dell'entità finanziaria o di un terzo designato a tal fine, nonché il diritto di consultare in loco copie della documentazione pertinente se di importanza critica per le operazioni del fornitore terzo di servizi di TIC, il cui effettivo esercizio non sia impedito o limitato da altri accordi contrattuali o politiche di attuazione;

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

(c) l'impegno del fornitore terzo di servizi di TIC a cooperare senza riserve nel corso delle ispezioni e degli audit svolti in loco dalle autorità competenti, dall'autorità di sorveglianza capofila, dall'entità finanziaria o da un soggetto terzo designato, e a fornire dettagli sull'ambito di applicazione, le modalità e la frequenza di tali ispezioni e audit;

In deroga alla lettera b), il fornitore terzo di servizi di TIC e l'entità finanziaria possono convenire che i diritti di accesso, ispezione e audit possano essere delegati a una terza parte indipendente, nominata dal fornitore terzo di servizi di TIC, e che l'entità finanziaria sia in grado di richiedere in qualsiasi momento informazioni e garanzie alla terza parte sulle prestazioni del fornitore terzo di servizi di TIC.

2 ter. Gli accordi contrattuali per la fornitura di servizi di TIC da parte di un fornitore terzo di servizi di TIC stabilito in un paese terzo e definito come critico ai sensi dell'articolo 28, paragrafo 9, sono tenuti, fermi restando i paragrafi 2 e 2 bis del presente articolo, a:

(a) stabilire che il contratto sia retto dal diritto di uno Stato membro; e

(b) garantire che l'organismo congiunto di sorveglianza e l'autorità di sorveglianza capofila possano svolgere i compiti specificati all'articolo 30 sulla base delle competenze elencate all'articolo 31.

I servizi per i quali sono conclusi gli accordi contrattuali non sono obbligatoriamente eseguiti dall'entità costituita nell'Unione in virtù del diritto di uno Stato membro.

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.

3 bis. Le autorità competenti hanno facoltà di accedere agli accordi contrattuali di cui al presente articolo. Le parti di tali accordi contrattuali possono decidere di omettere informazioni sensibili o riservate sotto il profilo commerciale prima di accordare tale accesso alle autorità competenti, purché queste ultime siano pienamente informate della portata e della natura delle omissioni.

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). ***Nell'elaborazione di tali progetti di norme tecniche di regolamentazione, le AEV tengono conto delle dimensioni delle entità finanziarie, della natura, della portata e della complessità dei suoi servizi, delle sue attività e delle sue operazioni, nonché del suo profilo di rischio globale.***

Le AEV presentano detti progetti di norme tecniche di regolamentazione alla Commissione entro il [GU: inserire la data corrispondente a ***18 mesi*** 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 ***dell'organismo*** di sorveglianza istituito ai sensi dell'articolo 29, paragrafo 1***, nonché previa consultazione dell'ENISA***:

   (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.

   L'autorità di sorveglianza capofila nominata a norma del primo comma, lettera b), è responsabile della sorveglianza quotidiana del fornitore terzo di servizi di TIC critico.

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;

(f bis) la rilevanza e l'importanza dei servizi prestati dal pertinente fornitore terzo di servizi di TIC.

2 bis. Prima di procedere alla valutazione ai fini della designazione di cui al paragrafo 1, lettera a), l'organismo congiunto di sorveglianza informa il fornitore terzo di servizi di TIC.

L'organismo congiunto di sorveglianza notifica al fornitore terzo di servizi di TIC l'esito della valutazione di cui al primo comma fornendo un progetto di raccomandazione di criticità. Entro sei settimane dalla data di ricevimento del progetto di raccomandazione, il fornitore terzo di servizi di TIC può trasmettere una dichiarazione motivata sulla valutazione all'organismo congiunto di sorveglianza. La dichiarazione motivata contiene tutte le pertinenti informazioni supplementari ritenute appropriate dal fornitore terzo di servizi di TIC per migliorare la completezza e accuratezza della procedura di designazione o per contestare il progetto di raccomandazione di criticità. Il comitato congiunto delle AEV tiene debitamente conto della dichiarazione motivata e può richiedere ulteriori informazioni o prove al fornitore terzo di servizi di TIC prima di decidere in merito alla designazione.

