

Ns. Rif.: 225/24/VD

Milano, 2 agosto 2024

**OGGETTO: COMMISSIONE CONTROLLI INTERNI E COMMISSIONE ORGANIZZAZIONE E RISORSE UMANE**  
 Costituzione Gdl "DORA"

Cordiali saluti

Il Segretario Generale  
 Alessandro Carretta

**DISTRIBUZIONE:**

	COMMISSIONE CONTROLLI INTERNI	COMMISSIONE ORGANIZZAZIONE E RISORSE UMANE	e p.c.:
<b>AOSTA FACTOR</b>	Fabio BADERY Stefano SPANDONARI	Igor PATRUCCO	Alessandro BERTOLDO
<b>BANCA CF+</b>	Francesco LABELLARTE Pietro OTTAVIANI	Daniele TAORMINA Francesca DE FILIPPIS	DIREZIONE GENERALE Michele RONCHI
<b>BANCA DEL FUCINO</b>	DIREZIONE GENERALE	DIREZIONE GENERALE	DIREZIONE GENERALE Stefano CUPPERI
<b>BANCA IFIS</b>	Angelo FERRACCHIATI	Sara NICODEMO Polina VELEVA EMILOVA	Andrea BERNA Alberto STACCIONE
<b>BANCA MONTE DEI PASCHI DI SIENA</b>	Alessandro CAPANNOLI	Simone STARNINI Gabriele BARTOLOMMEI	Carmelo GIANIRACUSA
<b>BANCA PROGETTO</b>	Carolina KOWALCZUK Luca Pietro NOCERA	Claudio MINERDO Claudia CUNDARI	Giorgio GRAZIANI Giuseppe PIGNATELLI
<b>BANCA SISTEMA</b>	Franco POZZI	Nicolò FIORIO Raffaele SPINA	Andrea TRUPIA
<b>BANCO DESIO E BRIANZA</b>	DIREZIONE GENERALE	Emiliano MASSARELLI	Davide TOGNETTI
<b>BARCLAYS BANK IRELAND</b>	Massimo AGOSTI	Alessandro BERTOCCI	Alessandro RICCO
<b>BCC FACTORING</b>	Giacomo BORGIOLI Rossella SABATELLI	Giacomo BORGIOLI	Paolo IACHETTINI
<b>BFF BANK</b>	<b>Marina CORSI (*)</b> Gianluca POLETTI	Marilena FERRI	Massimiliano BELINGHERI
<b>BPER FACTOR</b>	<b>Matteo BIGARELLI (**)</b>	Stefano CLAPIS	Matteo BIGARELLI Vittorio GIUSTINIANI
<b>BURGO FACTOR</b>	DIREZIONE GENERALE	DIREZIONE GENERALE	Luca BERTINI
<b>CLESSIDRA FACTORING</b>	Rossella MAZZARINO Luca SIMIONATO	Andrea CAVERZAN Keoma GARBILLO	Gabriele PICCINI Keoma GARBILLO
<b>CREDEMFACTOR</b>	Lina SANTUCCI	Lorena GALIMBERTI	Gabriele DECO'
<b>CREDIT AGRICOLE FACTORING</b>	Luca CAIAZZO Giulio CESCATO	Luca FERRARI Sabrina MARTANI	Ivan TOMASSI
<b>EXPRIVIA</b>	DIREZIONE GENERALE	Roberta GULDEN	Dario GRECO
<b>FACTORCOOP</b>	Riccardo VANNINI	DIREZIONE GENERALE	Franco TAPPARO
<b>FACTORIT</b>	Tiziana MEZZANZANICA Alberto PONTI	Nuvola GIORI	Fabio BOLLINI
<b>FERCREDIT</b>	Virginia SALATINO	DIREZIONE GENERALE	Stefano PIERINI
<b>FIDIS</b>	Simonetta ARNULFO	DIREZIONE GENERALE	Andrea FAINA
<b>GENERALFINANCE</b>	Tommaso TOVAGLIERI John TSCHUOR	Ugo COLOMBO Cristiano PERONE	Massimo GIANOLLI
<b>GUBER BANCA</b>	Stefania ROSSETTI	Martina PELLICCIA Emanuela PULICINI	DIREZIONE GENERALE Simone PORCELLATI
<b>IFITALIA</b>	Paola SASSI	Luca BELLONI	Chiara BRACCI
<b>ILLIMITY BANK</b>	Franco MARCARINI	Franco MARCARINI	Franco MARCARINI
<b>INTESA SANPAOLO</b>	Andrea GARRONE Maurizio QUARZAGO	Anna CONTINI Federica MEROLA	Anna CARBONELLI
<b>ISTITUTO PER IL CREDITO SPORTIVO E CULTURALE</b>	Giuseppe NUSINER	Cristina ANTONELLI	DIREZIONE GENERALE Alfonso IAQUINANDI
<b>MBFACTA</b>	Alessia CASTAGNOLI	Carlo GIORGI	Enrico BUZZONI
<b>MCC FACTOR</b>	Antonio BALOTTA	Emanuele TARGIA	DIREZIONE GENERALE Alberto ROMANI
<b>SACE FCT</b>	Filippo RIZZUTO Cristina SPIZZICHINI	Marco SANSEVERINO <b>Silvia MASSARO (*)</b>	Daniele SCHRODER
<b>SG FACTORING</b>	Maria Cristina MINERVINO	Domenico GALLUZZO	Sylvain LOISEAU
<b>UNICREDIT FACTORING</b>	Filippo MERAVIGLIA MANTEGAZZA Stefano SALA	Davide GARIBOLDI <b>Daniela FERRARI (**)</b>	Daniela FERRARI

(\*) Coordinatore della Commissione

(\*\*) Presidente della Commissione

Il Regolamento (UE) 2022/2554 del Parlamento Europeo e del Consiglio del 14 dicembre 2022 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, (UE) n. 909/2014 e (UE) 2016/1011, cd. "Digital Operational Resilience Act" (DORA), stabilisce un framework vincolante per la gestione del rischio ICT nel settore finanziario, applicabile a tutte le banche e ai fornitori di servizi tecnologici critici. Il Regolamento, che entrerà in vigore nel gennaio 2025, mira a uniformare le normative sul rischio ICT a livello UE, migliorando la resilienza del sistema finanziario, introducendo requisiti per la gestione del rischio, la risposta agli incidenti, i test di resilienza e la gestione del rischio legato all'outsourcing nonché un sistema di monitoraggio e sanzionamento per le eventuali inadempienze da parte delle autorità di vigilanza.

Al fine di supportare gli Associati nel percorso di adeguamento a tali requisiti, d'intesa con i Presidenti e i Coordinatori delle Commissioni tecniche Controlli Interni e Organizzazione e Risorse Umane, si comunica la **costituzione del gruppo di lavoro "DORA"** con la finalità di uniformare la conoscenza degli Associati dei requisiti previsti dal Regolamento DORA e di contribuire alla risoluzione degli eventuali dubbi interpretativi residui, in vista della data di prima applicazione.

Si invitano i membri delle Commissioni in oggetto a comunicare il proprio interesse a partecipare ai lavori a [efact@assifact.it](mailto:efact@assifact.it) **entro il 26 agosto p.v.**

I lavori inizieranno ad inizio settembre.

Si ricorda che il presente documento, riservato agli Associati e non divulgabile all'esterno, è pubblicato nell'Area Commissioni dell'Area Riservata del sito associativo, a cui i membri delle Commissioni Tecniche possono accedere attraverso le credenziali personalizzate ricevute e che è possibile recuperare in autonomia le credenziali di accesso con il proprio indirizzo email cliccando su password o nome utente dimenticato: <https://areariservata.assifact.it>.

## I

*(Atti legislativi)*

## REGOLAMENTI

## REGOLAMENTO (UE) 2022/2554 DEL PARLAMENTO EUROPEO E DEL CONSIGLIO

del 14 dicembre 2022

**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, (UE) n. 909/2014 e (UE) 2016/1011****(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 <sup>(1)</sup>,visto il parere del Comitato economico e sociale europeo <sup>(2)</sup>,deliberando secondo la procedura legislativa ordinaria <sup>(3)</sup>,

considerando quanto segue:

- (1) Nell'era digitale le tecnologie dell'informazione e della comunicazione (TIC) sostengono sistemi complessi impiegati nelle attività quotidiane. Mantengono in funzione i principali settori delle nostre economie, tra cui il settore finanziario, e migliorano il funzionamento del mercato interno. Il crescente grado di digitalizzazione e interconnessione amplifica d'altra parte i rischi informatici, 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 delle attività delle entità finanziarie dell'Unione, ma la loro resilienza digitale deve ancora essere affrontata e integrata in maniera più efficace nei loro quadri operativi di portata più ampia.
- (2) Negli ultimi decenni, l'uso delle TIC ha conquistato un ruolo essenziale nella fornitura di servizi finanziari, al punto da acquisire oggi un'importanza critica nell'esecuzione delle consuete funzioni quotidiane di tutte le entità finanziarie. Ora la digitalizzazione riguarda ad esempio i pagamenti, che stanno progressivamente migrando dal contante e dal cartaceo verso soluzioni digitali, nonché la compensazione e il regolamento dei titoli, la negoziazione elettronica e algoritmica, le operazioni di prestito e finanziamento, la finanza tra pari (*peer-to-peer finance*), i rating del credito, la gestione dei crediti e le operazioni di back-office. Anche il settore assicurativo è stato trasformato

<sup>(1)</sup> GU C 343 del 26.8.2021, pag. 1.<sup>(2)</sup> GU C 155 del 30.4.2021, pag. 38.<sup>(3)</sup> Posizione del Parlamento europeo del 10 novembre 2022 (non ancora pubblicata nella Gazzetta ufficiale) e decisione del Consiglio del 28 novembre 2022.

dall'uso delle TIC, dall'emergere di intermediari assicurativi che offrono i loro servizi online e che operano con InsurTech fino alla sottoscrizione di assicurazioni digitali. Non solo l'intero settore finanziario è diventato in larga misura digitale, ma la digitalizzazione ha anche reso più marcate le interconnessioni e le dipendenze all'interno del settore e nei confronti di fornitori terzi di infrastrutture e servizi.

- (3) In una relazione del 2020 incentrata sul rischio informatico sistemico, 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, potrebbe costituire 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, senza trovare alcun ostacolo nelle frontiere geografiche. Gravi violazioni delle TIC che si verificano nel settore 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 ad esempio a pressanti richieste di rimborsi e a una generale perdita di fiducia nei mercati finanziari.
- (4) Negli ultimi anni, i rischi informatici hanno richiamato l'attenzione di responsabili politici e organismi di regolamentazione e normazione che, a livello nazionale, dell'Unione e internazionale, hanno cercato di migliorare la resilienza digitale, stabilire 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 il G7 e il G20, si propongono di fornire alle autorità competenti e agli operatori del mercato di varie giurisdizioni gli strumenti per potenziare la resilienza dei rispettivi sistemi finanziari. Tale lavoro è stato inoltre dettato dalla necessità di tenere debitamente conto dei rischi informatici nel contesto di un sistema finanziario globale altamente interconnesso e di perseguire una maggiore coerenza delle migliori prassi pertinenti.
- (5) Benché a livello dell'Unione e nazionale siano state adottate iniziative politiche e legislative mirate, i rischi informatici continuano a rappresentare una sfida per la resilienza operativa, le prestazioni e la stabilità del sistema finanziario dell'Unione. Le riforme che sono state introdotte sulla scia della crisi finanziaria del 2008 hanno rafforzato in primo luogo la resilienza finanziaria del settore finanziario dell'Unione, mirando a salvaguardare la competitività e la stabilità dell'Unione in una prospettiva 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 finanziaria 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) Nella comunicazione del 8 marzo 2018 intitolata «Piano d'azione per le tecnologie finanziarie: per un settore finanziario europeo più competitivo e innovativo» la Commissione 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 la fornitura efficace e ordinata dei servizi finanziari in tutta l'Unione, anche in situazioni di stress, preservando nel contempo la fiducia dei consumatori e degli operatori del mercato.
- (7) Nell'aprile 2019 l'Autorità europea di vigilanza (Autorità bancaria europea — ABE), istituita dal regolamento (UE) n. 1093/2010 del Parlamento europeo e del Consiglio <sup>(4)</sup>, l'Autorità europea di vigilanza (Autorità europea delle assicurazioni e delle pensioni aziendali e professionali — EIOPA) istituita dal regolamento (UE) n. 1094/2010 del Parlamento europeo e del Consiglio <sup>(5)</sup> e l'Autorità europea di vigilanza (Autorità europea degli strumenti finanziari e dei mercati — ESMA) istituita dal regolamento (UE) n. 1095/2010 del Parlamento europeo e del Consiglio <sup>(6)</sup>

<sup>(4)</sup> Regolamento (UE) n. 1093/2010 del Parlamento europeo e del Consiglio, del 24 novembre 2010, che istituisce l'Autorità europea di vigilanza (Autorità bancaria europea), modifica la decisione n. 716/2009/CE e abroga la decisione 2009/78/CE della Commissione (GU L 331 del 15.12.2010, pag. 12).

<sup>(5)</sup> Regolamento (UE) n. 1094/2010 del Parlamento europeo e del Consiglio, del 24 novembre 2010, che istituisce l'Autorità europea di vigilanza (Autorità europea delle assicurazioni e delle pensioni aziendali e professionali), modifica la decisione n. 716/2009/CE e abroga la decisione 2009/79/CE della Commissione (GU L 331 del 15.12.2010, pag. 48).

<sup>(6)</sup> Regolamento (UE) n. 1095/2010 del Parlamento europeo e del Consiglio, del 24 novembre 2010, che istituisce l'Autorità europea di vigilanza (Autorità europea degli strumenti finanziari e dei mercati), modifica la decisione n. 716/2009/CE e abroga la decisione 2009/77/CE della Commissione (GU L 331 del 15.12.2010, pag. 84).

(denominate collettivamente «autorità europee di vigilanza» o «AEV») hanno pubblicato congiuntamente pareri tecnici in cui si invocava l'adozione di un approccio coerente ai rischi informatici 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 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 la resilienza operativa digitale, rafforzando i mandati delle autorità competenti per consentire loro di vigilare sulla gestione dei rischi informatici nel settore finanziario al fine di proteggere l'integrità e l'efficienza del mercato interno ed agevolarne il regolare funzionamento.
- (9) Le disparità legislative e la disomogeneità degli approcci normativi o di vigilanza a livello nazionale per quanto riguarda i rischi informatici ostacolano il funzionamento del mercato interno dei servizi finanziari e intralciano il regolare esercizio della libertà di stabilimento e la libera prestazione di servizi per le entità finanziarie che operano su base transfrontaliera. Potrebbe risulterne falsata anche la concorrenza tra entità finanziarie dello stesso tipo attive in Stati membri diversi. È quanto accade 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 informatici derivanti da terzi. Le disparità provocate dagli sviluppi previsti a livello nazionale potrebbero produrre ostacoli ulteriori al funzionamento del mercato interno, a danno dei partecipanti al mercato e della stabilità finanziaria.
- (10) Ad oggi, dal momento che le disposizioni sui rischi informatici sono state trattate in modo soltanto parziale a livello di Unione, esistono carenze o sovrapposizioni in settori importanti, come la segnalazione degli incidenti connessi alle TIC e i test di resilienza operativa digitale, nonché 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 poiché 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 autonomamente sfide operative poste dai rischi informatici e dalla necessità di mitigare gli impatti avversi degli incidenti connessi alle TIC in maniera coerente ed efficiente sotto il profilo dei costi.
- (11) Dal momento che il codice unico non è accompagnato da un quadro generale per i rischi informatici o operativi, è necessario armonizzare ulteriormente i principali obblighi in materia di resilienza operativa digitale per tutte le entità finanziarie. Lo sviluppo delle capacità delle TIC e della resilienza complessiva da parte delle entità finanziarie, sulla base di tali obblighi fondamentali, al fine di far fronte ad interruzioni operative, contribuirebbe 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 interno, dovrebbe basarsi sulle disposizioni dell'articolo 114 del trattato sul funzionamento dell'Unione europea (TFUE) interpretate conformemente alla giurisprudenza costante della Corte di giustizia dell'Unione europea (Corte di giustizia).
- (12) Il presente regolamento mira a consolidare e aggiornare i requisiti in materia di rischi informatici nell'ambito dei requisiti in materia di rischi operativi che sono state finora trattati separatamente in vari atti giuridici dell'Unione. Tali atti 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 trattavano in maniera globale tutte le componenti della resilienza operativa. Le norme sui rischi operativi ulteriormente sviluppate in tali 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

informatici) rispetto a norme qualitative mirate concernenti le capacità di protezione, individuazione, contenimento, ripristino e rimedio in relazione agli incidenti connessi alle TIC, oppure le capacità di segnalazione e test digitali. Tali atti si prefiggevano principalmente lo scopo di trattare e aggiornare le norme fondamentali in materia di vigilanza prudenziale e integrità o condotta sul mercato. Tramite il consolidamento e l'aggiornamento delle diverse norme sui rischi informatici, tutte le disposizioni in materia di rischio digitale nel settore finanziario dovrebbero essere coerentemente riunite per la prima volta in un unico atto legislativo. Il presente regolamento colma pertanto le lacune o pone rimedio alle incoerenze di taluni fra i precedenti atti legislativi, anche per quanto riguarda la terminologia utilizzata, e fa esplicito riferimento ai rischi informatici tramite norme specifiche in materia di capacità di gestione dei rischi informatici, segnalazione degli incidenti, test di resilienza operativa e monitoraggio dei rischi informatici derivanti da terzi. Pertanto il presente regolamento dovrebbe altresì accrescere la consapevolezza dei rischi informatici e riconoscere che gli incidenti connessi alle TIC e la mancanza di resilienza operativa potrebbero compromettere la solidità delle entità finanziarie.

- (13) Nell'affrontare i rischi informatici è opportuno che le entità finanziarie seguano lo stesso approccio e le stesse norme basate su principi, tenendo conto delle loro dimensioni e del loro profilo di rischio complessivo, nonché della natura, della portata e della complessità dei loro servizi, delle loro attività e della loro operatività. La coerenza contribuisce ad accrescere la fiducia nel sistema finanziario e a preservarne la stabilità, soprattutto in tempi in cui l'elevata dipendenza da infrastrutture, piattaforme e sistemi di TIC comporta maggiori rischi digitali. Il rispetto dei fondamenti per la sicurezza dei sistemi TIC (*basic cyber hygiene*) 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) I regolamenti servono a ridurre la complessità normativa, favoriscono la convergenza della vigilanza, incrementano la certezza del diritto e contribuiscono altresì a limitare i costi di conformità, specialmente per le entità finanziarie che operano a livello transfrontaliero, e a ridurre le distorsioni della concorrenza. Pertanto, la scelta di un regolamento per istituire un quadro comune sulla resilienza operativa digitale delle entità finanziarie costituisce il metodo più idoneo per garantire l'applicazione omogenea e coerente di tutte le componenti della gestione dei rischi informatici da parte del settore finanziario dell'Unione.
- (15) La direttiva (UE) 2016/1148 del Parlamento europeo e del Consiglio <sup>(7)</sup> ha rappresentato il primo quadro orizzontale per la cibersicurezza adottato a livello di Unione, che 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 ha introdotto un meccanismo di identificazione a livello nazionale per gli operatori di servizi essenziali, solo alcuni enti creditizi, sedi di negoziazione e controparti centrali che sono stati identificati dagli Stati membri e rientrano in concreto nel suo ambito di applicazione e sono quindi tenuti a rispettare gli obblighi in materia di notifica degli incidenti e sicurezza connessi alle TIC contenute nella direttiva stessa. La direttiva (UE) 2022/2555 del Parlamento europeo e del Consiglio <sup>(8)</sup> stabilisce un criterio uniforme per stabilire quali entità rientrano nel suo ambito di applicazione (regola della soglia di dimensione), mantenendo nel contempo in tale ambito di applicazione anche i tre tipi di entità finanziarie.
- (16) Tuttavia, dal momento che il presente regolamento accresce il livello di armonizzazione delle varie componenti della resilienza digitale, introducendo requisiti in materia di gestione dei rischi informatici e segnalazione di incidenti connessi alle TIC più rigorosi rispetto a quelli contenuti nell'attuale normativa dell'Unione in materia di servizi finanziari, questo livello più elevato determina un incremento dell'armonizzazione anche rispetto ai requisiti di cui alla direttiva (UE) 2022/2555. Di conseguenza, il presente regolamento costituisce una *lex specialis* rispetto alla direttiva (UE) 2022/2555. Al tempo stesso, è essenziale mantenere un saldo rapporto tra il settore finanziario e il quadro orizzontale di cibersicurezza dell'Unione, come attualmente stabilito nella direttiva (UE) 2022/2555, per garantire la coerenza con le strategie di cibersicurezza adottate dagli Stati membri e permettere alle autorità di vigilanza finanziaria di venire a conoscenza degli incidenti informatici che colpiscono altri settori contemplati da tale direttiva.

<sup>(7)</sup> 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).

<sup>(8)</sup> Direttiva (UE) 2022/2555 del Parlamento europeo e del Consiglio, del 14 dicembre 2022, relativa a misure per un livello comune elevato di cibersicurezza nell'Unione, che modifica il regolamento (UE) n. 910/2014 e la direttiva (UE) 2018/1972 e che abroga la direttiva (UE) 2016/1148 (direttiva NIS 2) (cfr. pag. 80 della presente Gazzetta ufficiale).

- (17) A norma dell'articolo 4, paragrafo 2, del trattato sull'Unione europea e fatto salvo il controllo giurisdizionale della Corte di giustizia, il presente regolamento non dovrebbe pregiudicare la responsabilità degli Stati membri in relazione a funzioni essenziali dello Stato riguardanti la sicurezza pubblica, la difesa e la tutela della sicurezza nazionale, ad esempio per quanto riguarda la fornitura di informazioni che sarebbero contrarie alla tutela della sicurezza nazionale.
- (18) Per consentire l'apprendimento intersettoriale e attingere efficacemente alle esperienze di altri settori nella lotta alle minacce informatiche, le entità finanziarie di cui alla direttiva (UE) 2022/2555 dovrebbero continuare a far parte dell'«ecosistema» di quella direttiva [ad esempio il gruppo di cooperazione e i gruppi di intervento per la sicurezza informatica in caso di incidente (CSIRT)]. Le AEV e le autorità nazionali competenti dovrebbero poter partecipare alle discussioni strategiche delle politiche e ai lavori tecnici del gruppo di cooperazione ai sensi della direttiva, nonché scambiare informazioni e cooperare maggiormente con i punti di contatto unici designati o istituiti in conformità di tale direttiva. Le autorità competenti previste dal presente regolamento dovrebbero anche consultare i CSIRT e collaborare con loro. Le autorità competenti dovrebbero inoltre poter chiedere il parere tecnico delle autorità competenti designate o istituite in conformità della direttiva (UE) 2022/2555 e concludere accordi di cooperazione volti a garantire meccanismi di coordinamento efficaci e di risposta rapida.
- (19) Date le forti interconnessioni tra la resilienza digitale e la resilienza fisica delle entità finanziarie, nel presente regolamento e nella direttiva (UE) 2022/2557 del Parlamento europeo e del Consiglio <sup>(9)</sup> è necessario seguire un approccio coerente per quanto riguarda la resilienza dei soggetti critici. Dato che la resilienza fisica delle entità finanziarie è affrontata in modo globale dagli obblighi di gestione dei rischi informatici e di segnalazione disciplinati dal presente regolamento, gli obblighi di cui ai capi III e IV della direttiva (UE) 2022/2557 non dovrebbero applicarsi alle entità finanziarie che rientrano nell'ambito di applicazione di tale direttiva.
- (20) I fornitori di servizi di cloud computing sono una delle categorie di infrastrutture digitali contemplate dalla direttiva (UE) 2022/2555. Il quadro di sorveglianza dell'Unione (quadro di sorveglianza) istituito dal presente regolamento si applica a tutti i fornitori terzi critici di servizi TIC, compresi i fornitori di servizi di cloud computing che forniscono servizi TIC a entità finanziarie, e dovrebbe essere considerato complementare alla vigilanza condotta ai sensi della direttiva (UE) 2022/2555. Inoltre, in assenza di un quadro orizzontale dell'Unione 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.
- (21) Al fine di mantenere il pieno controllo sui rischi informatici, le entità finanziarie devono dotarsi di capacità generali per consentire una gestione dei rischi informatici forte ed efficace, nonché di politiche e meccanismi specifici per il trattamento di tutti gli incidenti connessi alle TIC e per la segnalazione degli incidenti più gravi connessi alle TIC. Analogamente, le entità finanziarie dovrebbero dotarsi di politiche per i test su processi, controlli e sistemi di TIC nonché per la gestione dei rischi informatici derivanti da terzi. È opportuno potenziare la resilienza operativa digitale di base per le entità finanziarie, consentendo tuttavia anche un'applicazione proporzionata dei requisiti a carico di talune entità finanziarie, in particolare le microimprese, così come le entità finanziarie soggette a un quadro semplificato per la gestione dei rischi informatici. Per agevolare una vigilanza efficace degli enti pensionistici aziendali o professionali che sia proporzionata e risponda alla necessità di ridurre gli oneri amministrativi a carico delle autorità competenti, le pertinenti disposizioni nazionali in materia di vigilanza applicabili a tali entità finanziarie dovrebbero tenere conto delle loro dimensioni e del loro profilo di rischio complessivo, nonché della natura, della portata e della complessità dei loro servizi, delle loro attività e della loro operatività, anche in caso di superamento delle soglie pertinenti di cui all'articolo 5 della direttiva (UE) 2016/2341 del Parlamento europeo e del Consiglio <sup>(10)</sup>. In particolare, le attività di vigilanza dovrebbero concentrarsi principalmente sulla necessità di affrontare i rischi gravi associati alla gestione dei rischi informatici di un'entità specifica.

<sup>(9)</sup> Direttiva (UE) 2022/2557 del Parlamento europeo e del Consiglio, del 14 dicembre 2022, sulla resilienza dei soggetti critici e che abroga la direttiva 2008/114/CE del Consiglio (cfr. pag. 164 della presente Gazzetta ufficiale).

<sup>(10)</sup> Direttiva (UE) 2016/2341 del Parlamento europeo e del Consiglio, del 14 dicembre 2016, relativa alle attività e alla vigilanza degli enti pensionistici aziendali o professionali (EPAP) (GU L 354 del 23.12.2016, pag. 37).

Le autorità competenti dovrebbero inoltre mantenere un approccio vigile ma proporzionato in relazione alla vigilanza degli enti pensionistici aziendali o professionali che, conformemente all'articolo 31 della direttiva (UE) 2016/2341, esternalizzano a fornitori di servizi una parte significativa delle loro attività principali, quali la gestione patrimoniale, i calcoli attuariali, la contabilità e la gestione dei dati.

- (22) 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 cibersecurity (ENISA) istituita dal regolamento (UE) 2019/881 del Parlamento europeo e del Consiglio <sup>(11)</sup> e dal gruppo di cooperazione istituito ai sensi della direttiva (UE) 2022/2555, ma in merito alla fissazione delle soglie e all'uso delle tassonomie si registrano ancora o possono emergere divergenze di approcci per le altre entità finanziarie. A causa di tali divergenze, vi sono una molteplicità di requisiti che le entità finanziarie devono rispettare, soprattutto quando operano in vari Stati membri oppure quando fanno parte di un gruppo finanziario. Inoltre, tali divergenze possono potenzialmente ostacolare la creazione di nuovi meccanismi uniformi o centralizzati dell'Unione che accelerano il processo di segnalazione e coadiuvano uno scambio di informazioni rapido e regolare tra le autorità competenti: elemento essenziale, quest'ultimo, per affrontare i rischi informatici nell'eventualità di attacchi su vasta scala con conseguenze potenzialmente sistemiche.
- (23) Al fine di ridurre gli oneri amministrativi e la potenziale duplicazione degli obblighi di segnalazione per talune entità finanziarie, l'obbligo di segnalazione degli incidenti a norma della direttiva (UE) 2015/2366 del Parlamento europeo e del Consiglio <sup>(12)</sup> dovrebbe cessare di applicarsi ai prestatori di servizi di pagamento che rientrano nell'ambito di applicazione del presente regolamento. Di conseguenza, gli enti creditizi, gli istituti di moneta elettronica, gli istituti di pagamento e i prestatori di servizi di informazione sui conti di cui all'articolo 33, paragrafo 1, di tale direttiva, dovrebbero, a decorrere dalla data di applicazione del presente regolamento, segnalare a norma del presente regolamento tutti gli incidenti operativi o relativi alla sicurezza dei pagamenti che sono stati precedentemente segnalati a norma di tale direttiva, indipendentemente dal fatto che si tratti di incidenti connessi alle TIC.
- (24) Per consentire alle autorità competenti di assolvere le funzioni di vigilanza acquisendo 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, il presente regolamento dovrebbe stabilire un solido regime di segnalazione degli incidenti connessi alle TIC in base ai cui requisiti sarebbero colmate le attuali lacune della normativa in materia di servizi finanziari ed eliminate le sovrapposizioni e le duplicazioni esistenti in modo da diminuire i costi. È 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 unico semplificato stabilito nel presente regolamento. Alle AEV si dovrebbe poi conferire il potere di precisare ulteriormente gli elementi pertinenti del quadro per la segnalazione degli incidenti connessi alle TIC come la tassonomia, i limiti temporali, le serie di dati, i modelli e le soglie applicabili. Per garantire la piena coerenza con la direttiva (UE) 2022/2555, alle entità finanziarie dovrebbe essere consentito, su base volontaria, di notificare all'autorità competente interessata le minacce informatiche significative qualora ritengano che la minaccia informatica sia rilevante per il sistema finanziario, gli utenti dei servizi o i clienti.
- (25) In taluni sottosettori finanziari sono stati elaborati requisiti in materia di test di resilienza operativa digitale che stabiliscono quadri che non sono sempre pienamente allineati. Ne è scaturita una potenziale duplicazione di costi per le entità finanziarie transfrontaliere, che rende complesso il reciproco riconoscimento dei risultati dei test di resilienza operativa digitale, il che a sua volta può frammentare il mercato interno.

<sup>(11)</sup> Regolamento (UE) 2019/881 del Parlamento europeo e del Consiglio, del 17 aprile 2019, relativo all'ENISA, l'Agenzia dell'Unione europea per la cibersecurity, e alla certificazione della cibersecurity per le tecnologie dell'informazione e della comunicazione, e che abroga il regolamento (UE) n. 526/2013 («regolamento sulla cibersecurity») (GU L 151 del 7.6.2019, pag. 15).

<sup>(12)</sup> Direttiva (UE) 2015/2366 del Parlamento europeo e del Consiglio, del 25 novembre 2015, relativa ai servizi di pagamento nel mercato interno, che modifica le direttive 2002/65/CE, 2009/110/CE e 2013/36/UE e il regolamento (UE) n. 1093/2010, e abroga la direttiva 2007/64/CE (GU L 337 del 23.12.2015, pag. 35).



- (26) Inoltre, qualora non si richiedano test relativi alle TIC, le vulnerabilità non sono individuate ed espongono quindi un'entità finanziaria a rischi informatici e, in ultima analisi, creano un rischio più elevato per la stabilità e l'integrità del settore finanziario. Senza un intervento dell'Unione, i test in materia di resilienza operativa digitale continuerebbero a essere incoerenti e non disporrebbero di un sistema di riconoscimento reciproco dei risultati dei test informatici fra le diverse giurisdizioni. È inoltre improbabile che altri sottosettori finanziari adottino regimi di test su scala significativa; pertanto essi si lascerebbero sfuggire i potenziali benefici di un quadro in materia di test, in termini di individuazione di vulnerabilità e rischi informatici, e verifica delle capacità di difesa e della continuità operativa, che contribuisca ad aumentare la fiducia di clienti, fornitori e partner commerciali. Per porre rimedio a tali sovrapposizioni, divergenze e carenze è necessario stabilire norme per un regime coordinato di test e agevolare così il riconoscimento reciproco dei test avanzati per le entità finanziarie che soddisfino i criteri di cui al presente regolamento.
- (27) La dipendenza delle entità finanziarie dall'uso dei servizi 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 tale 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.
- (28) Tale ampio uso dei servizi 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 altri requisiti normativi cui sono sottoposte oppure nell'applicare diritti specifici, quali i diritti di accesso o di audit, anche quando tali diritti siano previsti nei loro accordi contrattuali. Inoltre, molti di tali accordi contrattuali non contengono salvaguardie sufficienti per il monitoraggio esauriente dei processi di subappalto, e privano in tal modo l'entità finanziaria della capacità di valutare i rischi associati. Inoltre, dal momento che i fornitori terzi di servizi TIC spesso offrono servizi standardizzati a una clientela differenziata, tali accordi contrattuali non sono sempre idonei a soddisfare le esigenze individuali o specifiche dei soggetti del settore finanziario.
- (29) Anche se il diritto dell'Unione in materia di servizi finanziari contiene talune norme generali in materia di esternalizzazione, il monitoraggio della dimensione contrattuale non è sempre saldamente radicato nel diritto dell'Unione. In assenza di norme dell'Unione che si applichino in maniera chiara e mirata alle disposizioni contrattuali stipulate con fornitori terzi di servizi TIC, la fonte esterna dei rischi informatici rimane una questione non adeguatamente affrontata. È pertanto necessario stabilire alcuni principi fondamentali che indirizzino la gestione, da parte delle entità finanziarie, dei rischi informatici derivanti da terzi, che sono di particolare importanza quando le entità finanziarie ricorrono a fornitori terzi di servizi TIC a supporto delle loro funzioni essenziali o importanti. Tali principi dovrebbero essere accompagnati da una serie di diritti contrattuali di base concernenti vari elementi dell'esecuzione e della risoluzione degli accordi contrattuali, al fine di fornire alcune garanzie minime per rafforzare la capacità delle entità finanziarie di monitorare efficacemente tutti i rischi informatici che insorgono a livello di fornitori di servizi terzi. Tali principi sono complementari alla normativa settoriale applicabile all'esternalizzazione.
- (30) Oggi è evidente una certa carenza di omogeneità e convergenza per quanto riguarda il monitoraggio delle dipendenze da terzi nel settore delle TIC e dei rischi informatici derivanti da terzi. Nonostante gli sforzi per trattare l'esternalizzazione, come gli orientamenti dell'ABE in materia di esternalizzazione del 2019 e degli orientamenti dell'ESMA in materia di esternalizzazione a fornitori di servizi cloud del 2021, la questione più ampia del contrasto del rischio sistemico potenzialmente derivante dall'esposizione del settore finanziario a un ristretto numero di fornitori terzi critici di servizi TIC non è adeguatamente affrontata dal diritto dell'Unione. La carenza di norme a livello dell'Unione è aggravata dall'assenza di norme nazionali su strumenti e mandati che consentano alle autorità di vigilanza finanziaria 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.

- (31) Tenendo presenti i potenziali rischi sistemici derivanti dalla diffusione delle pratiche di esternalizzazione e dalla concentrazione dei servizi TIC forniti da terzi, e alla luce dell'inadeguatezza dei meccanismi nazionali nel fornire alle autorità di vigilanza finanziaria strumenti adeguati per quantificare, qualificare e rettificare le conseguenze dei rischi informatici che interessano i fornitori terzi critici di servizi TIC, è necessario stabilire un adeguato quadro di sorveglianza che preveda il monitoraggio costante delle attività di quei fornitori terzi di servizi TIC che sono fornitori terzi critici di servizi TIC per le entità finanziarie, garantendo nel contempo la riservatezza e la sicurezza dei clienti diversi dalle entità finanziarie. Sebbene la fornitura intragruppo di servizi TIC comporti rischi e benefici specifici, essa non dovrebbe essere automaticamente considerata meno rischiosa della fornitura di servizi TIC da parte di fornitori al di fuori di un gruppo finanziario e dovrebbe pertanto essere soggetta allo stesso quadro normativo. Tuttavia, quando i servizi TIC sono forniti dall'interno dello stesso gruppo finanziario, le entità finanziarie potrebbero esercitare un livello di controllo più elevato sui fornitori intragruppo, il che dovrebbe essere preso in considerazione nella valutazione complessiva del rischio.
- (32) Di fronte ai rischi informatici che si fanno sempre più complessi e sofisticati, la validità delle misure di individuazione e prevenzione dei rischi informatici dipende in larga misura da una costante condivisione delle analisi delle minacce e delle vulnerabilità tra le entità finanziarie. La condivisione delle informazioni contribuisce a creare una maggiore consapevolezza delle minacce informatiche. Ciò a sua volta accresce la capacità delle entità finanziarie di impedire che le minacce informatiche si trasformino in incidenti concreti connessi alle TIC e consente alle entità finanziarie di arginare in maniera più efficace l'impatto degli incidenti connessi alle TIC e di effettuare un ripristino più rapido. 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.
- (33) 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 quindi attualmente 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 sistema finanziario integrato. È pertanto importante rafforzare tali canali di comunicazione.
- (34) È opportuno incoraggiare le entità finanziarie a scambiarsi reciprocamente informazioni e analisi delle minacce informatiche e 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, partecipando a meccanismi di condivisione delle informazioni. È perciò necessario consentire l'emergere a livello dell'Unione di meccanismi volontari di condivisione delle informazioni i quali, se attuati in ambienti sicuri, aiuterebbero la comunità del settore finanziario a prevenire le minacce informatiche e a rispondervi collettivamente, contenendo rapidamente la diffusione dei rischi informatici e impedendo il potenziale contagio tramite i canali finanziari. Tali meccanismi dovrebbero essere conformi alle norme del diritto dell'Unione vigenti in materia di concorrenza di cui alla comunicazione della Commissione del 14 gennaio 2011 intitolata «Linee direttrici sull'applicabilità dell'articolo 101 del trattato sul funzionamento dell'Unione europea agli accordi di cooperazione orizzontale» nonché alle norme dell'Unione sulla protezione dei dati, in particolare il regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio <sup>(13)</sup>. Essi dovrebbero operare sulla base del ricorso a una o più basi giuridiche stabilite all'articolo 6 di tale regolamento, ad esempio 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, nonché nel contesto del trattamento dei dati personali necessario per adempiere un obbligo legale al quale è soggetto il titolare del trattamento, necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento ai sensi dell'articolo 6, paragrafo 1, lettere c) ed e), rispettivamente, di tale regolamento.

<sup>(13)</sup> 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).