Il comitato congiunto delle AEV notifica al fornitore terzo di servizi di TIC la sua designazione come critico. Il fornitore terzo di servizi di TIC dispone di un termine di almeno tre mesi dalla data di ricevimento della notifica per apportare gli adeguamenti necessari per consentire all'organismo congiunto di sorveglianza di svolgere i propri compiti ai sensi dell'articolo 30, nonché per informare le entità finanziarie alle quali il fornitore terzo presta servizi. Su richiesta debitamente giustificata del fornitore terzo di servizi di TIC designato, l'organismo congiunto di sorveglianza può concedere una proroga del periodo di adeguamento di massimo tre mesi.

3. Alla Commissione è conferito il potere di adottare ***un atto delegato*** conformemente all'articolo 50 per ***specificare ulteriormente*** 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. ***L'organismo congiunto di sorveglianza***, ***in consultazione con l'ENISA***, ***redige***, ***pubblica*** e ***aggiorna periodicamente*** 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, ***all'organismo congiunto*** di sorveglianza istituito ai sensi dell'articolo 29. ***L'organismo congiunto*** 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.

8 bis. Il comitato congiunto delle AEV, su raccomandazione dell'organismo congiunto di sorveglianza, designa i fornitori terzi di servizi di TIC stabiliti in un paese terzo che sono critici per le entità finanziarie a norma del paragrafo 1, lettera a).

Nel procedere alla designazione di cui al primo comma del presente paragrafo, le AEV e l'organismo congiunto di sorveglianza seguono le fasi procedurali di cui al paragrafo 2 bis.

9. Le entità finanziarie non ricorrono a un fornitore terzo di servizi di TIC ***critico*** stabilito in un paese terzo ***a meno che tale fornitore terzo di servizi di TIC non abbia un'impresa costituita nell'Unione a norma del diritto di uno Stato membro e non abbia concluso accordi contrattuali conformemente all'articolo 27, paragrafo 2 ter***.

Articolo 29

Struttura del quadro di sorveglianza

1. ***L'organismo*** congiunto ***di sorveglianza è istituito al fine*** di ***sorvegliare*** i rischi relativi alle TIC derivanti da terzi in tutti i settori finanziari ***e di condurre un'azione di sorveglianza diretta sui fornitori terzi di servizi di TIC designati come critici a norma dell'articolo 28***.

   Il ruolo dell'organismo congiunto di sorveglianza si limita a competenze di sorveglianza per i rischi relativi alle TIC legati ai servizi di TIC prestati a entità finanziarie da fornitori terzi di servizi di TIC critici.

   L'organismo congiunto 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. ***L'organismo congiunto*** 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.

L'organismo congiunto 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.

3. ***L'organismo congiunto*** di sorveglianza è composto dai ***direttori esecutivi*** delle AEV***,*** da un rappresentante di alto livello del personale in servizio ***delle AEV e da un rappresentante di alto livello di almeno otto autorità nazionali competenti***. ▌Un rappresentante della Commissione europea, del CERS, della BCE e dell'ENISA ***e almeno un esperto indipendente nominato a norma del paragrafo 3 bis del presente articolo*** partecipano ▌ in qualità di osservatori.

In seguito alla designazione annuale dei fornitori terzi di servizi di TIC critici a norma dell'articolo 28, paragrafo 1, lettera a), il comitato congiunto delle AEV decide quali autorità nazionali competenti saranno membri dell'organismo congiunto di sorveglianza, tenendo conto dei seguenti fattori:

(a) il numero di fornitori terzi di servizi di TIC critici stabiliti in uno Stato membro o che forniscono servizi nello stesso;

(b) la dipendenza delle entità finanziarie di uno Stato membro da fornitori terzi di servizi di TIC critici;

(c) le competenze di un'autorità nazionale competente in materia;

(d) le risorse e le capacità disponibili di un'autorità nazionale competente;

(e) la necessità di razionalizzare, snellire e rendere efficienti il funzionamento e il processo decisionale dell'organismo congiunto di sorveglianza.