- (35) Al fine di mantenere un elevato livello di resilienza operativa digitale per l'intero settore finanziario e al tempo stesso tenere il passo con gli sviluppi tecnologici, il presente regolamento dovrebbe affrontare i rischi derivanti da tutti i tipi di servizi TIC. A tal fine la definizione di servizi TIC nel contesto del presente regolamento dovrebbe essere intesa in senso lato e includere i servizi digitali e di dati forniti attraverso sistemi di TIC a uno o più utenti interni o esterni su base continuativa. Tale definizione dovrebbe includere, ad esempio, i cosiddetti servizi «over the top», che rientrano nella categoria dei servizi di comunicazione elettronica. Dovrebbe essere esclusa solo la limitata categoria dei servizi telefonici analogici tradizionali che possono essere considerati servizi di rete telefonica pubblica commutata (*Public Switched Telephone Network* — PSTN), servizi di rete terrestre, servizio telefonico tradizionale di base (*Plain Old Telephone Service* — POTS) o servizi di telefonia fissa.
- (36) Nonostante l'ampia portata prevista dal presente regolamento, l'applicazione delle norme in materia di resilienza operativa digitale dovrebbe tener conto delle differenze significative che si registrano tra le entità finanziarie in termini di dimensioni e profilo di rischio complessivo. Come principio generale, al momento di distribuire risorse e capacità per l'attuazione del quadro per la gestione dei rischi informatici, le entità finanziarie dovrebbero trovare il giusto equilibrio tra le proprie esigenze nel campo delle TIC, da un lato, e le loro dimensioni e il loro profilo di rischio complessivo, nonché la natura, la portata e la complessità dei loro servizi, delle loro attività e della loro operatività, dall'altro; le autorità competenti dovrebbero invece valutare e riesaminare costantemente l'approccio che guida tale distribuzione.
- (37) I prestatori di servizi di informazione sui conti di cui all'articolo 33, paragrafo 1, della direttiva (UE) 2015/2366 rientrano esplicitamente nell'ambito di applicazione del presente regolamento, tenendo conto della natura specifica delle loro attività e dei rischi che ne derivano. Inoltre, gli istituti di moneta elettronica e gli istituti di pagamento esentati a norma dell'articolo 9, paragrafo 1, della direttiva 2009/110/CE del Parlamento europeo e del Consiglio <sup>(14)</sup> e dell'articolo 32, paragrafo 1, della direttiva (UE) 2015/2366 rientrano nell'ambito di applicazione del presente regolamento anche se non hanno ottenuto l'autorizzazione a norma della direttiva 2009/110/CE a emettere moneta elettronica o se non hanno ottenuto l'autorizzazione a norma della direttiva (UE) 2015/2366 a prestare ed eseguire servizi di pagamento. Tuttavia, gli uffici postali di cui all'articolo 2, paragrafo 5, punto 3), della direttiva 2013/36/UE del Parlamento europeo e del Consiglio <sup>(15)</sup> sono esclusi dall'ambito di applicazione del presente regolamento. L'autorità competente per gli istituti di pagamento esentati a norma della direttiva (UE) 2015/2366, gli istituti di moneta elettronica esentati a norma della direttiva 2009/110/CE e i prestatori di servizi di informazione sui conti di cui all'articolo 33, paragrafo 1, della direttiva (UE) 2015/2366, dovrebbe essere l'autorità competente designata a norma dell'articolo 22 della direttiva (UE) 2015/2366.
- (38) Poiché le entità finanziarie di maggiori dimensioni potrebbero disporre di maggiori risorse e possono destinare rapidamente fondi allo sviluppo di strutture di governance e all'elaborazione di 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 aziendali per la supervisione degli accordi con i fornitori terzi di servizi TIC o per affrontare la gestione delle crisi, per organizzare la loro gestione dei rischi informatici secondo il modello delle tre linee di difesa o ancora per stabilire un modello interno di controllo e gestione del rischio e sottoporre ad audit interni il proprio quadro per la gestione dei rischi informatici.
- (39) Alcune entità finanziarie beneficiano di esenzioni o sono soggette a un quadro normativo meno rigoroso a norma della pertinente normativa settoriale dell'Unione. Tali entità finanziarie includono i gestori di fondi di investimento alternativi di cui all'articolo 3, paragrafo 2, della direttiva 2011/61/UE del Parlamento europeo e del Consiglio <sup>(16)</sup>, le imprese di assicurazione e di riassicurazione di cui all'articolo 4 della direttiva 2009/138/CE del Parlamento europeo e del Consiglio <sup>(17)</sup> e gli enti pensionistici aziendali o professionali che gestiscono schemi pensionistici che

<sup>(14)</sup> 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).

<sup>(15)</sup> Direttiva 2013/36/UE del Parlamento europeo e del Consiglio, del 26 giugno 2013, sull'accesso all'attività degli enti creditizi e sulla vigilanza prudenziale sugli enti creditizi e sulle imprese di investimento, che modifica la direttiva 2002/87/CE e abroga le direttive 2006/48/CE e 2006/49/CE (GU L 176 del 27.6.2013, pag. 338).

<sup>(16)</sup> Direttiva 2011/61/UE del Parlamento europeo e del Consiglio, dell'8 giugno 2011, sui gestori di fondi di investimento alternativi, che modifica le direttive 2003/41/CE e 2009/65/CE e i regolamenti (CE) n. 1060/2009 e (UE) n. 1095/2010 (GU L 174 dell'1.7.2011, pag. 1).

<sup>(17)</sup> Direttiva 2009/138/CE del Parlamento europeo e del Consiglio, del 25 novembre 2009, in materia di accesso ed esercizio delle attività di assicurazione e di riassicurazione (solvibilità II) (GU L 335 del 17.12.2009, pag. 1).

contano congiuntamente non più di 15 aderenti in totale. Alla luce di tali esenzioni non sarebbe proporzionato includere tali entità finanziarie nell'ambito di applicazione del presente regolamento. Inoltre, il presente regolamento riconosce le specificità della struttura del mercato dell'intermediazione assicurativa, con la conseguenza che gli intermediari assicurativi, gli intermediari riassicurativi e gli intermediari assicurativi a titolo accessorio che rientrano nella definizione di microimprese o di piccole o medie imprese non dovrebbero essere soggetti al presente regolamento.

- (40) Poiché le entità di cui all'articolo 2, paragrafo 5, punti da 4) a 23), della direttiva 2013/36/UE sono escluse dall'ambito di applicazione di tale direttiva, gli Stati membri dovrebbero quindi poter scegliere di esentare dall'applicazione del presente regolamento tali entità situate nei rispettivi territori.
- (41) Analogamente, al fine di allineare il presente regolamento all'ambito di applicazione della direttiva 2014/65/UE del Parlamento europeo e del Consiglio <sup>(18)</sup>, è altresì opportuno escludere dall'ambito di applicazione del presente regolamento le persone fisiche e giuridiche di cui agli articoli 2 e 3 di tale direttiva che sono autorizzate a prestare servizi di investimento senza dover ottenere un'autorizzazione a norma della direttiva 2014/65/UE. Tuttavia l'articolo 2 della direttiva 2014/65/UE esclude anche dall'ambito di applicazione di tale direttiva le entità considerate entità finanziarie ai fini del presente regolamento, quali i depositari centrali di titoli, gli organismi d'investimento collettivo o le imprese di assicurazione e di riassicurazione. L'esclusione dall'ambito di applicazione del presente regolamento delle persone e delle entità di cui agli articoli 2 e 3 di tale direttiva non dovrebbe comprendere tali depositari centrali di titoli, organismi d'investimento collettivo o imprese di assicurazione e di riassicurazione.
- (42) A norma del diritto settoriale dell'Unione, alcune entità finanziarie sono soggette a requisiti meno rigorosi o esenzioni per motivi legati alle loro dimensioni o ai servizi che forniscono. Tale categoria di entità finanziarie include le imprese di investimento piccole e non interconnesse, i piccoli enti pensionistici aziendali o professionali che possono essere esclusi dall'ambito di applicazione della direttiva (UE) 2016/2341 alle condizioni di cui all'articolo 5 di tale direttiva dallo Stato membro interessato e che gestiscono schemi pensionistici che contano congiuntamente non più di cento aderenti in totale, nonché gli enti esentati a norma della direttiva 2013/36/UE. Pertanto, conformemente al principio di proporzionalità e al fine di preservare lo spirito della normativa settoriale dell'Unione, è altresì opportuno che tali entità finanziarie siano soggette a un quadro semplificato per la gestione dei rischi informatici a norma del presente regolamento. La proporzionalità del quadro per la gestione dei rischi informatici riguardante tali entità finanziarie non dovrebbe essere modificata dalle norme tecniche di regolamentazione che devono essere elaborate dalle AEV. Inoltre, conformemente al principio di proporzionalità, è opportuno che anche gli istituti di pagamento di cui all'articolo 32, paragrafo 1, della direttiva (UE) 2015/2366 e gli istituti di moneta elettronica di cui all'articolo 9 della direttiva 2009/110/CE esentati conformemente al diritto nazionale che recepisce tali atti giuridici dell'Unione siano soggetti a un quadro semplificato per la gestione dei rischi informatici a norma del presente regolamento, mentre gli istituti di pagamento e gli istituti di moneta elettronica che non sono stati esentati conformemente al rispettivo diritto nazionale che recepisce la normativa settoriale dell'Unione dovrebbero rispettare il quadro generale stabilito dal presente regolamento.
- (43) Analogamente, le entità finanziarie che rientrano nella definizione di microimprese o sono soggette al quadro semplificato per la gestione dei rischi informatici a norma del presente regolamento non dovrebbero essere tenute a istituire una funzione per il monitoraggio degli accordi conclusi con i fornitori terzi di servizi TIC per l'uso di tali servizi, o a designare un dirigente di rango elevato quale responsabile della sorveglianza sulla relativa esposizione al rischio e sulla documentazione pertinente; ad attribuire la responsabilità della gestione e della sorveglianza dei rischi informatici a una funzione di controllo e garantire un adeguato livello di indipendenza di tale funzione per evitare conflitti d'interessi; a documentare e riesaminare almeno una volta all'anno il quadro per la gestione dei rischi informatici; a sottoporre ad audit interno periodico il quadro per la gestione dei rischi informatici; a svolgere valutazioni approfondite dopo modifiche di rilievo dei loro processi e delle loro infrastrutture di rete e dei sistemi informativi; a compiere periodicamente analisi dei rischi sui sistemi legacy; a sottoporre a verifiche di audit interno indipendenti l'attuazione dei piani di risposta e ripristino relativi alle TIC; a disporre di una funzione di gestione delle crisi; ad ampliare i test sulla continuità operativa e i piani di risposta e ripristino per descrivere gli scenari di passaggio tra le infrastrutture TIC primarie e quelle di ridondanza; a comunicare, su loro richiesta, alle autorità

<sup>(18)</sup> Direttiva 2014/65/UE del Parlamento europeo e del Consiglio, del 15 maggio 2014, relativa ai mercati degli strumenti finanziari e che modifica la direttiva 2002/92/CE e la direttiva 2011/61/UE (GU L 173 del 12.6.2014, pag. 349).

competenti una stima dei costi e delle perdite annuali aggregati causati da gravi incidenti connessi alle TIC; a mantenere capacità di TIC ridondanti; a comunicare alle autorità nazionali competenti le modifiche apportate a seguito dei riesami successivi agli incidenti connessi alle TIC; a monitorare costantemente i pertinenti sviluppi tecnologici, a istituire un programma di test di resilienza operativa digitale esaustivo quale parte integrante del quadro per la gestione dei rischi informatici di cui al presente regolamento o ad adottare e riesaminare periodicamente una strategia per i rischi informatici derivanti da terzi. Inoltre, le microimprese dovrebbero essere tenute a valutare la necessità di mantenere tali capacità di TIC ridondanti solo sulla base del loro profilo di rischio. Le microimprese dovrebbero beneficiare di un regime più flessibile per quanto riguarda i programmi di test di resilienza operativa digitale. Quando valutano il tipo e la frequenza dei test da svolgere, dovrebbero trovare il giusto equilibrio tra l'obiettivo di mantenere un'elevata resilienza operativa digitale, le risorse disponibili e il loro profilo di rischio complessivo. Le microimprese e le entità finanziarie soggette al quadro semplificato per la gestione dei rischi informatici a norma al presente regolamento dovrebbero essere esentate dall'obbligo di svolgere test avanzati di strumenti, sistemi e processi di TIC fondati su test di penetrazione guidati dalla minaccia (*threat-led penetration testing* — TLPT), in quanto solo le entità finanziarie che soddisfano i criteri di cui al presente regolamento dovrebbero essere tenute a svolgere tali test. Alla luce delle loro limitate capacità, le microimprese dovrebbero poter concordare con il fornitore terzo di servizi TIC di delegare i diritti di accesso, ispezione e audit dell'entità finanziaria a un terzo indipendente nominato dal fornitore terzo di servizi TIC, a condizione che l'entità finanziaria possa richiedere in qualsiasi momento al rispettivo terzo indipendente tutte le informazioni e le garanzie pertinenti sulle prestazioni del fornitore terzo di servizi TIC.

- (44) Dal momento che solo le entità finanziarie identificate 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 gravare soltanto su una piccola percentuale delle entità finanziarie.
- (45) Per garantire il pieno allineamento e la coerenza complessiva tra le strategie aziendali delle entità finanziarie, da un lato, e la gestione dei rischi informatici, dall'altro, è opportuno richiedere agli organi di gestione delle entità finanziarie di mantenere un ruolo attivo e fondamentale nella guida e nell'adeguamento del quadro per la gestione dei rischi informatici e della strategia globale di resilienza operativa digitale. Gli organi di gestione dovrebbero 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 osservare a tutti i livelli una rigorosa igiene informatica (*cyber hygiene*). La responsabilità principale dell'organo di gestione nell'affrontare i rischi informatici di un'entità finanziaria dovrebbe concretizzarsi nel principio guida di tale approccio complessivo, tradotto ulteriormente nel costante coinvolgimento dell'organo di gestione a controllare il monitoraggio della gestione dei rischi informatici.
- (46) Inoltre, il principio della piena e principale responsabilità dell'organo di gestione per la gestione dei rischi informatici dell'entità finanziaria si accompagna alla necessità di assicurare un livello di investimenti connessi alle TIC e un bilancio complessivo dell'entità finanziaria che consentirebbero all'entità finanziaria di conseguire un elevato livello di resilienza operativa digitale.
- (47) Sulla scia delle migliori prassi, linee guida, raccomandazioni e approcci pertinenti a livello internazionale, nazionale e settoriale in materia di gestione dei rischi informatici, il presente regolamento promuove una serie di principi che favoriscono una struttura complessiva della gestione dei rischi informatici. Di conseguenza, nella misura in cui le principali capacità introdotte dalle entità finanziarie soddisfano le varie funzioni nella gestione dei rischi informatici (identificazione, protezione e prevenzione, individuazione, risposta e ripristino, apprendimento, evoluzione e comunicazione) indicate nel presente regolamento, le entità finanziarie dovrebbero conservare la libertà di impiegare modelli di gestione dei rischi informatici strutturati o categorizzati in maniera diversa.
- (48) Per tenere il passo con l'evoluzione del contesto delle minacce informatiche, le entità finanziarie dovrebbero dotarsi di sistemi di TIC aggiornati, affidabili e capaci non solo per garantire il trattamento dei dati richiesto per i loro servizi, ma anche per assicurare una resilienza tecnologica sufficiente che consenta loro di fare adeguatamente fronte alle esigenze di trattamento aggiuntive derivanti da condizioni di stress del mercato o da altre situazioni avverse.

- (49) 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 conformemente alle loro politiche di backup. Tuttavia, tale ripresa non dovrebbe in alcun modo mettere a repentaglio l'integrità e la sicurezza dei sistemi informatici e di rete, né la disponibilità, l'autenticità, l'integrità o la riservatezza dei dati.
- (50) Il presente regolamento permette alle entità finanziarie di fissare i loro obiettivi di tempo di ripristino e punto di ripristino (*recovery time and recovery point objectives*) in maniera flessibile e quindi di fissare tali obiettivi tenendo conto della natura e della criticità delle funzioni pertinenti nonché di eventuali esigenze aziendali specifiche, ma per fissare tali obiettivi dovrebbero comunque essere tenute a effettuare una valutazione del potenziale impatto sull'efficienza del mercato.
- (51) I propagatori di attacchi informatici tendono a perseguire guadagni finanziari direttamente alla fonte, esponendo quindi le entità finanziarie a conseguenze significative. Per scongiurare il pericolo che i sistemi di TIC perdano l'integrità o divengano indisponibili e per evitare pertanto violazioni di dati e prevenire danni alle infrastrutture fisiche delle TIC, è opportuno migliorare e razionalizzare sensibilmente la segnalazione, da parte delle entità finanziarie, degli incidenti gravi connessi alle TIC. È opportuno armonizzare la segnalazione degli incidenti connessi alle TIC mediante l'introduzione di un obbligo per tutte le entità finanziarie di segnalare direttamente alle rispettive autorità competenti. Se un'entità finanziaria è soggetta alla vigilanza di più di un'autorità nazionale competente, gli Stati membri dovrebbero designare un'unica autorità competente quale destinataria di tale segnalazione. Gli enti creditizi classificati come significativi ai sensi dell'articolo 6, paragrafo 4, del regolamento (UE) n. 1024/2013 del Consiglio <sup>(19)</sup> dovrebbero presentare tale segnalazione alle autorità nazionali competenti, che dovrebbero successivamente trasmettere la segnalazione alla Banca centrale europea (BCE).
- (52) La segnalazione diretta dovrebbe consentire alle autorità di vigilanza finanziaria di avere immediato accesso alle informazioni relative agli incidenti gravi connessi alle TIC. Le autorità di vigilanza finanziaria dovrebbero a loro volta trasmettere i dettagli relativi agli incidenti gravi connessi alle TIC alle pubbliche autorità non finanziarie [quali le competenti autorità e i punti di contatto unici a norma della direttiva (UE) 2022/2555, le autorità nazionali per la protezione dei dati e le autorità di contrasto per gli incidenti gravi connessi alle TIC di natura penale], al fine di migliorare la consapevolezza di tali autorità in merito a tali incidenti e, nel caso dei CSIRT, di agevolare la tempestiva assistenza che può essere fornita alle entità finanziarie, se del caso. Gli Stati membri dovrebbero, inoltre, poter stabilire che le entità finanziarie stesse debbano fornire tali informazioni alle autorità pubbliche al di fuori del settore dei servizi finanziari. Tali flussi di informazioni dovrebbero consentire alle entità finanziarie di beneficiare rapidamente di qualsiasi contributo tecnico pertinente, di consulenza sui rimedi e del successivo seguito dato da tali autorità. Le informazioni sugli incidenti gravi 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, le analisi delle minacce informatiche e le vulnerabilità concernenti un determinato incidente, per promuovere una più ampia difesa collettiva.
- (53) Tutte le entità finanziarie dovrebbero essere tenute a effettuare segnalazioni di incidenti, ma tale obbligo non dovrebbe interessarle tutte allo stesso modo. Infatti, si dovrebbe procedere a una debita calibrazione delle soglie di rilevanza pertinenti, nonché delle tempistiche delle segnalazioni, nel contesto degli atti delegati basati sulle norme tecniche di regolamentazione che le AEV devono elaborare, al fine di cogliere unicamente gli incidenti gravi connessi alle TIC. Inoltre, le specificità delle entità finanziarie dovrebbero essere prese in considerazione nello stabilire il calendario per gli obblighi di segnalazione.
- (54) Il presente regolamento dovrebbe imporre agli enti creditizi, agli istituti di pagamento, ai prestatori di servizi di informazione sui conti e agli istituti di moneta elettronica di segnalare tutti gli incidenti operativi o relativi alla sicurezza dei pagamenti — precedentemente segnalati a norma della direttiva (UE) 2015/2366 — indipendentemente dalla natura TIC dell'incidente.

<sup>(19)</sup> 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).