L'organismo congiunto di sorveglianza condivide la propria documentazione e le proprie decisioni con tutte le autorità nazionali competenti che non sono membri dell'organismo congiunto di sorveglianza.

Il lavoro dell'organismo congiunto di sorveglianza è sostenuto e assistito da personale dedicato di tutte le AEV.

3 bis. L'esperto indipendente di cui al paragrafo 3 del presente articolo è nominato osservatore dall'organismo congiunto di sorveglianza al termine di una procedura di presentazione delle domande pubblica e trasparente.

L'esperto indipendente è nominato sulla base dell'esperienza maturata in settori quali la stabilità finanziaria, la resilienza operativa digitale e le questioni di sicurezza delle TIC per un mandato di due anni.

L'esperto indipendente nominato non è titolare di cariche a livello nazionale, unionale o internazionale. L'esperto indipendente agisce in piena indipendenza e obiettività nell'interesse esclusivo dell'Unione nel suo insieme, senza chiedere né ricevere istruzioni da parte di istituzioni od organi dell'Unione, governi degli Stati membri o altri soggetti pubblici o privati.

L'organismo congiunto di sorveglianza può decidere di nominare osservatori più esperti indipendenti.

4. Ai sensi dell'articolo 16 dei regolamenti (UE) n. 1093/2010, (UE) n. 1094/2010 e (UE) n. 1095/2010, le AEV formulano orientamenti ***entro il [GU: inserire la data corrispondente a 18 mesi dopo la data di entrata in vigore del presente regolamento]*** sulla cooperazione tra ***l'organismo congiunto di sorveglianza, l'autorità di sorveglianza capofila*** 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 ***l'organismo congiunto di sorveglianza***, nonché forniscono dettagli sullo scambio di informazioni necessario alle autorità competenti per garantire il seguito da dare alle raccomandazioni inviate ***dall'organismo congiunto di sorveglianza*** ai fornitori terzi di servizi di TIC critici a norma dell'articolo 31, paragrafo 1, lettera d).

5. 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.

6. ***L'organismo*** congiunto ***di sorveglianza presenta*** 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***, nominata a norma dell'articolo 28, paragrafo 1, lettera b), assume un ruolo di guida e coordinamento per quanto riguarda la sorveglianza quotidiana dei fornitori terzi di servizi di TIC critici e funge da primo punto di contatto per tali fornitori.***

1 bis. ***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. ***Tale valutazione si concentra essenzialmente sui servizi di TIC a sostegno di funzioni critiche o importanti prestate dai fornitori terzi di servizi di TIC critici alle entità finanziarie, ma può anche essere più ampia se pertinente ai fini della valutazione dei rischi cui tali funzioni sono esposte.***

2. La valutazione di cui al paragrafo 1 ***bis*** 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 ***gravi*** 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 ***bis effettuata dall'autorità di sorveglianza capofila***, ***l'organismo congiunto di sorveglianza, sotto il coordinamento e le indicazioni dell'autorità*** di sorveglianza capofila***, elabora e propone*** un piano di sorveglianza individuale, chiaro, dettagliato e motivato per ciascun fornitore terzo di servizi di TIC critico.

Nell'elaborazione del progetto di piano di sorveglianza, l'organismo congiunto di sorveglianza consulta tutte le autorità competenti e tutti i punti di contatto unici pertinenti di cui all'articolo 8 della direttiva (UE) 2016/1148 per garantire che non vi siano incoerenze o duplicazioni con gli obblighi del fornitore terzo di servizi di TIC critico previsti da tale direttiva.