- (55) Le AEV dovrebbero essere incaricate di valutare la fattibilità e le condizioni per una possibile centralizzazione delle segnalazioni di incidenti connessi alle TIC a livello dell'Unione. Tale centralizzazione potrebbe consistere in un unico polo dell'UE per la segnalazione di incidenti gravi connessi alle TIC che riceva direttamente le segnalazioni pertinenti e le notifichi automaticamente alle autorità nazionali competenti o che si limiti a centralizzare le segnalazioni pertinenti trasmesse dalle competenti autorità nazionali e pertanto assolva una funzione di coordinamento. Le AEV dovrebbero essere incaricate di preparare in collaborazione con la BCE e l'ENISA, una relazione comune che esamini la praticabilità dell'istituzione di un unico polo dell'UE.
- (56) Per conseguire un elevato livello di resilienza operativa digitale, e in linea sia con le pertinenti norme internazionali (ad esempio, gli elementi fondamentali del G7 per i test di penetrazione basati su minacce) che con i quadri applicati nell'Unione, come TIBER-EU, le entità finanziarie dovrebbero sottoporre periodicamente a test i propri sistemi di TIC e il proprio personale con responsabilità connesse alle TIC per valutare l'efficacia delle relative capacità di prevenzione, individuazione, risposta e ripristino, allo scopo di scoprire e affrontare le potenziali vulnerabilità in materia di TIC. Per rispecchiare le differenze esistenti tra i vari sottosettori finanziari e all'interno di ognuno di essi per quanto riguarda il livello di preparazione delle entità finanziarie in materia di cibersicurezza, i test dovrebbero comprendere un'ampia varietà di strumenti e azioni, dalla valutazione dei requisiti di base (ad esempio valutazione e scansione delle vulnerabilità, analisi open source, valutazioni della sicurezza delle reti, analisi delle lacune, esami della sicurezza fisica, questionari e soluzioni di scansione del software, esami del codice sorgente ove possibile, e test basati su scenari, test di compatibilità, test di prestazione o test end-to-end) fino a test più avanzati tramite TLPT. Tali test avanzati dovrebbero essere richiesti solo per le entità finanziarie che, nell'ambito delle TIC, hanno raggiunto la maturità sufficiente per svolgerli in modo ragionevole. I test di resilienza operativa digitale previsti dal presente regolamento dovrebbero essere pertanto più impegnativi per le entità finanziarie che soddisfano i criteri di cui al presente regolamento (ad esempio, enti creditizi grandi, sistemici e maturi a livello di TIC, le sedi di negoziazione, i depositari centrali di titoli e le controparti centrali ecc.) rispetto alle altre entità finanziarie. Allo stesso tempo i test di resilienza operativa digitale tramite TLPT dovrebbero essere più rilevanti per le entità finanziarie che operano in sottosettori chiave dei servizi finanziari e che assolvono una funzione sistemica (ad esempio pagamenti, attività bancaria, e compensazione e regolamento) e meno rilevanti per altri sottosettori (ad esempio gestori di patrimoni e agenzie di rating del credito).
- (57) Le entità finanziarie coinvolte in attività transfrontaliere e che esercitano la libertà di stabilimento o la libera fornitura di servizi all'interno dell'Unione dovrebbero rispettare gli obblighi di un unico quadro di riferimento per i test avanzati (ossia i TLPT) nel proprio Stato membro di origine; tali test dovrebbero comprendere le infrastrutture delle TIC di tutte le giurisdizioni in cui il gruppo finanziario transfrontaliero opera all'interno dell'Unione, permettendo a tali gruppi finanziari transfrontalieri di sostenere i costi dei test connessi alle TIC in un'unica giurisdizione.
- (58) Per avvalersi delle competenze già acquisite da talune autorità competenti, in particolare per quanto riguarda l'attuazione del quadro di riferimento TIBER-EU, il presente regolamento dovrebbe consentire agli Stati membri di designare un'autorità pubblica unica responsabile nel settore finanziario, a livello nazionale, per tutte le questioni relative ai TLPT, o alle autorità competenti, in assenza di tale designazione, di delegare l'esercizio dei compiti connessi ai TLPT a un'altra autorità finanziaria nazionale competente.
- (59) Poiché il presente regolamento non impone alle entità finanziarie di coprire tutte le funzioni essenziali o importanti in un unico TLPT, le entità finanziarie dovrebbero essere libere di determinare quali e quante funzioni essenziali o importanti dovrebbero essere incluse nell'ambito di applicazione di tale test.
- (60) I test congiunti ai sensi del presente regolamento - che comportano la partecipazione di diverse entità finanziarie a un TLPT e per cui un fornitore terzo di servizi TIC può direttamente stipulare accordi contrattuali con un soggetto incaricato dello svolgimento dei test esterno — dovrebbero essere ammessi solo qualora ci si attenda ragionevolmente che la qualità o la sicurezza dei servizi prestati dal fornitore terzo di servizi TIC a clienti che sono entità non rientranti nell'ambito di applicazione del presente regolamento, o la riservatezza dei dati relativi a tali servizi, subiscano ripercussioni negative. I test congiunti dovrebbero inoltre essere soggetti a garanzie (direzioni da parte di un'entità finanziaria designata, calibrazione del numero di entità finanziarie partecipanti), al fine di assicurare un rigoroso esercizio di test per le entità finanziarie coinvolte che soddisfano gli obiettivi del TLPT conformemente al presente regolamento.

- (61) Allo scopo di sfruttare le risorse interne disponibili a livello aziendale, il presente regolamento dovrebbe consentire il ricorso a soggetto incaricato dello svolgimento dei test interni ai fini dell'esecuzione del TLPT, a condizione che vi sia l'approvazione da parte delle autorità di vigilanza, che non vi sia alcun conflitto d'interessi e che vi sia un'alternanza periodica nel ricorso a soggetto incaricato dello svolgimento dei test interni ed esterni (ogni tre test), imponendo nel contempo che il fornitore di analisi delle minacce nel TLPT sia sempre esterno all'entità finanziaria. La responsabilità di condurre il TLPT dovrebbe rimanere interamente a carico dell'entità finanziaria. Le attestazioni fornite dalle autorità dovrebbero essere finalizzate esclusivamente al riconoscimento reciproco e non dovrebbero precludere eventuali azioni di follow-up necessarie per affrontare i rischi informatici a cui l'entità finanziaria è esposta, né dovrebbero essere considerati un avallo da parte delle autorità di vigilanza delle capacità di gestione e attenuazione dei rischi informatici di un'entità finanziaria.
- (62) Per un solido monitoraggio dei rischi informatici derivanti da terzi nel settore finanziario, è necessario stabilire una serie di norme basate su principi che guidino le entità finanziarie nel monitoraggio dei rischi che si presentano nel contesto di funzioni esternalizzate a fornitori terzi di servizi TIC, in particolare per i servizi TIC a supporto di funzioni essenziali o importanti, nonché più in generale nel contesto di tutte le dipendenze da terzi nel settore delle TIC.
- (63) Per far fronte alla complessità delle varie fonti di rischi informatici, tenendo conto nel contempo della molteplicità e della diversità dei fornitori di soluzioni tecnologiche che consentono un'agevole fornitura di servizi finanziari, il presente regolamento dovrebbe applicarsi a un'ampia gamma di fornitori terzi di servizi TIC, compresi i fornitori di servizi di cloud computing, software, servizi di analisi dei dati e i fornitori di servizi di centri di elaborazione dati. Analogamente, poiché le entità finanziarie dovrebbero individuare e gestire in modo efficace e coerente tutti i tipi di rischio, anche nel contesto dei servizi TIC acquisiti all'interno di un gruppo finanziario, è opportuno chiarire che le imprese appartenenti a un gruppo finanziario e che forniscono servizi TIC prevalentemente alla loro impresa madre o a imprese figlie o succursali della loro impresa madre, nonché le entità finanziarie che forniscono servizi TIC ad altre entità finanziarie, dovrebbero essere considerate anch'esse fornitori terzi di servizi TIC ai sensi del presente regolamento. Infine, alla luce dell'evoluzione del mercato dei servizi di pagamento, sempre più dipendente da soluzioni tecniche complesse, e in vista delle tipologie emergenti di servizi di pagamento e di soluzioni connesse ai pagamenti, anche i partecipanti all'ecosistema dei servizi di pagamento, che prestano attività di trattamento dei pagamenti o gestiscono infrastrutture di pagamento, dovrebbero essere considerati fornitori terzi di servizi TIC ai sensi del presente regolamento, ad eccezione delle banche centrali quando gestiscono sistemi di pagamento o di regolamento titoli e delle autorità pubbliche quando forniscono servizi connessi alle TIC nel contesto dell'espletamento di funzioni di Stato.
- (64) Un'entità finanziaria dovrebbe rimanere sempre responsabile del rispetto dei propri obblighi previsti dal presente regolamento. Le entità finanziarie dovrebbero svolgere il monitoraggio dei rischi emergenti a livello di fornitori terzi di servizi TIC secondo un approccio basato sulla proporzionalità, tenendo debitamente conto della natura, della portata, della complessità e della rilevanza delle loro dipendenze dai servizi 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.
- (65) Lo svolgimento di tale monitoraggio dovrebbe seguire un approccio strategico ai rischi informatici derivanti da terzi, formalizzato con l'adozione, da parte dell'organo di gestione dell'entità finanziaria, di una strategia dedicata per i rischi informatici derivanti da terzi 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 ai lavori nel contesto del quadro di sorveglianza istituito dal presente regolamento, tutte le entità finanziarie dovrebbero essere obbligate a tenere un registro delle informazioni contenente tutti gli accordi contrattuali sull'uso dei servizi TIC prestati da fornitori terzi di servizi TIC. Le autorità di vigilanza finanziaria dovrebbero avere la possibilità di richiedere il registro completo o chiedere sezioni specifiche dello stesso, ottenendo in tal modo informazioni essenziali per acquisire una più ampia comprensione delle dipendenze delle entità finanziarie in materia di TIC.
- (66) Una meticolosa analisi precontrattuale dovrebbe precedere la conclusione formale degli accordi contrattuali e costituirne la base, in particolare concentrandosi su elementi quali la criticità o l'importanza dei servizi sostenuti dal contratto sulle TIC previsto, le necessarie approvazioni da parte delle autorità di vigilanza o altre condizioni, il possibile rischio di concentrazione che ne deriva, nonché applicando la dovuta diligenza nel processo di selezione e valutazione dei fornitori terzi di servizi TIC e valutando i potenziali conflitti d'interessi. Per gli accordi contrattuali riguardanti funzioni essenziali o importanti, le entità finanziarie dovrebbero prendere in considerazione l'utilizzo da parte dei fornitori terzi di servizi TIC degli standard più aggiornati ed elevati in materia di sicurezza delle informazioni. La risoluzione degli accordi contrattuali potrebbe giustificarsi almeno sulla base di una serie di



circostanze che attestino carenze addebitabili al fornitore terzo di servizi TIC, in particolare rilevanti violazioni di leggi o condizioni contrattuali, circostanze che rivelano una potenziale alterazione dell'esercizio delle funzioni previste negli accordi contrattuali, punti deboli del fornitore terzo di servizi TIC emersi nella sua gestione complessiva dei rischi informatici o circostanze che indicano l'incapacità dell'autorità competente interessata di vigilare efficacemente sull'entità finanziaria.

- (67) Per far fronte all'impatto sistemico del rischio di concentrazione di servizi TIC forniti da terzi, il presente regolamento promuove una soluzione equilibrata tramite l'assunzione di un approccio flessibile e graduale verso tale rischio di concentrazione, in quanto l'imposizione di massimali rigidi o restrizioni rigorose potrebbe intralciare lo svolgimento dell'attività economica e limitare la libertà contrattuale. Le entità finanziarie dovrebbero valutare meticolosamente le disposizioni contrattuali previste per verificare la probabilità che tali rischi si presentino, anche mediante analisi approfondite degli accordi di subappalto, soprattutto quando siano conclusi con fornitori terzi di servizi TIC stabiliti in un paese terzo. In questa fase, e allo scopo di trovare il giusto equilibrio tra l'imperativo di preservare la libertà contrattuale e quello di garantire la stabilità finanziaria, non si considera opportuno prevedere norme su massimali e limiti rigorosi alle esposizioni verso terzi nel settore delle TIC. Nel contesto del quadro di sorveglianza, un'autorità di sorveglianza capofila nominata ai sensi del presente regolamento, dovrebbe, rispetto a fornitori terzi critici di servizi TIC, accertarsi con particolare cura di comprendere a fondo le dimensioni delle interdipendenze, di scoprire i casi specifici in cui un elevato grado di concentrazione di fornitori terzi critici di servizi TIC nell'Unione potrebbe compromettere l'integrità e la stabilità del sistema finanziario dell'Unione e di mantenere un dialogo con i fornitori terzi critici di servizi TIC laddove tale rischio specifico sia identificato.
- (68) Per valutare e monitorare costantemente la capacità del fornitore terzo di servizi TIC di erogare in sicurezza i servizi all'entità finanziaria senza effetti avversi sulla resilienza operativa digitale di quest'ultima, è opportuno armonizzare diversi elementi contrattuali chiave con i fornitori terzi di servizi TIC. Tale armonizzazione dovrebbe coprire gli ambiti minimi che sono cruciali per consentire un monitoraggio completo, da parte dell'entità finanziaria, dei rischi che potrebbero derivare dal fornitore terzo di servizi TIC, nella prospettiva dell'esigenza dell'entità finanziaria di garantire la propria resilienza digitale, poiché dipendente in larga misura dalla stabilità, dalla funzionalità, dalla disponibilità e dalla sicurezza dei servizi TIC ricevuti.
- (69) In sede di rinegoziazione degli accordi contrattuali al fine di perseguire la conformità con i requisiti del presente regolamento, le entità finanziarie e i fornitori terzi di servizi TIC dovrebbero garantire la copertura delle principali disposizioni contrattuali di cui al presente regolamento.
- (70) La definizione di «funzione essenziale o importante» di cui al presente regolamento comprende le «funzioni essenziali» definite all'articolo 2, paragrafo 1, punto 35), della direttiva 2014/59/UE del Parlamento europeo e del Consiglio <sup>(20)</sup>. Di conseguenza, le funzioni ritenute essenziali ai sensi della direttiva 2014/59/UE sono incluse nella definizione di funzioni essenziali ai sensi del presente regolamento.
- (71) Indipendentemente dall'essenzialità o dall'importanza della funzione supportata dai servizi TIC, gli accordi contrattuali dovrebbero, in particolare, contenere le descrizioni complete di funzioni e servizi, l'indicazione delle località in cui si esercitano tali funzioni e deve aver luogo il trattamento dei dati nonché le descrizioni dei livelli di servizio. Altri elementi essenziali per consentire il monitoraggio, da parte di un'entità finanziaria, dei rischi informatici derivanti da terzi sono: disposizioni contrattuali che specificano in che modo il fornitore terzo di servizi TIC garantisce l'accessibilità, la disponibilità, l'integrità, la sicurezza e la protezione dei dati personali; disposizioni che stabiliscono le pertinenti garanzie per consentire l'accesso, il ripristino e la restituzione dei dati in caso di insolvenza, risoluzione o cessazione dell'operatività del fornitore terzo di servizi TIC, nonché disposizioni che impongono al fornitore terzo di servizi TIC di prestare assistenza in caso di incidenti connessi alle TIC in relazione ai servizi forniti, senza costi supplementari oppure a un costo stabilito ex ante; disposizioni sull'obbligo per il

<sup>(20)</sup> Direttiva 2014/59/UE del Parlamento europeo e del Consiglio, del 15 maggio 2014, che istituisce un quadro di risanamento e risoluzione degli enti creditizi e delle imprese di investimento e che modifica la direttiva 82/891/CEE del Consiglio, e le direttive 2001/24/CE, 2002/47/CE, 2004/25/CE, 2005/56/CE, 2007/36/CE, 2011/35/UE, 2012/30/UE e 2013/36/UE e i regolamenti (UE) n. 1093/2010 e (UE) n. 648/2012, del Parlamento europeo e del Consiglio (GU L 173 del 12.6.2014, pag. 190).

fornitore terzo di servizi TIC di cooperare senza riserve con le autorità competenti e con le autorità di risoluzione dell'entità finanziaria; e disposizioni sui diritti di risoluzione e sui relativi termini minimi di preavviso per la risoluzione degli accordi contrattuali, conformemente alle attese delle autorità competenti e delle autorità di risoluzione.

- (72) In aggiunta a tali disposizioni contrattuali e al fine di garantire che le entità finanziarie mantengano il pieno controllo di tutti gli sviluppi a livello di soggetti terzi che potrebbero comprometterne la sicurezza delle TIC, i contratti per la fornitura di servizi TIC a supporto di funzioni essenziali o importanti dovrebbero altresì prevedere quanto segue: le descrizioni complete dei livelli di servizio, con precisi obiettivi quantitativi e qualitativi, in termini di prestazioni, in modo da consentire l'applicazione, senza indebito ritardo, di opportune azioni correttive qualora i livelli di servizio concordati non siano rispettati; i pertinenti termini di preavviso e obblighi di segnalazione per il fornitore terzo di servizi TIC nel caso di sviluppi che possano incidere seriamente sulla capacità di tale fornitore di fornire efficacemente i rispettivi servizi TIC; l'obbligo per il fornitore terzo di servizi TIC di attuare e testare i piani operativi d'emergenza e di disporre di misure, strumenti e politiche per la sicurezza delle TIC che consentano la fornitura sicura dei servizi, nonché di partecipare e di cooperare pienamente al TLPT svolto dall'entità finanziaria.
- (73) I contratti per la fornitura di servizi TIC a supporto di funzioni essenziali o importanti dovrebbero altresì contenere disposizioni che consentano i diritti di accesso, ispezione e audit da parte dell'entità finanziaria o di un soggetto terzo designato, nonché il diritto di ottenere copia, quali strumenti fondamentali per il monitoraggio costante, da parte delle entità finanziarie, delle prestazioni del fornitore terzo di servizi TIC, insieme alla piena collaborazione di quest'ultimo nel corso delle ispezioni. Analogamente, l'autorità competente dell'entità finanziaria dovrebbe poter godere del diritto, sulla base di preavvisi, di ispezionare e sottoporre a verifiche di audit il fornitore terzo di servizi TIC, fatta salva la protezione delle informazioni riservate.
- (74) Tali accordi contrattuali dovrebbero inoltre prevedere strategie di uscita dedicate che consentano in particolare periodi di transizione obbligatori durante i quali i fornitori terzi di servizi TIC dovrebbero continuare a prestare i pertinenti servizi, allo scopo di ridurre il rischio di perturbazioni a livello dell'entità finanziaria o di consentire a quest'ultima di passare senza inconvenienti all'utilizzo di altri fornitori terzi di servizi TIC o, in alternativa, di adottare soluzioni interne, in funzione della complessità del servizio TIC fornito. Inoltre, le entità finanziarie che rientrano nell'ambito di applicazione della direttiva 2014/59/UE dovrebbero garantire che i pertinenti contratti per i servizi TIC siano solidi e pienamente applicabili in caso di risoluzione di tali entità finanziarie. In linea con le aspettative delle autorità di risoluzione, tali entità finanziarie dovrebbero pertanto garantire che i pertinenti contratti di servizi TIC siano resilienti in caso di risoluzione. Finché continuano a rispettare i loro obblighi di pagamento, tali entità finanziarie dovrebbero garantire, tra gli altri requisiti, che i pertinenti contratti per i servizi TIC contengano clausole di non risoluzione, di non sospensione e di immodificabilità in caso di ristrutturazione o risoluzione.
- (75) Inoltre, l'utilizzo volontario di clausole contrattuali standard elaborate da autorità pubbliche o istituzioni dell'Unione, in particolare l'utilizzo di clausole contrattuali elaborate dalla Commissione per i servizi di cloud computing, potrebbe costituire un'ulteriore preziosa risorsa per le entità finanziarie e per i fornitori terzi di servizi TIC, accrescendo il loro livello di certezza del diritto in merito all'utilizzo di servizi di cloud computing nel settore finanziario, in completa conformità con i requisiti e le aspettative definiti dalla normativa dell'Unione in materia di servizi finanziari. L'elaborazione di clausole contrattuali standard 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 standard 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.
- (76) Per promuovere la convergenza e l'efficienza negli approcci di vigilanza quando si affrontano rischi relativi alle TIC derivanti da terzi nel settore finanziario, nonché per rafforzare la resilienza operativa digitale delle entità finanziarie che dipendono da fornitori terzi critici di servizi TIC per la fornitura di servizi TIC che sostengono la fornitura dei servizi finanziari e contribuire così a preservare la stabilità del sistema finanziario dell'Unione e l'integrità del mercato interno per i servizi finanziari, è opportuno assoggettare i fornitori terzi critici di servizi TIC a un quadro di sorveglianza dell'Unione. Sebbene l'istituzione del quadro di sorveglianza sia giustificata dal valore aggiunto di un'azione intrapresa a livello dell'Unione e in virtù del ruolo intrinseco e delle specificità dell'utilizzo dei servizi TIC

nella fornitura di servizi finanziari, è opportuno ricordare, nel contempo, che tale soluzione appare adeguata solo nel contesto del presente regolamento, che tratta specificamente della resilienza operativa digitale nel settore finanziario. Tuttavia, tale quadro di sorveglianza non dovrebbe essere considerato un nuovo modello di vigilanza dell'Unione in altri settori delle attività e dei servizi finanziari.