Il piano di sorveglianza è adottato con cadenza annuale dal consiglio direttivo dell'autorità di sorveglianza capofila.

Prima dell'adozione, il progetto di piano ***di sorveglianza*** è comunicato ▌ al fornitore terzo di servizi di TIC critico.

Una volta ricevuto il progetto di piano di sorveglianza, il fornitore terzo di servizi di TIC critico dispone di sei settimane per riesaminare il progetto di piano di sorveglianza e inviare una dichiarazione motivata. Tale dichiarazione motivata può essere inviata solo se il fornitore terzo di servizi di TIC critico è in grado di dimostrare che l'esecuzione del piano di sorveglianza avrebbe un impatto sproporzionato sui clienti non soggetti al presente regolamento o rappresenterebbe una perturbazione per questi ultimi, o che esiste una soluzione più efficace o efficiente per gestire i rischi relativi alle TIC individuati. In caso di invio di una siffatta dichiarazione, il fornitore terzo di servizi di TIC critico suggerisce all'organismo congiunto di sorveglianza una soluzione più efficace o efficiente per conseguire gli obiettivi del progetto di piano di sorveglianza.

Prima di adottare il piano di sorveglianza, il consiglio direttivo dell'autorità di sorveglianza capofila esamina debitamente la dichiarazione motivata e può richiedere informazioni o prove aggiuntive al fornitore terzo di servizi di TIC.

4. Allorché i piani di sorveglianza annuali di cui al paragrafo 3 sono stati ***adottati*** 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'organismo congiunto*** di sorveglianza.

Articolo 31

Poteri di sorveglianza

1. Ai fini dello svolgimento dei compiti previsti dalla presente sezione, all'autorità di sorveglianza capofila sono conferiti i poteri indicati di seguito ***per i servizi prestati dai fornitori terzi di servizi di TIC critici alle entità finanziarie***:

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

   (b) condurre indagini e ispezioni ***in loco*** 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 al paragrafo ***1 bis***;

1 bis. Ai fini dello svolgimento dei compiti stabiliti nella presente sezione, e sulla base delle informazioni ottenute dall'autorità di sorveglianza capofila e dei risultati delle indagini condotte dall'autorità di sorveglianza capofila, l'organismo congiunto di sorveglianza ha il potere di 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'organismo congiunto di sorveglianza*** 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'organismo congiunto di sorveglianza*** 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'organismo congiunto di sorveglianza*** 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 ***e non ha un'impresa costituita nell'Unione ai sensi del diritto di uno Stato membro***;

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

– ***il subappalto comporterà rischi gravi ed evidenti per l'entità finanziaria o per la stabilità finanziaria del sistema finanziario dell'Unione.***

1 ter. I poteri di cui ai paragrafi 1 e 1 bis sono esercitati in relazione ai servizi di TIC che supportano funzioni non critiche o importanti forniti dal fornitore terzo di servizi di TIC critico, se necessario.

1 quater. Nell'esercizio dei poteri di cui ai paragrafi 1 e 1 bis del presente articolo, l'autorità di sorveglianza capofila e l'organismo congiunto di sorveglianza tengono debitamente conto del quadro istituito dalla direttiva (UE) 2016/1148 e, se necessario, consultano le pertinenti autorità competenti istituite da tale direttiva, al fine di evitare inutili duplicazioni delle misure tecniche e organizzative che potrebbero applicarsi ai fornitori terzi di servizi di TIC critici ai sensi di tale direttiva.