- (77) Il quadro di sorveglianza dovrebbe applicarsi solo ai fornitori terzi critici di servizi TIC. Dovrebbe pertanto esserci un meccanismo di designazione, in modo da tenere conto della dimensione e della natura della dipendenza del settore finanziario da tali fornitori terzi di servizi TIC. Tale meccanismo dovrebbe comportare una serie di criteri quantitativi e qualitativi per fissare i parametri di criticità come base per l'inclusione nel quadro di sorveglianza. Al fine di garantire l'accuratezza di tale valutazione, e indipendentemente dalla struttura aziendale del fornitore terzo di servizi TIC, tali criteri, nel caso di un fornitore terzo di servizi TIC appartenente a un gruppo più ampio, dovrebbero prendere in considerazione l'intera struttura del gruppo del fornitore terzo di servizi TIC. Da un lato, i fornitori terzi critici di servizi TIC, che non sono designati automaticamente in virtù dell'applicazione di tali criteri, dovrebbero avere la possibilità di aderire al quadro di sorveglianza su base volontaria; dall'altro, i fornitori terzi di servizi TIC, che sono già soggetti ai quadri dei meccanismi di sorveglianza che sostengono l'assolvimento dei compiti del Sistema europeo di banche centrali di cui all'articolo 127, paragrafo 2, TFUE, dovrebbero esserne esentati.
- (78) Analogamente, anche le entità finanziarie che forniscono servizi TIC ad altre entità finanziarie, pur appartenendo alla categoria dei fornitori terzi di servizi TIC ai sensi del presente regolamento, dovrebbero essere esentate dal quadro di sorveglianza in quanto già soggette ai meccanismi di vigilanza istituiti dalla pertinente normativa dell'Unione in materia di servizi finanziari. Ove applicabile, le autorità competenti dovrebbero tenere conto, nell'ambito delle loro attività di vigilanza, dei rischi informatici posti alle entità finanziarie dalle entità finanziarie che forniscono servizi TIC. Allo stesso modo, a causa degli attuali meccanismi di monitoraggio dei rischi a livello di gruppo, la stessa esenzione dovrebbe essere introdotta per i fornitori terzi di servizi TIC che prestano servizi prevalentemente alle entità del loro stesso gruppo. Anche i fornitori terzi di servizi TIC che prestano servizi TIC unicamente in uno Stato membro a entità finanziarie attive solo in tale Stato membro dovrebbero essere esentati dal meccanismo di designazione a causa delle loro attività limitate e della mancanza di impatto transfrontaliero.
- (79) La trasformazione digitale che interessa i servizi finanziari ha portato a un livello senza precedenti di utilizzo dei servizi TIC e di dipendenza da essi. Poiché è divenuto inconcepibile fornire servizi finanziari senza l'utilizzo di servizi di cloud computing, soluzioni software e servizi connessi ai dati, l'ecosistema finanziario dell'Unione è diventato intrinsecamente codipendente da taluni servizi TIC prestati dai fornitori di servizi TIC. Alcuni di questi fornitori, innovatori nello sviluppo e nell'applicazione di tecnologie basate sulle TIC, svolgono un ruolo significativo nella fornitura di servizi finanziari, o sono diventati parte integrante della catena del valore dei servizi finanziari. Sono quindi divenuti fondamentali per la stabilità e l'integrità del sistema finanziario dell'Unione. Questa diffusa dipendenza dai servizi prestati da fornitori terzi critici di servizi TIC, unitamente all'interdipendenza dei sistemi informativi di vari operatori di mercato, crea un rischio diretto, e potenzialmente grave, per il sistema dei servizi finanziari dell'Unione e per la continuità della fornitura di servizi finanziari, qualora i fornitori terzi critici di servizi TIC fossero colpiti da perturbazioni operative o gravi incidenti informatici. Gli incidenti informatici hanno la capacità distintiva di moltiplicarsi e propagarsi in tutto il sistema finanziario a un ritmo notevolmente più rapido rispetto ad altri tipi di rischi monitorati nel settore finanziario e possono estendersi a tutti i settori e oltre i confini geografici. Sono potenzialmente in grado di evolvere verso una crisi sistemica, in cui la fiducia nel sistema finanziario si è erosa a causa dell'interruzione delle funzioni che sostengono l'economia reale, o di ingenti perdite finanziarie, raggiungendo un livello che il sistema finanziario non è in grado di sopportare, o che richiede la messa a punto di pesanti misure di assorbimento degli shock. Per evitare che tali scenari si verifichino e compromettano in tal modo la stabilità finanziaria e l'integrità dell'Unione, è essenziale assicurare la convergenza delle pratiche di vigilanza connesse ai rischi informatici derivanti da terzi nella finanza, in particolare attraverso nuove norme che consentano la sorveglianza da parte dell'Unione dei fornitori terzi critici di servizi TIC.

- (80) Il quadro di sorveglianza dipende in larga misura dal grado di collaborazione tra l'autorità di sorveglianza capofila e il fornitore terzo critico di servizi TIC che presta alle entità finanziarie servizi che incidono sulla fornitura di servizi finanziari. Una sorveglianza efficace si basa, tra l'altro, sulla capacità dell'autorità di sorveglianza capofila di svolgere efficacemente missioni di monitoraggio e ispezioni per valutare le norme, i controlli e i processi utilizzati dai fornitori terzi critici di servizi TIC, nonché per valutare il potenziale impatto cumulativo delle loro attività sulla stabilità finanziaria e sull'integrità del sistema finanziario. Allo stesso tempo, è fondamentale che i fornitori terzi critici di servizi TIC seguano le raccomandazioni dell'autorità di sorveglianza capofila e rispondano alle sue preoccupazioni. Poiché la mancanza di cooperazione da parte di un fornitore terzo di servizi TIC critico che fornisce servizi che incidono sulla fornitura di servizi finanziari, come il rifiuto di concedere l'accesso ai propri locali o di trasmettere informazioni, priverebbe in ultima analisi l'autorità di sorveglianza capofila dei suoi strumenti essenziali per valutare i rischi informatici derivanti da terzi e potrebbe incidere negativamente sulla stabilità finanziaria e sull'integrità del sistema finanziario, occorre prevedere anche un regime sanzionatorio commisurato.
- (81) In tale contesto, la necessità dell'autorità di sorveglianza capofila di imporre penalità di mora per obbligare i fornitori terzi critici di servizi TIC a rispettare gli obblighi in materia di trasparenza e accesso di cui al presente regolamento non dovrebbe essere messa a repentaglio dalle difficoltà derivanti dall'applicazione di tali penalità di mora in relazione a fornitori terzi critici di servizi TIC stabiliti in paesi terzi. Al fine di garantire l'applicabilità di tali penalità e consentire una rapida introduzione delle procedure a tutela dei diritti della difesa dei fornitori terzi critici di servizi TIC nel contesto del meccanismo di designazione e della formulazione di raccomandazioni, tali fornitori terzi critici di servizi TIC che forniscono alle entità finanziarie servizi che incidono sulla fornitura di servizi finanziari dovrebbero essere tenuti a mantenere un'adeguata presenza commerciale nell'Unione. Data la natura della sorveglianza e l'assenza di accordi comparabili in altre giurisdizioni, non esistono meccanismi alternativi adeguati che garantiscano tale obiettivo mediante una cooperazione efficace con le autorità di vigilanza finanziaria nei paesi terzi in relazione al monitoraggio dell'impatto dei rischi operativi digitali posti dai fornitori terzi di servizi TIC sistemici, che rientrano nella designazione di fornitori terzi critici di servizi TIC stabiliti in paesi terzi. Pertanto, onde continuare a fornire servizi TIC a entità finanziarie nell'Unione, un fornitore terzo di servizi TIC stabilito in un paese terzo che sia stato designato come critico a norma del presente regolamento dovrebbe stipulare, entro 12 mesi da tale designazione, tutti gli accordi necessari per garantire la propria integrazione nell'Unione, mediante l'istituzione di un'impresa figlia, quale definita nell'acquis dell'Unione, segnatamente nella direttiva 2013/34/UE del Parlamento europeo e del Consiglio <sup>(21)</sup>.
- (82) L'obbligo di istituire un'impresa figlia nell'Unione non dovrebbe impedire al fornitore terzo critico di servizi TIC di prestare servizi TIC e il relativo sostegno tecnico da impianti e infrastrutture situati al di fuori dell'Unione. Il presente regolamento non impone un obbligo di localizzazione dei dati poiché non impone di conservare o trattare i dati nell'Unione.
- (83) I fornitori terzi critici di servizi TIC dovrebbero essere in grado di fornire servizi TIC da ovunque nel mondo, non necessariamente o non solo da locali situati nell'Unione. Le attività di sorveglianza dovrebbero essere svolte in primo luogo in locali situati nell'Unione e interagendo con soggetti situati nell'Unione, comprese le imprese figlie istituite da fornitori terzi critici di servizi TIC a norma del presente regolamento. Tuttavia, tali azioni all'interno dell'Unione potrebbero essere insufficienti per consentire all'autorità di sorveglianza capofila di svolgere pienamente ed efficacemente i propri compiti ai sensi del presente regolamento. L'autorità di sorveglianza capofila dovrebbe pertanto essere in grado di esercitare i pertinenti poteri di sorveglianza anche nei paesi terzi. L'esercizio di tali poteri nei paesi terzi dovrebbe consentire all'autorità di sorveglianza capofila di esaminare le strutture dalle quali i servizi TIC o di assistenza tecnica sono effettivamente forniti o gestiti dal fornitore terzo critico di servizi TIC, e dovrebbe fornire all'autorità di sorveglianza capofila una comprensione completa e operativa della gestione dei rischi informatici da parte del fornitore terzo critico di servizi TIC. La possibilità per l'autorità di sorveglianza capofila, in quanto agenzia dell'Unione, di esercitare poteri al di fuori del territorio dell'Unione dovrebbe essere debitamente inquadrata da condizioni pertinenti, in particolare il consenso del fornitore terzo critico di servizi TIC interessato. Analogamente, le autorità pertinenti del paese terzo dovrebbero essere informate dell'esercizio nel proprio territorio delle attività dell'autorità di sorveglianza capofila e non essersi opposte. Tuttavia, al fine di garantire un'attuazione efficace e fatte salve le rispettive competenze delle istituzioni dell'Unione e degli Stati membri, tali poteri devono

<sup>(21)</sup> Direttiva 2013/34/UE del Parlamento europeo e del Consiglio, del 26 giugno 2013, relativa ai bilanci d'esercizio, ai bilanci consolidati e alle relative relazioni di talune tipologie di imprese, recante modifica della direttiva 2006/43/CE del Parlamento europeo e del Consiglio e abrogazione delle direttive 78/660/CEE e 83/349/CEE del Consiglio (GU L 182 del 29.6.2013, pag. 19).

altresì essere pienamente basati sulla conclusione di accordi di cooperazione amministrativa con le autorità pertinenti del paese terzo interessato. Il presente regolamento dovrebbe pertanto consentire alle AEV di concludere accordi di cooperazione amministrativa con le autorità pertinenti dei paesi terzi, che non dovrebbero altrimenti generare obblighi giuridici in capo all'Unione e ai suoi Stati membri.

- (84) Per facilitare la comunicazione con l'autorità di sorveglianza capofila e garantire un'adeguata rappresentanza, i fornitori terzi critici di servizi TIC che fanno parte di un gruppo dovrebbero designare una persona giuridica come punto di coordinamento.
- (85) Il quadro di sorveglianza non dovrebbe pregiudicare la competenza degli Stati membri per quanto attiene allo svolgimento di proprie missioni di sorveglianza o di monitoraggio nei confronti di fornitori terzi di servizi TIC che non sono designati come critici ai sensi del presente regolamento ma sono considerati importanti a livello nazionale.
- (86) Per sfruttare l'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 informatici, conformemente ai propri compiti in materia di cibersicurezza. Dovrebbe essere coadiuvato da un nuovo sottocomitato (forum di sorveglianza) che dovrebbe svolgere il lavoro preparatorio, sia per le singole decisioni rivolte a fornitori terzi critici di servizi TIC, sia per la formulazione di raccomandazioni collettive, relative in particolare all'analisi comparativa dei programmi di sorveglianza per i fornitori terzi critici di servizi TIC, nonché all'identificazione delle migliori prassi riguardanti il rischio di concentrazione delle TIC.
- (87) Per far sì che i fornitori terzi critici di servizi TIC siano soggetti a una sorveglianza adeguata ed efficace a livello dell'Unione, il presente regolamento prevede che una qualunque delle tre AEV possa essere designata come autorità di sorveglianza capofila. L'assegnazione individuale di un fornitore terzo critico di servizi TIC a una delle tre AEV dovrebbe essere fondata su una valutazione della prevalenza delle entità finanziarie che operano nei settori finanziari per i quali tale AEV è competente. Tale approccio dovrebbe portare a una ripartizione equilibrata dei compiti e delle responsabilità tra le tre AEV, nel contesto dell'esercizio delle funzioni di sorveglianza, e dovrebbe utilizzare al meglio le risorse umane e le competenze tecniche disponibili in ciascuna delle tre AEV.
- (88) Alle autorità di sorveglianza capofila dovrebbero essere attribuiti i poteri necessari per condurre indagini, effettuare ispezioni in fuori sede o presso i locali e le sedi dei fornitori terzi critici di servizi TIC e ottenere informazioni complete e aggiornate. Tali poteri dovrebbero consentire all'autorità di sorveglianza capofila di acquisire un'immagine realistica del tipo, delle dimensioni e dell'impatto dei rischi informatici derivanti da terzi cui sono esposte le entità finanziarie e, in ultima analisi, il sistema finanziario dell'Unione. Affidare alle AEV il ruolo di sorveglianza principale è un prerequisito per comprendere e affrontare la dimensione sistemica dei rischi informatici nel settore finanziario. L'impatto dei fornitori terzi critici di servizi TIC sul settore finanziario dell'Unione e i problemi causati dal rischio di concentrazione delle TIC che ne possono derivare esigono un approccio collettivo a livello dell'UE. L'esecuzione contestuale di molteplici audit e diritti di accesso, effettuata separatamente da varie autorità competenti, con un coordinamento scarso o nullo tra di esse, impedirebbe alle autorità di vigilanza finanziaria di ottenere un quadro completo ed esaustivo dei rischi informatici derivanti da terzi nell'Unione, e provocherebbe anzi sovrapposizioni, oneri e complessità per i fornitori terzi critici di servizi TIC qualora fossero soggetti a un gran numero di richieste di monitoraggio e ispezione.
- (89) A causa dell'impatto significativo del fatto di essere designati come critici, il presente regolamento dovrebbe garantire che i diritti dei fornitori terzi critici di servizi TIC siano preservati in tutte le fasi di attuazione del quadro di sorveglianza. Prima di essere designati come critici, tali fornitori dovrebbero, ad esempio, avere il diritto di presentare all'autorità di sorveglianza capofila una dichiarazione motivata contenente tutte le informazioni pertinenti ai fini della valutazione relativa alla loro designazione. Dal momento che all'autorità di sorveglianza capofila dovrebbe essere conferito il potere di presentare raccomandazioni su questioni concernenti i rischi informatici e sui rimedi idonei, ivi compreso il potere di opporsi a determinate disposizioni contrattuali suscettibili in ultima analisi di incidere sulla stabilità dell'entità finanziaria o del sistema finanziario, prima di finalizzare tali raccomandazioni i fornitori terzi critici di servizi TIC dovrebbero altresì avere l'opportunità di fornire spiegazioni riguardo all'impatto previsto delle soluzioni, proposte nelle raccomandazioni, sui clienti che sono entità non

rientranti nell'ambito di applicazione del presente regolamento, formulando soluzioni per attenuare i rischi. I fornitori terzi critici di servizi TIC in disaccordo con le raccomandazioni dovrebbero presentare una spiegazione motivata della loro intenzione di non uniformarsi alla raccomandazione. Se tale spiegazione motivata non è presentata o è ritenuta insufficiente, l'autorità di sorveglianza capofila dovrebbe pubblicare un avviso pubblico che descriva sommariamente la questione dell'inosservanza.

- (90) Nell'ambito delle loro funzioni relative alla vigilanza prudenziale delle entità finanziarie, le autorità competenti dovrebbero debitamente includere il compito di verificare il rispetto sostanziale delle raccomandazioni formulate dall'autorità di sorveglianza capofila. Le autorità competenti dovrebbero poter imporre alle entità finanziarie di adottare misure supplementari per affrontare i rischi individuati nelle raccomandazioni dell'autorità di sorveglianza capofila e dovrebbero, a tempo debito, pubblicare notifiche a tal fine. Se l'autorità di sorveglianza capofila rivolge raccomandazioni ai fornitori terzi critici di servizi TIC sottoposti a vigilanza ai sensi della direttiva (UE) 2022/2555, le autorità competenti dovrebbero poter consultare, su base volontaria e prima di adottare misure supplementari, le autorità competenti ai sensi di tale direttiva per promuovere un approccio coordinato nei confronti dei fornitori terzi critici di servizi TIC in questione.
- (91) L'esercizio della sorveglianza dovrebbe essere guidato da tre principi operativi volti a garantire: a) uno stretto coordinamento tra le AEV nel loro ruolo di autorità di sorveglianza capofila, attraverso una rete di sorveglianza comune, b) la coerenza con il quadro istituito dalla direttiva (UE) 2022/2555 (attraverso una consultazione volontaria degli organismi ai sensi di tale direttiva per evitare la duplicazione di misure rivolte ai fornitori terzi critici di servizi TIC), e c) l'applicazione della diligenza per ridurre al minimo il rischio potenziale di perturbazione dei servizi forniti dai fornitori terzi critici di servizi TIC ai clienti che sono entità non rientranti nell'ambito di applicazione del presente regolamento.
- (92) Il quadro di sorveglianza non dovrebbe rimpiazzare, né in alcun modo o in alcuna parte sostituirsi, alla prescrizione relativa alla gestione, da parte delle entità finanziarie, dei rischi derivanti dal ricorso a fornitori terzi di servizi TIC, compreso l'obbligo di mantenere un monitoraggio costante degli accordi contrattuali stipulati con fornitori terzi critici di servizi TIC. Analogamente, il quadro di sorveglianza non dovrebbe incidere sulla piena responsabilità delle entità finanziarie per quanto riguarda il rispetto e l'adempimento di tutti gli obblighi di legge previsti dal presente regolamento e dalla pertinente normativa in materia di servizi finanziari.
- (93) Per evitare duplicazioni e sovrapposizioni, è opportuno che le autorità competenti si astengano dall'adozione individuale di misure per il monitoraggio dei rischi derivanti da fornitori terzi critici di servizi TIC; a tale riguardo, esse dovrebbero affidarsi alla pertinente valutazione dell'autorità di sorveglianza capofila. Eventuali misure dovrebbero in ogni caso essere coordinate e concordate preliminarmente con l'autorità di sorveglianza capofila nel contesto dell'esercizio dei compiti del quadro di sorveglianza.
- (94) Per promuovere la convergenza a livello internazionale sull'utilizzo delle migliori prassi per il riesame e il monitoraggio della gestione del rischio digitale derivante da fornitori terzi di servizi TIC, è opportuno incoraggiare le AEV a stipulare accordi di cooperazione con le pertinenti autorità normative e di vigilanza di paesi terzi.
- (95) Per sfruttare utilmente le competenze specifiche, le capacità tecniche e l'esperienza del personale specializzato nella gestione dei rischi operativi e informatici all'interno delle autorità competenti, le tre AEV e, su base volontaria, le autorità competenti ai sensi della direttiva (UE) 2022/2555 e l'autorità di sorveglianza capofila dovrebbero tener conto delle capacità e conoscenze delle autorità di vigilanza nazionali e istituire gruppi destinati a esaminare i singoli fornitori terzi critici di servizi TIC, riunendo gruppi multidisciplinari che coadiuvino la preparazione e l'attuazione delle attività di sorveglianza, comprese le indagini generali e le ispezioni dei fornitori terzi critici di servizi TIC, nonché l'eventuale seguito necessario da dare a queste attività.
- (96) Mentre i costi derivanti dai compiti di sorveglianza sarebbero interamente finanziati dalle commissioni applicate ai fornitori terzi critici di servizi TIC, è tuttavia probabile che le AEV debbano sostenere, prima dell'avvio del quadro di sorveglianza, costi per l'attuazione di sistemi di TIC dedicati a sostegno dell'imminente sorveglianza, poiché sarebbe necessario sviluppare e attivare in anticipo sistemi di TIC dedicati. Il presente regolamento prevede pertanto un modello di finanziamento ibrido, in base al quale il quadro di sorveglianza sarebbe, in quanto tale, interamente finanziato tramite commissioni, mentre lo sviluppo dei sistemi di TIC delle AEV sarebbe finanziato dai contributi dell'Unione e delle autorità nazionali competenti.

- (97) Al fine di garantire il corretto esercizio dei propri compiti ai sensi del presente regolamento, le autorità competenti dovrebbero detenere tutti i necessari poteri per vigilare, indagare e imporre sanzioni. Esse dovrebbero, in linea di principio, pubblicare avvisi relativi alle sanzioni amministrative che irrogano. Poiché è possibile che entità finanziarie e fornitori terzi di servizi TIC siano stabiliti in Stati membri diversi e siano sottoposti a vigilanza da parte di differenti autorità competenti, è opportuno che l'applicazione del presente regolamento sia agevolata, da una parte, attraverso una stretta cooperazione tra le autorità competenti interessate, compresa la BCE per quanto riguarda i compiti specifici a essa attribuiti dal regolamento (UE) n. 1024/2013 del Consiglio, e, dall'altra, mediante consultazioni con le AEV tramite il reciproco scambio di informazioni e l'offerta di assistenza nel contesto delle attività di vigilanza pertinenti.
- (98) Per quantificare e qualificare ulteriormente i criteri per la designazione di fornitori terzi di servizi TIC come 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 TFUE al fine di integrare il presente regolamento precisando ulteriormente l'impatto sistemico che un guasto o un'indisponibilità operativa presso un fornitore terzo di servizi TIC potrebbe esercitare sulle entità finanziarie cui fornisce servizi TIC, il numero di enti a rilevanza sistemica a livello globale (*global systemically important institutions* — G-SII) o di altri enti a rilevanza sistemica (*other systemically important institutions* — O-SII) che dipendono dal rispettivo fornitore terzo di servizi TIC, il numero di fornitori terzi di servizi TIC attivi su uno specifico mercato, i costi della migrazione di dati e di carichi di lavoro relativi alle TIC ad altri fornitori terzi di servizi TIC, nonché l'importo delle commissioni per le attività di sorveglianza e le relative modalità di pagamento. È di particolare importanza che durante i lavori preparatori la Commissione svolga adeguate consultazioni, anche a livello di esperti, e che tali consultazioni siano condotte nel rispetto dei principi stabiliti nell'accordo interistituzionale «Legiferare meglio» del 13 aprile 2016 <sup>(23)</sup>. In particolare, al fine di garantire la partecipazione su un piede di parità alla preparazione degli atti delegati, il Parlamento europeo e il Consiglio dovrebbero ricevere tutti i documenti contemporaneamente agli esperti degli Stati membri, e i loro esperti dovrebbero avere sistematicamente accesso alle riunioni dei gruppi di esperti della Commissione incaricati della preparazione di tali atti delegati.
- (99) Le norme tecniche di regolamentazione dovrebbero garantire la coerente armonizzazione i requisiti contenuti nel presente regolamento. Nel loro ruolo di organismi con una competenza altamente specializzata, le AEV dovrebbero elaborare progetti di norme tecniche di regolamentazione che non comportino scelte politiche e presentarli alla Commissione. È opportuno elaborare norme tecniche di regolamentazione nei settori della gestione dei rischi informatici, della segnalazione di incidenti gravi connessi alle TIC e dei test, nonché per quanto riguarda i requisiti principali per un solido monitoraggio dei rischi informatici derivanti da terzi. La Commissione e le AEV dovrebbero fare in modo che tutte le entità finanziarie possano applicare tali norme e requisiti in misura proporzionata alle loro dimensioni e al loro profilo di rischio complessivo, nonché alla natura, alla portata e alla complessità dei loro servizi, delle loro attività e della loro operatività. Alla Commissione si dovrebbe conferire il potere di adottare tali norme tecniche di regolamentazione mediante atti delegati a norma dell'articolo 290 TFUE e degli articoli da 10 a 14 dei regolamenti (UE) n. 1093/2010, (UE) n. 1094/2010 e (UE) n. 1095/2010.
- (100) Per rendere più agevolmente comparabili le segnalazioni sugli incidenti gravi connessi alle TIC e sui gravi incidenti operativi o relativi alla sicurezza dei pagamenti, nonché per garantire la trasparenza sugli accordi contrattuali per l'utilizzo di servizi TIC offerti da fornitori terzi, le AEV dovrebbero elaborare progetti di norme tecniche di attuazione che introducano modelli, formulari e procedure standardizzati per la segnalazione, da parte delle entità finanziarie, degli incidenti gravi connessi alle TIC e di gravi incidenti operativi o relativi alla sicurezza dei pagamenti, nonché modelli standardizzati per il registro delle informazioni. Al momento di elaborare tali norme, le AEV dovrebbero tenere conto delle dimensioni e del profilo di rischio complessivo dell'entità finanziaria, nonché della natura, della portata e della complessità dei suoi servizi, delle sue attività e delle sue operazioni. È opportuno conferire alla Commissione il potere di adottare tali norme tecniche di attuazione mediante atti di esecuzione a norma dell'articolo 291 TFUE e dell'articolo 15 dei regolamenti (UE) n. 1093/2010, (UE) n. 1094/2010 e (UE) n. 1095/2010.

<sup>(23)</sup> GUL 123 del 12.5.2016, pag. 1.

- (101) 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 nei regolamenti (CE) n. 1060/2009 <sup>(23)</sup>, (UE) n. 648/2012 <sup>(24)</sup>, (UE) n. 600/2014 <sup>(25)</sup> e (UE) n. 909/2014 <sup>(26)</sup> del Parlamento europeo e del Consiglio, è opportuno conferire alle AEV, a livello individuale o collettivo tramite il comitato congiunto, il mandato di sottoporre 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 gestione dei rischi informatici.
- (102) Dal momento che il presente regolamento, assieme alla direttiva (UE) 2022/2556 del Parlamento europeo e del Consiglio <sup>(27)</sup>, comporta il consolidamento delle disposizioni per la gestione dei rischi informatici 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 e il regolamento (UE) 2016/1011 <sup>(28)</sup> del Parlamento europeo e del Consiglio, per garantire completa coerenza è opportuno modificare tali regolamenti per precisare che le disposizioni applicabili in materia di rischi informatici sono stabilite nel presente regolamento.
- (103) È pertanto opportuno limitare l'ambito di applicazione dei pertinenti articoli relativi al rischio operativo, in base ai quali nei regolamenti (CE) n. 1060/2009, (UE) n. 648/2012, (UE) n. 600/2014, (UE) n. 909/2014 e (UE) 2016/1011 era stato conferito il mandato di adottare atti delegati e di esecuzione, allo scopo di riprendere nel presente regolamento tutte le disposizioni sugli aspetti relativi alla resilienza operativa digitale che oggi fanno parte di quei regolamenti.
- (104) Il potenziale rischio informatico sistemico connesso all'utilizzo delle infrastrutture di TIC che consentono il funzionamento dei sistemi di pagamento e la prestazione di attività di trattamento dei pagamenti dovrebbe essere debitamente affrontato a livello dell'Unione attraverso norme armonizzate in materia di resilienza digitale. A tal fine, la Commissione dovrebbe valutare rapidamente la necessità di rivedere l'ambito di applicazione del presente regolamento allineando nel contempo tale revisione all'esito del riesame complessivo previsto dalla direttiva (UE) 2015/2366. Numerosi attacchi su vasta scala verificatisi nel corso dell'ultimo decennio dimostrano che i sistemi di pagamento sono diventati esposti alle minacce informatiche. Collocati al centro della catena dei servizi di pagamento e caratterizzati da forti interconnessioni con l'intero sistema finanziario, i sistemi di pagamento e le attività di trattamento dei pagamenti hanno acquisito un'importanza cruciale per il funzionamento dei mercati finanziari dell'Unione. Gli attacchi informatici contro tali sistemi possono causare gravi perturbazioni delle attività a livello operativo, con ripercussioni dirette su funzioni economiche fondamentali, quali l'agevolazione dei pagamenti, e effetti indiretti sui relativi processi economici. Fino all'istituzione a livello dell'Unione di un regime armonizzato e della supervisione degli operatori dei sistemi di pagamento e dei soggetti incaricati del trattamento delle operazioni, gli Stati membri possono, al fine di applicare pratiche di mercato analoghe, trarre ispirazione dai requisiti in materia di resilienza operativa digitale stabiliti dal presente regolamento nell'applicare le norme nei confronti degli operatori di sistemi di pagamento e dei soggetti incaricati del trattamento delle operazioni sottoposti a vigilanza nelle rispettive giurisdizioni.
- 
- <sup>(23)</sup> Regolamento (CE) n. 1060/2009 del Parlamento europeo e del Consiglio, del 16 settembre 2009, relativo alle agenzie di rating del credito (GU L 302 del 17.11.2009, pag. 1).
- <sup>(24)</sup> Regolamento (UE) n. 648/2012 del Parlamento europeo e del Consiglio, del 4 luglio 2012, sugli strumenti derivati OTC, le controparti centrali e i repertori di dati sulle negoziazioni (GU L 201 del 27.7.2012, pag. 1).
- <sup>(25)</sup> Regolamento (UE) n. 600/2014 del Parlamento europeo e del Consiglio, del 15 maggio 2014, sui mercati degli strumenti finanziari e che modifica il regolamento (UE) n. 648/2012 (GU L 173 del 12.6.2014, pag. 84).
- <sup>(26)</sup> Regolamento (UE) n. 909/2014 del Parlamento europeo e del Consiglio, del 23 luglio 2014, relativo al miglioramento del regolamento titoli nell'Unione europea e ai depositari centrali di titoli e recante modifica delle direttive 98/26/CE e 2014/65/UE e del regolamento (UE) n. 236/2012 (GU L 257 del 28.8.2014, pag. 1).
- <sup>(27)</sup> Direttiva (UE) 2022/2556 del Parlamento europeo e del Consiglio, del 14 dicembre 2022, che modifica le direttive 2009/65/CE, 2009/138/CE, 2011/61/UE, 2013/36/UE, 2014/59/UE, 2014/65/UE, (UE) 2015/2366 e (UE) 2016/2341 per quanto riguarda la resilienza operativa digitale per il settore finanziario (cfr. pag. 153 della presente Gazzetta ufficiale).
- <sup>(28)</sup> 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).



- (105) Poiché l'obiettivo del presente regolamento, ossia il conseguimento di un elevato livello di resilienza operativa digitale per le entità finanziarie regolamentate, non può essere conseguito in misura sufficiente dagli Stati membri, in quanto richiede l'armonizzazione di varie norme differenti nel diritto dell'Unione e nel diritto nazionale, ma, a motivo della portata o degli effetti dell'azione in questione, può essere conseguito meglio a livello di Unione, quest'ultima può intervenire in base al principio di sussidiarietà sancito dall'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.
- (106) Conformemente all'articolo 42, paragrafo 1, del regolamento (UE) 2018/1725 del Parlamento europeo e del Consiglio <sup>(29)</sup>, il Garante europeo della protezione dei dati è stato consultato e ha formulato il suo parere il 10 maggio 2021 <sup>(30)</sup>,

HANNO ADOTTATO IL PRESENTE REGOLAMENTO:

## CAPO I

### **Disposizioni generali**

#### Articolo 1

#### **Oggetto**

1. Al fine di conseguire un livello comune elevato di resilienza operativa digitale, il presente regolamento stabilisce i seguenti obblighi uniformi in relazione alla sicurezza dei sistemi informatici e di rete che sostengono i processi commerciali delle entità finanziarie:

- a) obblighi applicabili alle entità finanziarie in materia di:
- i) gestione dei rischi delle tecnologie dell'informazione e della comunicazione (TIC);
  - ii) segnalazione alle autorità competenti degli incidenti gravi connessi alle TIC e notifica, su base volontaria, delle minacce informatiche significative;
  - iii) segnalazione alle autorità competenti, da parte delle entità finanziarie di cui all'articolo 2, paragrafo 1, lettere da a) a d), di gravi incidenti operativi o relativi alla sicurezza dei pagamenti;
  - iv) test di resilienza operativa digitale;
  - v) condivisione di dati e di informazioni in relazione alle vulnerabilità e alle minacce informatiche;
  - vi) misure relative alla solida gestione dei rischi informatici derivanti da terzi;
- b) obblighi relativi agli accordi contrattuali stipulati tra fornitori terzi di servizi TIC ed entità finanziarie;
- c) norme per l'istituzione e l'attuazione di un quadro di sorveglianza per i fornitori terzi critici di servizi TIC, 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 materie trattate dal presente regolamento.

2. Quanto alle entità finanziarie identificate come soggetti essenziali o importanti ai sensi delle norme nazionali che recepiscono l'articolo 3 della direttiva 2022/2555, il presente regolamento è considerato un atto giuridico settoriale dell'Unione ai sensi dell'articolo 4 di tale direttiva.

3. Il presente regolamento lascia impregiudicata la responsabilità degli Stati membri per quanto riguarda le funzioni essenziali dello Stato concernenti la sicurezza pubblica, la difesa e la sicurezza nazionale conformemente al diritto dell'Unione.

<sup>(29)</sup> Regolamento (UE) 2018/1725 del Parlamento europeo e del Consiglio, del 23 ottobre 2018, sulla tutela delle persone fisiche in relazione al trattamento dei dati personali da parte delle istituzioni, degli organi e degli organismi dell'Unione e sulla libera circolazione di tali dati, e che abroga il regolamento (CE) n. 45/2001 e la decisione n. 1247/2002/CE (GU L 295 del 21.11.2018, pag. 39).

<sup>(30)</sup> GU C 229 del 15.6.2021, pag. 16.

*Articolo 2***Ambito di applicazione**

1. Fatti salvi i paragrafi 3 e 4, il presente regolamento si applica alle entità seguenti:
  - a) enti creditizi;
  - b) istituti di pagamento, compresi gli istituti di pagamento esentati a norma della direttiva (UE) 2015/2366;
  - c) prestatori di servizi di informazione sui conti;
  - d) istituti di moneta elettronica, compresi gli istituti di moneta elettronica esentati a norma della direttiva 2009/110/CE;
  - e) imprese di investimento;
  - f) fornitori di servizi per le cripto-attività autorizzati a norma del regolamento del Parlamento europeo e del Consiglio concernente i mercati delle cripto-attività e recante modifica dei regolamenti (UE) n. 1093/2010 e (UE) n. 1095/2010 e delle direttive 2013/36/UE e (UE) 2019/1937 (regolamento sui mercati delle cripto-attività) ed emittenti di token collegati ad attività;
  - g) depositari centrali di titoli;
  - h) controparti centrali;
  - i) sedi di negoziazione;
  - j) repertori di dati sulle negoziazioni;
  - k) gestori di fondi di investimento alternativi;
  - l) società di gestione;
  - m) fornitori di servizi di comunicazione dati;
  - n) imprese di assicurazione e di riassicurazione;
  - o) intermediari assicurativi, intermediari riassicurativi e intermediari assicurativi a titolo accessorio;
  - p) enti pensionistici aziendali o professionali;
  - q) agenzie di rating del credito;
  - r) amministratori di indici di riferimento critici;
  - s) fornitori di servizi di crowdfunding;
  - t) repertori di dati sulle cartolarizzazioni;
  - u) fornitori terzi di servizi TIC.
2. Ai fini del presente regolamento le entità di cui al paragrafo 1 lettere da a) a t) sono definite collettivamente «entità finanziarie».
3. Il presente regolamento non si applica a:
  - a) gestori di fondi di investimento alternativi di cui all'articolo 3, paragrafo 2, della direttiva 2011/61/UE;
  - b) imprese di assicurazione e di riassicurazione di cui all'articolo 4 della direttiva 2009/138/UE;
  - c) enti pensionistici aziendali o professionali che gestiscono schemi pensionistici che contano congiuntamente non più di 15 aderenti in totale;
  - d) persone fisiche o giuridiche esentate a norma degli articoli 2 e 3 della direttiva 2014/65/UE;
  - e) intermediari assicurativi, intermediari riassicurativi e intermediari assicurativi a titolo accessorio che sono microimprese o piccole o medie imprese;
  - f) uffici dei conti correnti postali di cui all'articolo 2, paragrafo 5, punto 3), della direttiva 2013/36/UE.

4. Gli Stati membri possono escludere dall'ambito di applicazione del presente regolamento le entità di cui all'articolo 2, paragrafo 5, punti da 4) a 23), della direttiva 2013/36/UE che sono situati nei rispettivi territori. Qualora uno Stato membro si avvalga di tale facoltà, e in occasione di ogni successiva modifica, ne informa la Commissione. La Commissione mette tali informazioni a disposizione del pubblico sul suo sito web o attraverso altri canali facilmente accessibili.

### Articolo 3

#### Definizioni

Ai fini del presente regolamento si applicano le definizioni seguenti:

- 1) «resilienza operativa digitale»: la capacità dell'entità finanziaria di costruire, assicurare e riesaminare la propria integrità e affidabilità operativa, garantendo, direttamente o indirettamente tramite il ricorso ai servizi offerti da fornitori terzi di servizi TIC, l'intera gamma delle capacità connesse alle TIC necessarie per garantire la sicurezza dei sistemi informatici e di rete utilizzati dall'entità finanziaria, su cui si fondano la costante offerta dei servizi finanziari e la loro qualità, anche in occasione di perturbazioni;
- 2) «sistema informatico e di rete»: un sistema informatico e di rete quali definiti all'articolo 6, punto 1), della direttiva (UE) 2022/2555;
- 3) «sistema legacy»: un sistema di TIC che ha raggiunto la fine del suo ciclo di vita (fine vita), non si presta ad aggiornamenti o correzioni per motivi tecnologici o commerciali, o non è più supportato dal suo fornitore o da un fornitore terzo di servizi TIC, ma è ancora in uso e supporta le funzioni dell'entità finanziaria;
- 4) «sicurezza dei sistemi informatici e di rete»: la sicurezza dei sistemi informatici e di rete quale definita all'articolo 6, punto 2), della direttiva (UE) 2022/2555;
- 5) «rischi informatici»: qualunque circostanza ragionevolmente identificabile in relazione all'uso dei sistemi informatici e di rete che, qualora si concretizzi, può compromettere la sicurezza dei sistemi informatici e di rete, di eventuali strumenti o processi dipendenti dalle tecnologie, di operazioni e processi, oppure della fornitura dei servizi causando effetti avversi nell'ambiente digitale o fisico;
- 6) «patrimonio informativo»: una raccolta di informazioni, tangibili o intangibili, che è importante proteggere;
- 7) «risorse TIC»: software o hardware presenti nei sistemi informatici e di rete utilizzati dall'entità finanziaria;
- 8) «incidente connesso alle TIC»: un singolo evento, o una serie di eventi collegati non programmati dall'entità finanziaria, che compromette la sicurezza dei sistemi informatici e di rete e ha un impatto avverso sulla disponibilità, autenticità, integrità o riservatezza dei dati o sui servizi forniti dall'entità finanziaria;
- 9) «incidente operativo o di sicurezza dei pagamenti»: un singolo evento o una serie di eventi collegati non programmati dalle entità finanziarie di cui all'articolo 2, paragrafo 1, lettere da a) a d), connessi alle TIC o meno, che hanno un impatto avverso sulla disponibilità, autenticità, integrità o riservatezza, la disponibilità, l'integrità o l'autenticità dei dati connessi ai pagamenti o sui servizi connessi ai pagamenti forniti dall'entità finanziaria;
- 10) «grave incidente TIC»: un incidente connesso alle TIC che ha un impatto avverso sui sistemi informatici e di rete a supporto delle funzioni essenziali o importanti dell'entità finanziaria;
- 11) «grave incidente operativo o di sicurezza dei pagamenti»: un incidente operativo o di sicurezza dei pagamenti che ha un impatto avverso sui servizi connessi ai pagamenti forniti;
- 12) «minaccia informatica»: minaccia informatica quale definita all'articolo 2, punto 8), del regolamento (UE) 2019/881;
- 13) «minaccia informatica significativa»: una minaccia informatica le cui caratteristiche tecniche indicano che potrebbe potenzialmente causare un grave incidente TIC o un grave incidente operativo o di sicurezza dei pagamenti;
- 14) «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;