2. ***Prima di ultimare ed emettere raccomandazioni a norma del paragrafo 1 bis, l'organismo congiunto di sorveglianza informa il fornitore terzo di servizi di TIC critico in merito alle sue intenzioni e offre al fornitore terzo di servizi di TIC l'opportunità di fornire informazioni che ritiene dovrebbero essere ragionevolmente prese in considerazione prima che la raccomandazione sia ultimata o al fine di mettere in discussione le raccomandazioni previste. I motivi per mettere in discussione una raccomandazione possono includere il fatto che ci sarebbe un impatto sproporzionato o una perturbazione per i clienti non soggetti al presente regolamento o che esiste una soluzione più efficace o efficiente per gestire il rischio individuato.***

3. I fornitori terzi di servizi di TIC critici cooperano in buona fede con l'autorità di sorveglianza capofila ***e l'organismo congiunto di sorveglianza*** e ***li coadiuvano*** nell'adempimento dei ***loro*** compiti.

4. L'autorità di sorveglianza capofila può ***decidere, in caso di inosservanza totale o parziale delle misure che devono essere adottate a norma del paragrafo 1, lettere a), b) o c), e dopo la scadenza di un periodo di almeno 60 giorni di calendario dalla data in cui il fornitore terzo di servizi di TIC critico ha ricevuto la notifica della misura, di*** imporre una penalità di mora al fine di costringere il fornitore terzo di servizi di TIC critico ***a conformarsi***.

4 bis. ***La penalità di mora di cui al paragrafo 4 è imposta dall'autorità di sorveglianza capofila solo in ultima istanza e nei casi in cui il fornitore terzo di servizi di TIC critico non abbia rispettato le misure che devono essere adottate a norma del paragrafo 1, lettere a), b) o 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 ***fino*** all'1% del fatturato medio quotidiano realizzato a livello mondiale ***connesso ai servizi forniti alle entità finanziarie contemplate nel presente regolamento*** 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.

   I fornitori terzi di servizi di TIC critici sono tenuti a fornire le informazioni di cui al primo comma solo in relazione ai servizi prestate alle entità finanziarie soggette al presente regolamento e che utilizzano i servizi dei fornitori terzi di servizi di TIC critici per funzioni critiche o importanti. I fornitori terzi di servizi di TIC critici comunicano all'entità finanziaria pertinente le richieste specifiche riguardanti tale entità finanziaria.

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 ***mediante decisione*** 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 ***ragionevole*** 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 ***o quando tali informazioni non siano fornite entro il termine indicato alla lettera d)***;

(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 ***35***, paragrafo 1, può svolgere le necessarie indagini sui fornitori terzi di servizi di TIC ***conformemente al principio di proporzionalità***. ***Nello svolgimento dell'indagine, l'autorità di sorveglianza capofila procede con cautela e garantisce che i diritti dei clienti di fornitori terzi di servizi di TIC critici che non sono oggetto del presente regolamento siano protetti, anche in relazione all'impatto sui livelli di servizio, sulla disponibilità dei dati e sulla riservatezza***.

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) ***esaminare, in modo protetto,*** 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.

Il potere di effettuare ispezioni in loco di cui al primo comma non è limitato ai siti nell'Unione, a condizione che l'ispezione di un sito in un paese terzo soddisfi tutti i seguenti requisiti:

- ***è necessario che l'autorità di sorveglianza capofila svolga i suoi compiti a norma del presente regolamento;***
- ***occorre che vi sia un collegamento diretto con la fornitura di servizi di TIC a entità finanziarie dell'Unione;***
- ***è pertinente ai fini di un'indagine in corso.***

1 bis. Nello svolgimento di ispezioni in loco, l'autorità di sorveglianza capofila e il gruppo di esaminatori procedono con cautela e garantiscono che siano tutelati i diritti dei clienti dei fornitori terzi di servizi di TIC critici che non sono oggetto del presente regolamento, anche in relazione all'impatto sui livelli di servizio, sulla disponibilità dei dati e sulla riservatezza.

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 ***ritenuti appropriati e tecnologicamente rilevanti dall'autorità di sorveglianza capofila e*** utilizzati per la fornitura dei servizi alle entità finanziarie, o che vi contribuiscono.