- 15) «analisi delle minacce»: informazioni aggregate, trasformate, analizzate, interpretate o arricchite per offrire il contesto necessario al processo decisionale e consentire 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;
- 16) «vulnerabilità»: debolezza, predisposizione o difetto di una risorsa, un sistema, un processo o un controllo potenzialmente sfruttabile;
- 17) «test di penetrazione guidato dalla minaccia (TLPT)»: un quadro che imita le tattiche, le tecniche e le procedure di attori reali della minaccia che sono percepiti come minaccia informatica autentica, che consente di eseguire un test dei sistemi di produzione attivi e critici dell'entità finanziaria in maniera controllata, mirata e basata sull'analisi della minaccia (*red team*);
- 18) «rischi informatici 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 TIC offerti da fornitori terzi o da subappaltatori di tali fornitori, anche mediante accordi di esternalizzazione;
- 19) «fornitore terzo di servizi TIC»: un'impresa che fornisce servizi TIC;
- 20) «fornitore intragruppo di servizi TIC»: un'impresa che fa parte di un gruppo finanziario e fornisce prevalentemente servizi TIC a entità finanziarie dello stesso gruppo o a entità finanziarie appartenenti allo stesso sistema di tutela istituzionale (*institutional protection scheme*), comprese le loro società madri, imprese figlie e succursali o altre entità di proprietà comune o sotto controllo comune;
- 21) «servizi TIC»: servizi digitali e di dati forniti attraverso sistemi di TIC a uno o più utenti interni o esterni su base continuativa, inclusi l'hardware come servizio e i servizi hardware, comprendenti la fornitura di assistenza tecnica mediante aggiornamenti di software e firmware da parte del fornitore dell'hardware, esclusi i servizi telefonici analogici tradizionali;
- 22) «funzione essenziale o importante»: una funzione la cui interruzione comprometterebbe sostanzialmente i risultati finanziari di un'entità finanziaria o ancora la solidità o la continuità dei suoi servizi e delle sue attività, o la cui esecuzione 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 normativa applicabile in materia di servizi finanziari;
- 23) «fornitore terzo critico di servizi TIC»: un fornitore terzo di servizi TIC designato come critico in conformità dell'articolo 31;
- 24) «fornitore terzo di servizi TIC stabilito in un paese terzo»: un fornitore terzo di servizi TIC che è una persona giuridica stabilita in un paese terzo che ha stipulato un accordo contrattuale con un'entità finanziaria per la fornitura di servizi TIC;
- 25) «impresa figlia»: impresa figlia ai sensi dell'articolo 2, punto 10), e dell'articolo 22 della direttiva 2013/34/UE;
- 26) «gruppo»: un gruppo quale definito all'articolo 2, punto 11), della direttiva 2013/34/UE;
- 27) «impresa madre»: impresa madre ai sensi dell'articolo 2, punto 9), e dell'articolo 22 della direttiva 2013/34/UE;
- 28) «subappaltatore di TIC stabilito in un paese terzo»: un subappaltatore di TIC che è una persona giuridica stabilita in un paese terzo che ha stipulato un accordo contrattuale con un fornitore terzo di servizi TIC o con un fornitore terzo di servizi TIC stabilito in un paese terzo;
- 29) «rischio di concentrazione delle TIC»: l'esposizione a fornitori terzi critici di servizi TIC, 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 essi potrebbero mettere a repentaglio la capacità di un'entità finanziaria di assolvere funzioni essenziali o importanti oppure di assorbire altri tipi di effetti avversi, comprese perdite cospicue, o potrebbero mettere a repentaglio la stabilità finanziaria dell'intera Unione;

- 30) «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 del Parlamento europeo e del Consiglio <sup>(31)</sup>, 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 e alla pertinente disposizione del regolamento sui mercati delle cripto-attività oppure le persone equivalenti che gestiscono di fatto l'entità o che assolvono funzioni chiave conformemente al pertinente diritto dell'Unione o nazionale;
- 31) «ente creditizio»: ente creditizio ai sensi dell'articolo 4, paragrafo 1, punto 1), del regolamento (UE) n. 575/2013 del Parlamento europeo e del Consiglio <sup>(32)</sup>;
- 32) «ente esentato dalla direttiva 2013/36/UE»: un'entità di cui all'articolo 2, paragrafo 5, punti da 4) a 23), della direttiva 2013/36/UE;
- 33) «impresa di investimento»: un'impresa di investimento quale definita all'articolo 4, paragrafo 1, punto 1), della direttiva 2014/65/UE;
- 34) «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 del Parlamento europeo e del Consiglio <sup>(33)</sup>;
- 35) «istituto di pagamento»: un istituto di pagamento quale definito all'articolo 4, punto 4), della direttiva (UE) 2015/2366;
- 36) «istituto di pagamento esentato a norma della direttiva (UE) 2015/2366»: un istituto di pagamento esentato a norma dell'articolo 32, paragrafo 1, della direttiva (UE) 2015/2366;
- 37) «prestatore di servizi di informazione sui conti»: un prestatore di servizi di informazione sui conti di cui all'articolo 33, paragrafo 1, della direttiva (UE) 2015/2366;
- 38) «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;
- 39) «istituto di moneta elettronica esentato a norma della direttiva 2009/110/CE»: un istituto di moneta elettronica; che beneficia di un'esenzione ai sensi dell'articolo 9, paragrafo 1, della direttiva 2009/110/CE;
- 40) «controparte centrale»: una controparte centrale quale definita all'articolo 2, punto 1), del regolamento (UE) n. 648/2012;
- 41) «repertorio di dati sulle negoziazioni»: un repertorio di dati sulle negoziazioni quale definito all'articolo 2, punto 2), del regolamento (UE) n. 648/2012;
- 42) «depositario centrale di titoli»: un depositario centrale di titoli quale definito all'articolo 2, paragrafo 1, punto 1), del regolamento (UE) n. 909/2014;
- 43) «sede di negoziazione»: una sede di negoziazione quale definita all'articolo 4, paragrafo 1, punto 24), della direttiva 2014/65/UE;
- 44) «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;
- 45) «società di gestione»: una società di gestione quale definita all'articolo 2, paragrafo 1, lettera b), della direttiva 2009/65/CE;
- 46) «fornitore di servizi di comunicazione dati»: un fornitore di servizi di comunicazione dati ai sensi del regolamento (UE) n. 600/2014, articolo 2, paragrafo 1, punti da 34) a 36);
- 47) «impresa di assicurazione»: impresa di assicurazione ai sensi dell'articolo 13, punto 1), della direttiva 2009/138/CE;
- 48) «impresa di riassicurazione»: impresa di riassicurazione ai sensi dell'articolo 13, punto 4), della direttiva 2009/138/CE;

<sup>(31)</sup> Direttiva 2009/65/CE del Parlamento europeo e del Consiglio, del 13 luglio 2009, concernente il coordinamento delle disposizioni legislative, regolamentari e amministrative in materia di taluni organismi d'investimento collettivo in valori mobiliari (OICVM) (GU L 302 del 17.11.2009, pag. 32).

<sup>(32)</sup> Regolamento (UE) n. 575/2013, del Parlamento europeo e del Consiglio, del 26 giugno 2013, relativo ai requisiti prudenziali per gli enti creditizi e che modifica il regolamento (UE) n. 648/2012 (GU L 176 del 27.6.2013, pag. 1).

<sup>(33)</sup> Regolamento (UE) 2019/2033 del Parlamento europeo e del Consiglio, del 27 novembre 2019, relativo ai requisiti prudenziali delle imprese di investimento e che modifica i regolamenti (UE) n. 1093/2010, (UE) n. 575/2013, (UE) n. 600/2014 e (UE) n. 806/2014 (GU L 314 del 5.12.2019, pag. 1).

- 49) «intermediario assicurativo»: un intermediario assicurativo quale definito all'articolo 2, paragrafo 1, punto 3), della direttiva (UE) 2016/97 del Parlamento europeo e del Consiglio <sup>(34)</sup>;
- 50) «intermediario assicurativo a titolo accessorio»: un intermediario assicurativo quale definito all'articolo 2, paragrafo 1, punto 4), della direttiva (UE) 2016/97;
- 51) «intermediario riassicurativo»: un intermediario riassicurativo quale definito all'articolo 2, paragrafo 1, punto 5), della direttiva (UE) 2016/97;
- 52) «ente pensionistico aziendale o professionale»: un ente pensionistico aziendale o professionale quale definito all'articolo 6, punto 1), della direttiva 2016/2341;
- 53) «piccolo ente pensionistico aziendale o professionale»: un ente pensionistico aziendale o professionale che gestisce schemi pensionistici che contano congiuntamente meno di 100 aderenti in totale;
- 54) «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;
- 55) «fornitore di servizi per le cripto-attività»: un fornitore di servizi per le cripto-attività quale definito alla pertinente disposizione del regolamento sui mercati delle cripto-attività;
- 56) «emittente di token collegati ad attività»: un emittente di token collegati ad attività quale definito alla pertinente disposizione del regolamento sui mercati delle cripto-attività;
- 57) «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;
- 58) «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 del Parlamento europeo e del Consiglio <sup>(35)</sup>;
- 59) «repertorio di dati sulle cartolarizzazioni»: un repertorio di dati sulle cartolarizzazioni quale definito all'articolo 2, punto 23), del regolamento (UE) 2017/2402 del Parlamento europeo e del Consiglio <sup>(36)</sup>;
- 60) «microimpresa»: un'entità finanziaria, diversa da una sede di negoziazione, una controparte centrale, un repertorio di dati sulle negoziazioni o un depositario centrale di titoli, che occupa meno di 10 persone e realizza un fatturato annuo e/o un totale di bilancio annuo non superiore a 2 milioni di EUR;
- 61) «autorità di sorveglianza capofila»: l'autorità europea di vigilanza designata a norma dell'articolo 31, paragrafo 1, lettera b), del presente regolamento;
- 62) «comitato congiunto»: il comitato di cui all'articolo 54 dei regolamenti (UE) n. 1093/2010, (UE) n. 1094/2010 e (UE) n. 1095/2010;
- 63) «piccola impresa»: un'entità finanziaria che occupa 10 o più persone ma meno di 50 persone e realizza un fatturato annuo e/o un totale di bilancio annuo che supera 2 milioni di EUR ma non superiore a 10 milioni di EUR;
- 64) «media impresa»: un'entità finanziaria che non è una piccola impresa, occupa meno di 250 persone e realizza un fatturato annuo non superiore a 50 milioni di EUR e/o un bilancio annuo non superiore a 43 milioni di EUR;
- 65) «autorità pubblica»: qualsiasi ente governativo o altro ente della pubblica amministrazione, comprese le banche centrali nazionali.

<sup>(34)</sup> Direttiva (UE) 2016/97 del Parlamento europeo e del Consiglio, del 20 gennaio 2016, sulla distribuzione assicurativa (GU L 26 del 2.2.2016, pag. 19).

<sup>(35)</sup> Regolamento (UE) 2020/1503 del Parlamento europeo e del Consiglio, del 7 ottobre 2020, relativo ai fornitori europei di servizi di crowdfunding per le imprese, e che modifica il regolamento (UE) 2017/1129 e la direttiva (UE) 2019/1937 (GU L 347 del 20.10.2020, pag. 1).

<sup>(36)</sup> Regolamento (UE) 2017/2402 del Parlamento europeo e del Consiglio, del 12 dicembre 2017, che stabilisce un quadro generale per la cartolarizzazione, instaura un quadro specifico per cartolarizzazioni semplici, trasparenti e standardizzate e modifica le direttive 2009/65/CE, 2009/138/CE e 2011/61/UE e i regolamenti (CE) n. 1060/2009 e (UE) n. 648/2012 (GU L 347 del 28.12.2017, pag. 35).

*Articolo 4***Principio di proporzionalità**

1. Le entità finanziarie attuano le norme di cui al capo II conformemente al principio di proporzionalità, tenendo conto delle loro dimensioni e del loro profilo di rischio complessivo, nonché della natura, della portata e della complessità dei loro servizi, delle loro attività e della loro operatività.
2. Inoltre, l'applicazione dei capi III e IV e del capo V, sezione I, da parte delle entità finanziarie è proporzionata alle loro dimensioni e al loro profilo di rischio complessivo, nonché alla natura, alla portata e alla complessità dei loro servizi, delle loro attività e della loro operatività, come specificamente previsto dalle pertinenti norme di tali capi.
3. Le autorità competenti prendono in considerazione l'applicazione del principio di proporzionalità da parte delle entità finanziarie in sede di riesame della coerenza del quadro per la gestione dei rischi informatici sulla base delle relazioni presentate su richiesta delle autorità competenti a norma dell'articolo 6, paragrafo 5, e dell'articolo 16, paragrafo 2.

*CAPO II***Gestione dei rischi informatici***Sezione I**Articolo 5***Governance e organizzazione**

1. Le entità finanziarie predispongono un quadro di gestione e di controllo interno che garantisce una gestione efficace e prudente di tutti i rischi informatici, conformemente all'articolo 6, paragrafo 4, al fine di acquisire 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 informatici di cui all'articolo 6, paragrafo 1, vigila su tale attuazione e ne è responsabile.

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

- a) assume la responsabilità finale per la gestione dei rischi informatici dell'entità finanziaria;
- b) predispone politiche miranti a garantire il mantenimento di standard elevati di disponibilità, autenticità, integrità e riservatezza dei dati;
- c) definisce chiaramente ruoli e responsabilità per tutte le funzioni connesse alle TIC e stabilisce adeguati meccanismi di governance al fine di garantire una comunicazione, una cooperazione e un coordinamento efficaci e tempestivi tra tali funzioni;
- d) ha la responsabilità generale di definire e approvare la strategia di resilienza operativa digitale di cui all'articolo 6, paragrafo 8, compresa la determinazione del livello appropriato di tolleranza per i rischi informatici dell'entità finanziaria, ai sensi dell'articolo 6, paragrafo 8, lettera b);
- e) approva, supervisiona e riesamina periodicamente l'attuazione della politica di continuità operativa delle TIC e dei piani di risposta e ripristino relativi alle TIC dell'entità finanziaria, di cui rispettivamente all'articolo 11, paragrafi 1 e 3, che possono essere adottati come politica specifica dedicata che costituisce parte integrante della politica generale di continuità operativa e del piano di risposta e ripristino dell'entità finanziaria;
- f) approva e riesamina periodicamente i piani interni di audit in materia di TIC dell'entità finanziaria, gli audit in materia di TIC e le più importanti modifiche a essi apportate;
- g) assegna e riesamina periodicamente le risorse finanziarie adeguate per soddisfare le esigenze di resilienza operativa digitale dell'entità finanziaria rispetto a tutti i tipi di risorse, compresi i pertinenti programmi di sensibilizzazione sulla sicurezza delle TIC e le attività di formazione sulla resilienza operativa digitale di cui all'articolo 13, paragrafo 6, nonché le competenze in materia di TIC per tutto il personale;

- h) approva e riesamina periodicamente la politica dell'entità finanziaria relativa alle modalità per l'uso dei servizi TIC prestati dal fornitore terzo di servizi TIC;
  - i) istituisce a livello aziendale canali di comunicazione che gli consentono di essere debitamente informato in merito a quanto segue:
    - i) gli accordi conclusi con i fornitori terzi di servizi TIC sull'uso di tali servizi;
    - ii) le relative eventuali modifiche importanti e pertinenti previste riguardo ai fornitori terzi di servizi TIC;
    - iii) il potenziale impatto di tali modifiche sulle funzioni essenziali o importanti soggette agli accordi in questione, compresa una sintesi dell'analisi del rischio per valutare l'impatto di tali modifiche, nonché almeno gli gravi incidenti TIC e il loro impatto, le misure di risposta e ripristino e le misure correttive.
3. Le entità finanziarie diverse dalle microimprese istituiscono un ruolo al fine di monitorare gli accordi conclusi con i fornitori terzi di servizi TIC per l'uso di tali servizi, oppure designano un dirigente di rango elevato quale responsabile della sorveglianza sulla relativa esposizione al rischio e sulla documentazione pertinente.
4. I membri dell'organo di gestione dell'entità finanziaria mantengono attivamente aggiornate conoscenze e competenze adeguate per comprendere e valutare i rischi informatici e il loro impatto sulle operazioni dell'entità finanziaria, anche seguendo una formazione specifica su base regolare, commisurata ai rischi informatici gestiti.

## Sezione II

### Articolo 6

#### **Quadro per la gestione dei rischi informatici**

1. Nell'ambito del sistema di gestione globale del rischio, le entità finanziarie predispongono un quadro per la gestione dei rischi informatici solido, esaustivo e adeguatamente documentato, che consenta loro di affrontare i rischi informatici in maniera rapida, efficiente ed esaustiva, assicurando un elevato livello di resilienza operativa digitale.
2. Il quadro per la gestione dei rischi informatici comprende almeno strategie, politiche, procedure, protocolli e strumenti in materia di TIC necessari per proteggere debitamente e adeguatamente tutti i patrimoni informativi e i risorse TIC, compresi software, hardware e server, nonché tutte le pertinenti infrastrutture e componenti fisiche, quali i locali, i centri di elaborazione dati e le aree designate come sensibili, così da garantire che tutti i patrimoni informativi e i risorse TIC siano adeguatamente protetti contro i rischi, compresi i danneggiamenti e l'accesso o l'uso non autorizzati.
3. Conformemente al proprio quadro per la gestione dei rischi informatici, le entità finanziarie riducono al minimo l'impatto dei rischi informatici applicando strategie, politiche, procedure, protocolli e strumenti in materia di TIC adeguati. Forniscono alle autorità competenti, su richiesta di queste ultime, informazioni complete e aggiornate sui rischi informatici e sul proprio quadro per la gestione dei rischi informatici.
4. Le entità finanziarie diverse dalle microimprese attribuiscono la responsabilità della gestione e della sorveglianza dei rischi informatici a una funzione di controllo, di cui assicurano un livello appropriato d'indipendenza per evitare conflitti d'interessi. Le entità finanziarie garantiscono un'opportuna separazione e indipendenza tra funzioni di gestione dei rischi informatici, funzioni di controllo e funzioni di audit interno, secondo il modello delle tre linee di difesa o secondo un modello interno di controllo e gestione del rischio.
5. Il quadro per la gestione dei rischi informatici è documentato e riesaminato almeno una volta all'anno, o periodicamente in caso di microimprese, nonché in occasione di gravi incidenti TIC e in seguito a indicazioni 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. È presentata all'autorità competente, su sua richiesta, una relazione in merito al riesame del quadro per la gestione dei rischi informatici.



6. Il quadro per la gestione dei rischi informatici delle entità finanziarie, diverse dalle microimprese, è sottoposto periodicamente a verifiche di audit interne effettuate da addetti all'audit in linea con i piani di audit delle entità finanziarie. Tali addetti all'audit possiedono conoscenze, competenze ed esperienze adeguate in materia di rischi informatici, nonché un'adeguata indipendenza. La frequenza e l'oggetto delle verifiche di audit in materia di TIC sono commisurati ai rischi connessi alle TIC cui è esposta l'entità finanziaria.

7. Sulla base delle conclusioni dell'audit interno in materia di TIC, le entità finanziarie istituiscono un procedimento formale per darvi seguito, comprendente regole per la verifica tempestiva delle risultanze critiche e l'adozione di rimedi.