5. Prima di qualsiasi ***ispezione*** 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***, delle altre AEV,*** 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'organismo congiunto di sorveglianza*** adotta le raccomandazioni rivolte al fornitore terzo di servizi di TIC critico in forza dei poteri che gli 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 ***e l'organismo congiunto di sorveglianza*** 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 ***dell'organismo congiunto di sorveglianza*** 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'organismo congiunto di sorveglianza*** ai sensi dell'articolo 31, paragrafo 1 ***bis***, i fornitori terzi di servizi di TIC critici comunicano ***all'organismo congiunto di sorveglianza*** se hanno intenzione di attenersi alle raccomandazioni. ***L'organismo congiunto di sorveglianza trasmette*** immediatamente le informazioni alle autorità competenti ***delle entità finanziarie interessate***.

2. Le autorità competenti ***informano le entità finanziarie che hanno concluso accordi contrattuali con fornitori terzi di servizi di TIC critici in merito ai rischi individuati nelle raccomandazioni rivolte dall'organismo congiunto di sorveglianza a tali fornitori terzi di servizi di TIC critici a norma dell'articolo 31, paragrafo 1 bis, e*** verificano se le entità finanziarie tengono conto dei rischi individuati. ***L'organismo congiunto di sorveglianza verifica se i fornitori terzi di servizi di TIC critici hanno affrontato i rischi individuati in tali raccomandazioni.***

3. ***Qualora gli obiettivi normativi non possano essere garantiti da altre misure e le autorità nazionali competenti abbiano inviato segnalazioni di allerta alle entità finanziarie interessate sulla base delle informazioni comunicate dall'organismo congiunto di sorveglianza, il consiglio dell'autorità di sorveglianza capofila può decidere, su raccomandazione dell'organismo congiunto di sorveglianza e previa consultazione delle*** autorità competenti ***delle*** entità finanziarie ***interessate***, di sospendere temporaneamente, in tutto o in parte, l'utilizzo o l'introduzione di un servizio prestato ***alle entità finanziarie esposte ai*** rischi identificati nelle raccomandazioni trasmesse al fornitore terzo di servizi di TIC critico fino a quando non siano stato affrontati ***tali*** rischi. Laddove si renda necessario, ***e come misura di ultima istanza,*** le autorità competenti possono chiedere ***ai fornitori terzi di servizi di TIC critici*** di risolvere, in tutto o in parte, gli accordi contrattuali pertinenti stipulati con ***le entità finanziarie esposte ai rischi individuati***.

4. Al momento di adottare le decisioni di cui al paragrafo 3, ***il consiglio dell'autorità di sorveglianza capofila tiene*** 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.

   (d bis) se la sospensione o la risoluzione introduce un rischio di continuità per le operazioni commerciali dell'utente del servizio del fornitore terzo di servizi di TIC critico.

4 bis. Le decisioni di cui al paragrafo 3 sono attuate soltanto quando sono state debitamente informate in merito tutte le entità finanziarie interessate. Alle entità finanziarie interessate è concesso un periodo di tempo, che non va al di là di quanto strettamente

necessario, per adeguare i loro accordi di esternalizzazione e contrattuali con i fornitori terzi di servizi di TIC critici in modo da non compromettere la resilienza operativa digitale ed eseguire le loro strategie di uscita e i piani di transizione di cui all'articolo 25.

I fornitori terzi di servizi di TIC critici soggetti alle decisioni di cui al paragrafo 3 cooperano pienamente con le entità finanziarie interessate.

5. Le autorità competenti informano ***l'organismo congiunto di sorveglianza*** in merito alle misure e agli approcci adottati nell'ambito dei propri compiti di vigilanza in relazione alle entità finanziarie.

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 ***derivanti dall'esecuzione dei compiti di cui alla presente sezione*** ed è proporzionato al fatturato del fornitore.

1 bis. Qualora venga stipulato un accordo amministrativo con un'autorità di regolamentazione e di vigilanza di un paese terzo a norma del paragrafo 1 del presente articolo, tale autorità può far parte del gruppo di esaminatori di cui all'articolo 35, paragrafo 1.

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 ***si adoperano per*** scambiarsi reciprocamente ***e con i fornitori terzi di servizi di TIC critici*** 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 ***e dei fornitori terzi di servizi di TIC***, in particolare svolgendo opera di sensibilizzazione in merito alle minacce informatiche, contenendo o inibendo la capacità di diffusione delle minacce informatiche e rafforzando capacità di difesa, tecniche di individuazione delle minacce, strategie di attenuazione o fasi di risposta e ripristino;

   (b) si svolge entro comunità fidate di entità finanziarie ***e di fornitori terzi di servizi di TIC***;

   (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[26] e delle linee direttrici sulla politica in materia di concorrenza[27].

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.

---

[26] 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).

[27] 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).

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;

(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 ***e gli offerenti*** di cripto-attività, gli emittenti ***e gli offerenti*** 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 ***e gli operatori di sistemi di regolamento 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 ***(UE) 2016/1011***;

(r) per i fornitori di servizi di crowdfunding, l'autorità competente designata in conformità dell'articolo ***29*** del regolamento ***(UE) 2020/1503***;

(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 ***sono*** invitate ***a partecipare*** ai lavori del gruppo di cooperazione***, nella misura in cui tali lavori riguardano, rispettivamente, le attività di vigilanza e di sorveglianza in relazione alle entità elencate al punto 7 dell'allegato II della direttiva (UE) 2016/1148 che sono state designate anche come fornitori terzi di servizi di TIC critici ai sensi dell'articolo 28 del presente regolamento***.

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.

2 bis. L'autorità di sorveglianza capofila informa le autorità competenti designate a norma della direttiva (UE) 2016/1148, e collabora con queste ultime, prima di svolgere indagini e ispezioni in loco di carattere generale a norma degli articoli 33 e 34 del presente regolamento.

Articolo 43

Comunicazione, cooperazione e attività finanziarie intersettoriali

1. Le AEV, tramite il comitato congiunto e in collaborazione con le autorità competenti, la BCE, ***il comitato di risoluzione unico per le informazioni relative alle entità che rientrano nell'ambito di applicazione del regolamento (UE) n. 806/2014*** 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 ***significativa*** minaccia ***informatica*** 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***,*** la BCE***, le autorità nazionali di risoluzione e il comitato di risoluzione unico per le informazioni relative alle entità che rientrano nell'ambito di applicazione del regolamento (UE) n. 806/2014*** 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 ***considerati*** 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 ***12 mesi*** 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, ***le sanzioni imposte e, in via eccezionale,*** 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]. ***La Commissione elabora una relazione sulla delega di potere al più tardi nove mesi prima della scadenza del periodo di cinque anni. La delega di potere è tacitamente prorogata per periodi di identica durata, a meno che il Parlamento europeo o il Consiglio non si oppongano a tale proroga al più tardi tre mesi prima della scadenza di ciascun periodo.***

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 a norma 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 ***tre*** 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 ***tre*** 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 ***Detta relazione contiene almeno i seguenti elementi:***

(a) ***la possibilità di estendere l'ambito di applicazione del presente regolamento agli operatori dei sistemi di pagamento;***

(b) ***il carattere volontario della comunicazione di minacce informatiche significative;***

(c) i criteri per la designazione dei fornitori terzi di servizi di TIC critici, di cui all'articolo 28, paragrafo 2; ***e***

(d) ***l'efficienza del processo decisionale dell'organismo congiunto di sorveglianza e lo scambio di informazioni tra l'organismo congiunto di sorveglianza e le autorità nazionali competenti non membri.***

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].";

I

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) "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 ***24*** 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.

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
Il presidente

Per il Consiglio
Il presidente

PROCEDURA DELLA COMMISSIONE COMPETENTE PER IL MERITO

Titolo	Resilienza operativa digitale per il settore finanziario e modifica dei regolamenti (CE) n. 1060/2009, (UE) n. 648/2012, (UE) n. 600/2014 e (UE) n. 909/2014
Riferimenti	COM(2020)0595 – C9-0304/2020 – 2020/0266(COD)
Presentazione della proposta al PE	24.9.2020
Commissione competente per il merito Annuncio in Aula	ECON 17.12.2020
Commissioni competenti per parere Annuncio in Aula	ITRE 17.12.2020 IMCO 17.12.2020
Pareri non espressi Decisione	ITRE 15.10.2020 IMCO 27.10.2020
Relatori Nomina	Billy Kelleher 15.10.2020
Esame in commissione	14.4.2021 14.6.2021
Approvazione	1.12.2021
Esito della votazione finale	+: –: 0: 44 5 5
Membri titolari presenti al momento della votazione finale	Gerolf Annemans, Gunnar Beck, Marek Belka, Isabel Benjumea Benjumea, Stefan Berger, Gilles Boyer, Engin Eroglu, Markus Ferber, Jonás Fernández, Raffaele Fitto, Frances Fitzgerald, Luis Garicano, Sven Giegold, Valentino Grant, Claude Gruffat, José Gusmão, Enikő Győri, Eero Heinäluoma, Danuta Maria Hübner, Stasys Jakeliūnas, France Jamet, Billy Kelleher, Ondřej Kovařík, Georgios Kyrtsos, Aurore Lalucq, Philippe Lamberts, Aušra Maldeikienė, Pedro Marques, Costas Mavrides, Jörg Meuthen, Csaba Molnár, Siegfried Mureşan, Caroline Nagtegaal, Luděk Niedermayer, Lefteris Nikolaou-Alavanos, Lídia Pereira, Kira Marie Peter-Hansen, Sirpa Pietikäinen, Evelyn Regner, Antonio Maria Rinaldi, Alfred Sant, Martin Schirdewan, Joachim Schuster, Ralf Seekatz, Pedro Silva Pereira, Paul Tang, Irene Tinagli, Ernest Urtasun, Inese Vaidere, Johan Van Overtveldt, Stéphanie Yon-Courtin, Marco Zanni, Roberts Zīle
Supplenti presenti al momento della votazione finale	Lefteris Christoforou
Deposito	7.12.2021

VOTAZIONE FINALE PER APPELLO NOMINALE
IN SEDE DI COMMISSIONE COMPETENTE PER IL MERITO

44	+
ECR	Raffaele Fitto, Johan Van Overtveldt, Roberts Zīle
NI	Enikő Győri
PPE	Isabel Benjumea Benjumea, Stefan Berger, Lefteris Christoforou, Markus Ferber, Frances Fitzgerald, Danuta Maria Hübner, Georgios Kyrtsos, Aušra Maldeikienė, Siegfried Mureşan, Luděk Niedermayer, Lídia Pereira, Sirpa Pietikäinen, Ralf Seekatz, Inese Vaidere
Renew	Gilles Boyer, Engin Eroglu, Luis Garicano, Billy Kelleher, Ondřej Kovařík, Caroline Nagtegaal, Stéphanie Yon-Courtin
S&D	Marek Belka, Jonás Fernández, Eero Heinäluoma, Aurore Lalucq, Pedro Marques, Costas Mavrides, Csaba Molnár, Evelyn Regner, Alfred Sant, Joachim Schuster, Pedro Silva Pereira, Paul Tang, Irene Tinagli
Verts/ALE	Sven Giegold, Claude Gruffat, Stasys Jakeliūnas, Philippe Lamberts, Kira Marie Peter-Hansen, Ernest Urtasun

5	-
ID	Gerolf Annemans, Gunnar Beck, France Jamet, Jörg Meuthen
NI	Lefteris Nikolaou-Alavanos

5	0
ID	Valentino Grant, Antonio Maria Rinaldi, Marco Zanni
The Left	José Gusmão, Martin Schirdewan

Significato dei simboli utilizzati:
+ : favorevoli
- : contrari
0 : astenuti