8. Il quadro per la gestione dei rischi informatici comprende una strategia di resilienza operativa digitale che definisce le modalità di attuazione del quadro. A tal fine, la strategia di resilienza operativa digitale include metodi per affrontare i rischi informatici e conseguire specifici obiettivi in materia di TIC:

- a) spiegando in che modo il quadro per la gestione dei rischi informatici sostiene gli obiettivi e la strategia commerciale dell'entità finanziaria;
- b) fissando il livello di tolleranza per i rischi informatici, 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, compresi indicatori chiave di prestazione e parametri chiave di rischio;
- d) spiegando l'architettura di riferimento a livello di TIC e le eventuali modifiche necessarie per conseguire specifici obiettivi commerciali;
- e) delineando i differenti meccanismi introdotti per individuare incidenti connessi alle TIC, prevenire il loro impatto e proteggersi dallo stesso;
- f) documentando l'attuale situazione di resilienza operativa digitale sulla base del numero di gravi incidenti TIC segnalati, nonché l'efficacia delle misure preventive;
- g) attuando test di resilienza operativa digitale, conformemente al capo IV del presente regolamento;
- h) delineando una strategia di comunicazione in caso di incidenti connessi alle TIC di cui è richiesta la divulgazione a norma dell'articolo 14.

9. Le entità finanziarie possono, nel contesto della strategia di resilienza operativa digitale di cui al paragrafo 8, definire una strategia olistica per le TIC a livello di gruppo o di entità, basata su una varietà di fornitori, che indichi le principali dipendenze da fornitori terzi di servizi TIC e che spieghi la logica sottesa alla ripartizione degli appalti tra i fornitori terzi di servizi TIC.

10. Le entità finanziarie possono, conformemente alla normativa settoriale dell'Unione e nazionale, esternalizzare a imprese interne o esterne al gruppo i compiti di verifica della conformità ai requisiti in materia di gestione dei rischi informatici. In caso di esternalizzazione, l'entità finanziaria rimane pienamente responsabile di verificare la conformità ai requisiti in materia di gestione dei rischi informatici.

#### Articolo 7

#### **Sistemi, protocolli e strumenti di TIC**

Al fine di affrontare e gestire i rischi informatici, le entità finanziarie utilizzano e mantengono aggiornati sistemi, protocolli e strumenti di TIC che sono:

- a) idonei alle dimensioni delle operazioni a supporto dello svolgimento delle attività delle entità finanziarie, conformemente al principio di proporzionalità di cui all'articolo 4;
- b) affidabili;
- c) dotati di capacità sufficiente per elaborare in maniera accurata i dati necessari per lo svolgimento delle attività e la tempestiva fornitura dei servizi, 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) 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.

## Articolo 8

### Identificazione

1. Nell'ambito del quadro per la gestione dei rischi informatici di cui all'articolo 6, paragrafo 1, le entità finanziarie identificano, classificano e documentano adeguatamente tutte le funzioni commerciali supportate dalle TIC, i ruoli e le responsabilità, i patrimoni informativi e le risorse TIC a supporto delle suddette funzioni, nonché i ruoli e le dipendenze rispettivi in materia di rischi informatici. Le entità finanziarie riesaminano, secondo necessità e almeno una volta all'anno, l'adeguatezza di tale classificazione e di altri documenti eventualmente pertinenti.
2. Le entità finanziarie identificano costantemente tutte le fonti di rischio relative alle TIC, in particolare l'esposizione al rischio da e verso altre entità finanziarie, e valutano le minacce informatiche e le vulnerabilità in materia di TIC pertinenti per le loro funzioni commerciali supportate dalle TIC, per i loro patrimoni informativi e per i loro risorse TIC. Le entità finanziarie riesaminano periodicamente, e almeno una volta all'anno, gli scenari di rischio che esercitano un impatto su di loro.
3. Le entità finanziarie diverse dalle microimprese effettuano una valutazione del rischio in occasione di ogni modifica di rilievo dell'infrastruttura del sistema informatico e di rete, dei processi o delle procedure che incidono sulle loro funzioni commerciali supportate dalle TIC, sui loro patrimoni informativi o sulle loro risorse TIC.
4. Le entità finanziarie identificano tutti i patrimoni informativi e le risorse TIC, compresi quelli su siti remoti, le risorse di rete e le attrezzature hardware, e mappano quelle considerate essenziali. Effettuano la mappatura della configurazione dei patrimoni informativi e delle risorse TIC, nonché dei collegamenti e delle interdipendenze tra i diversi patrimoni informativi e risorse TIC.
5. Le entità finanziarie identificano e documentano tutti i processi dipendenti da fornitori terzi di servizi TIC e identificano le interconnessioni con detti fornitori che offrono servizi a supporto di funzioni essenziali o importanti.
6. Ai fini dei paragrafi 1, 4 e 5, le entità finanziarie mantengono inventari pertinenti e li aggiornano periodicamente e in occasione di ogni modifica di rilievo di cui al paragrafo 3.
7. Le entità finanziarie diverse dalle microimprese effettuano periodicamente, almeno una volta all'anno e in ogni caso prima e dopo la connessione di tecnologie, applicazioni o sistemi, una valutazione del rischio specifica per tutti i sistemi legacy.

## Articolo 9

### 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 la sicurezza e il funzionamento dei sistemi e degli strumenti di TIC e riducono al minimo l'impatto dei rischi informatici sui sistemi di TIC adottando politiche, procedure e strumenti adeguati per la sicurezza delle TIC.
2. Le entità finanziarie definiscono, acquisiscono e attuano politiche, procedure, protocolli e strumenti per la sicurezza delle TIC miranti a garantire la resilienza, la continuità e la disponibilità dei sistemi di TIC, in particolare quelli a supporto di funzioni essenziali o importanti, nonché a mantenere standard elevati di disponibilità, autenticità, integrità e riservatezza dei dati conservati, in uso o in transito.
3. Al fine di conseguire gli obiettivi di cui al paragrafo 2 le entità finanziarie usano soluzioni e processi TIC appropriati conformemente all'articolo 4. Tali soluzioni e processi TIC:
  - a) garantiscono la sicurezza dei mezzi di trasferimento dei dati;
  - 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) prevengono la mancanza di disponibilità, il deterioramento dell'autenticità o dell'integrità, le violazioni della riservatezza e la perdita di dati;

- d) assicurano la protezione dei dati contro i rischi derivanti dalla gestione dei dati, 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 informatici di cui all'articolo 6, paragrafo 1, le entità finanziarie:
- a) elaborano e documentano una politica di sicurezza dell'informazione che definisce le norme per tutelare la disponibilità, l'autenticità, l'integrità e la riservatezza dei dati, dei patrimoni informativi e delle risorse TIC, compresi quelli dei loro clienti, se del caso;
  - b) seguendo un approccio basato sul rischio, realizzano una solida struttura di gestione della rete e delle infrastrutture impiegando tecniche, metodi e protocolli adeguati, che possono includere l'applicazione di meccanismi automatizzati, per isolare i patrimoni informativi colpiti in caso di attacchi informatici;
  - c) attuano politiche che limitano l'accesso fisico o logico ai patrimoni informativi e alle risorse TIC unicamente a quanto è necessario per funzioni e attività legittime e approvate, e stabiliscono a tale scopo una serie di politiche, procedure e controlli concernenti i diritti di accesso e garantiscono una solida amministrazione degli stessi;
  - d) attuano politiche e protocolli riguardanti robusti meccanismi di autenticazione, basati su norme pertinenti e sistemi di controllo dedicati, e misure di protezione delle chiavi crittografiche di cifratura dei dati sulla scorta dei risultati di processi approvati per la classificazione dei dati e la valutazione dei rischi informatici;
  - e) attuano politiche, procedure e controlli documentati per la gestione delle modifiche delle TIC, comprese le modifiche apportate a componenti software, hardware e firmware, sistemi o parametri di 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 documentate, idonee ed esaustive in materia di correzioni ed aggiornamenti.

Ai fini della lettera b) del primo comma, le entità finanziarie progettano l'infrastruttura di connessione di rete in modo che sia possibile isolarla o segmentarla istantaneamente, al fine di ridurre al minimo e prevenire il contagio, soprattutto per i processi finanziari interconnessi.

Ai fini della lettera e) del primo comma, il processo di gestione delle modifiche delle TIC è approvato da linee di gestione adeguate e comprende protocolli specifici in essere.

#### Articolo 10

#### Individuazione

1. Le entità finanziarie predispongono meccanismi per individuare tempestivamente le attività anomale, conformemente all'articolo 17, compresi i problemi di prestazione della rete delle TIC e gli incidenti a esse connessi, nonché per individuare i potenziali singoli punti di vulnerabilità (*points of failure*) importanti.

Tutti i meccanismi di individuazione di cui al primo comma sono periodicamente testati in conformità dell'articolo 25.

2. I meccanismi di individuazione di cui al paragrafo 1 prevedono molteplici livelli di controllo, definiscono soglie di allarme e criteri per l'attivazione e l'avvio dei processi di risposta agli incidenti connessi alle TIC, compresi 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 di eventuali anomalie e incidenti connessi alle TIC, in particolare attacchi informatici.

4. I fornitori di servizi di comunicazione dati 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 11

**Risposta e ripristino**

1. All'interno del quadro per la gestione dei rischi informatici di cui all'articolo 6, paragrafo 1, e in base ai requisiti di identificazione stabiliti all'articolo 8, le entità finanziarie predispongono una politica di continuità operativa delle TIC esaustiva, la quale può essere adottata come una politica specifica dedicata che costituisce parte integrante della politica generale di continuità operativa dell'entità finanziaria.

2. Le entità finanziarie attuano la politica di continuità operativa delle TIC tramite accordi, piani, procedure e meccanismi appositi, appropriati e documentati, miranti a:

- a) garantire la continuità delle funzioni essenziali o importanti dell'entità finanziaria;
- b) rispondere in maniera rapida, appropriata ed efficace e trovare una soluzione a tutti gli incidenti connessi alle TIC, in modo da limitare i danni e privilegiare la ripresa delle attività e le azioni di ripristino;
- c) attivare senza ritardo 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 12;
- d) stimare in via preliminare impatti, danni e perdite;
- e) 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 14, e comunicare tali informazioni alle autorità competenti, conformemente all'articolo 19.

3. All'interno del quadro per la gestione dei rischi informatici di cui all'articolo 6, paragrafo 1, le entità finanziarie attuano i piani di risposta e ripristino relativi alle TIC associati; per le entità finanziarie diverse dalle microimprese tali piani sono soggetti a un audit interno indipendente.

4. Le entità finanziarie predispongono, mantengono e testano periodicamente opportuni piani di continuità operativa delle TIC, in particolare per quanto riguarda le funzioni essenziali o importanti esternalizzate o appaltate tramite accordi con fornitori terzi di servizi TIC.

5. Nell'ambito della politica generale di continuità operativa, le entità finanziarie effettuano un'analisi dell'impatto sulle attività aziendali (*Business Impact Analysis* — BIA) delle loro esposizioni a gravi perturbazioni delle attività. Nel quadro della BIA, le entità finanziarie valutano l'impatto potenziale di gravi perturbazioni delle attività mediante criteri quantitativi e qualitativi, utilizzando, se del caso, dati interni ed esterni e analisi di scenario. La BIA tiene conto della criticità delle funzioni commerciali, dei processi di supporto, delle dipendenze da terzi e dei patrimoni informativi individuati e mappati, nonché delle loro interdipendenze. Le entità finanziarie provvedono affinché le risorse TIC e i servizi TIC siano progettati e utilizzati in piena conformità con la BIA, in particolare garantendo adeguatamente la ridondanza di tutte le componenti essenziali.

6. All'interno della gestione complessiva dei rischi informatici, le entità finanziarie:

- a) testano i piani di continuità operativa delle TIC e i piani di risposta e ripristino relativi alle TIC in relazione ai sistemi di TIC a supporto di tutte le funzioni almeno una volta all'anno nonché in caso di modifiche di rilievo ai sistemi di TIC a supporto di funzioni essenziali o importanti;
- b) testano i piani di comunicazione delle crisi istituiti in conformità dell'articolo 14.

Ai fini del primo comma, lettera a), le entità finanziarie diverse dalle microimprese inseriscono nei piani dei test scenari di attacchi informatici e del passaggio 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 12.

Le entità finanziarie riesaminano periodicamente la politica di continuità operativa delle TIC e i piani di risposta e ripristino relativi 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.

7. Le entità finanziarie diverse dalle microimprese si dotano di una funzione di gestione delle crisi che, in caso di attivazione dei piani di continuità operativa delle TIC o dei piani di risposta e ripristino relativi alle TIC, fissa, tra l'altro, procedure chiare per la gestione della comunicazione interna ed esterna delle crisi, in conformità dell'articolo 14.
8. Le entità finanziarie rendono prontamente accessibili le registrazioni delle attività svolte prima e durante le perturbazioni in cui vengono attivati i piani di continuità operativa delle TIC e i piani di risposta e ripristino relativi alle TIC.
9. Le controparti centrali trasmettono alle autorità competenti copie dei risultati dei test di continuità operativa delle TIC o di esercizi analoghi.
10. Le entità finanziarie, diverse dalle microimprese, comunicano alle autorità competenti, su loro richiesta di queste ultime, una stima dei costi e delle perdite annuali aggregati causati da incidenti gravi connessi alle TIC.
11. A norma dell'articolo 16 dei regolamenti (UE) n. 1093/2010, (UE) n. 1094/2010 e (UE) n. 1095/2010, le AEV elaborano, tramite il comitato congiunto, entro il 17 luglio 2024 orientamenti comuni sulla stima dei costi e delle perdite annuali aggregati di cui al paragrafo 10.

## Articolo 12

### **Politiche e procedure di backup — Procedure e metodi di ripristino e recupero**

1. Al fine di assicurare che i sistemi e i dati di TIC siano ripristinati riducendo al minimo il periodo di inattività e limitando la perturbazione e le perdite, all'interno del proprio quadro per la gestione dei rischi informatici le entità finanziarie elaborano e documentano:
  - a) le politiche e procedure di backup che precisano il perimetro dei dati soggetti a backup e la frequenza minima del backup, in base alla criticità delle informazioni o al livello di riservatezza dei dati;
  - b) le procedure e i metodi di ripristino e recupero.

2. Le entità finanziarie si dotano di sistemi di backup che possono essere attivati conformemente alle politiche e alle procedure di backup, come pure alle procedure e ai metodi di ripristino e recupero. L'attivazione dei sistemi di backup non mette a repentaglio la sicurezza dei sistemi informatici e di rete né, la disponibilità, l'autenticità, l'integrità o la riservatezza dei dati. I test delle procedure di backup e di ripristino nonché delle procedure e dei metodi di recupero sono effettuati periodicamente.

3. Nel ripristino dei dati di backup effettuato utilizzando i propri sistemi, le entità finanziarie impiegano sistemi di TIC che sono fisicamente e logicamente segregati dal sistema di TIC sorgente. I sistemi di TIC sono protetti in maniera sicura da qualsiasi accesso non autorizzato o corruzione delle TIC e consentono il tempestivo ripristino dei servizi attraverso il backup dei dati e dei sistemi ove necessario.

Per le controparti centrali, 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.

I fornitori di servizi di comunicazione dati mantengono inoltre risorse adeguate e dispongono di attrezzature di back-up e ripristino per offrire e mantenere in ogni momento i loro servizi.

4. Le entità finanziarie, diverse dalle microimprese, mantengono capacità di TIC ridondanti, dotate di risorse e funzioni sufficienti e adeguate a soddisfare le esigenze commerciali. Le microimprese valutano la necessità di mantenere tali capacità di TIC ridondanti sulla base del loro profilo di rischio.
5. I depositari centrali di titoli mantengono almeno un sito secondario di trattamento dati dotato di risorse, capacità, funzioni e personale adeguati a soddisfare le esigenze commerciali.

Il sito secondario di trattamento dati è:

- a) ubicato geograficamente a distanza dal sito primario per garantire che esso abbia 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 delle funzioni essenziali o importanti in maniera identica al sito primario, oppure di fornire il livello di servizi necessario a garantire che l'entità finanziaria svolga le proprie operazioni essenziali nell'ambito degli obiettivi di ripristino;
- c) immediatamente accessibile al personale dell'entità finanziaria per garantire la continuità delle funzioni essenziali o importanti qualora il sito primario di trattamento dati divenga indisponibile.

6. Nel determinare gli obiettivi in materia di punti di ripristino e tempi di ripristino di ciascuna funzione, le entità finanziarie tengono conto del fatto che si tratti di una funzione essenziale 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 effettuano le verifiche necessarie, comprese eventuali verifiche multiple e controlli incrociati, per assicurare che sia mantenuto il più elevato livello di integrità dei dati. Questi controlli sono effettuati anche al momento di ricostruire i dati provenienti da portatori di interessi esterni, per assicurare la piena coerenza di tutti i dati tra i sistemi.

### Articolo 13

#### **Apprendimento ed evoluzione**

1. Le entità finanziarie dispongono 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 che un grave incidente connesso alle TIC ha perturbato le loro attività principali, le entità finanziarie svolgono un riesame successivo a tale incidente 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 11.

Le entità finanziarie diverse dalle microimprese comunicano, su richiesta, alle autorità competenti le modifiche attuate a seguito del riesame successivo all'incidente connesso alle TIC di cui al primo comma.

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, ove ritenuto opportuno;
- 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 26 e 27 e da incidenti connessi alle TIC realmente avvenuti, in particolare attacchi informatici, insieme alle difficoltà riscontrate al momento dell'attivazione dei piani di continuità operativa delle TIC e dei piani di risposta e ripristino relativi alle TIC, nonché 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 informatici. Tali risultanze costituiscono la base per opportune revisioni delle relative componenti del quadro per la gestione dei rischi informatici di cui all'articolo 6, paragrafo 1.

4. Le entità finanziarie monitorano l'efficacia dell'attuazione della loro strategia di resilienza operativa digitale stabilita all'articolo 6, paragrafo 8. Tracciano l'evoluzione nel tempo dei rischi informatici, analizzano la frequenza, i tipi, le dimensioni e l'evoluzione degli incidenti connessi alle TIC, in particolare gli attacchi informatici e i relativi schemi, al fine di comprendere il livello di esposizione ai rischi informatici — segnatamente in relazione alle funzioni essenziali o importanti — e migliorare la maturità informatica e la preparazione dell'entità finanziaria.

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

6. Le entità finanziarie elaborano programmi di sensibilizzazione sulla sicurezza delle TIC nonché attività di formazione sulla resilienza operativa digitale, che rappresentano moduli obbligatori nei programmi di formazione del personale. Tali programmi e attività di formazione riguardano tutti i dipendenti e gli alti dirigenti, e presentano un livello di complessità commisurato all'ambito delle loro funzioni. Se del caso, le entità finanziarie includono anche i fornitori terzi di servizi TIC nei loro sistemi di formazione pertinenti, conformemente all'articolo 30, paragrafo 2, lettera i).

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

#### Articolo 14

### Comunicazione

1. All'interno del quadro per la gestione dei rischi informatici di cui all'articolo 6, paragrafo 1, le entità finanziarie predispongono piani di comunicazione delle crisi che consentano una divulgazione responsabile di informazioni riguardanti, almeno, gravi incidenti connessi alle TIC o vulnerabilità ai clienti e alle controparti nonché al pubblico, a seconda dei casi.

2. All'interno del quadro per la gestione dei rischi informatici, le entità finanziarie attuano politiche di comunicazione per il personale interno 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 informatici, in particolare il personale responsabile della risposta e del ripristino, e il personale che è necessario informare.

3. Nell'entità finanziaria vi è almeno una persona incaricata di attuare la strategia di comunicazione per gli incidenti connessi alle TIC e assolvere a tal fine la funzione di informazione al pubblico e ai media.

#### Articolo 15

### Ulteriore armonizzazione di strumenti, metodi, processi e politiche di gestione del rischio informatico

Tramite il comitato congiunto e in consultazione con l'Agenzia dell'Unione europea per la cibersicurezza (ENISA), le AEV elaborano progetti di norme tecniche di regolamentazione comuni al fine di:

- a) specificare ulteriori elementi da inserire nelle strategie, nelle politiche, nelle procedure, nei protocolli e negli strumenti in materia di sicurezza delle TIC di cui all'articolo 9, paragrafo 2, allo scopo di garantire la sicurezza delle reti, introdurre salvaguardie adeguate contro le intrusioni e l'uso improprio dei dati, preservare la disponibilità, l'autenticità, l'integrità e la riservatezza dei dati, inserire tecniche crittografiche e assicurare un'accurata e pronta trasmissione dei dati senza gravi perturbazioni né indebiti ritardi;
- b) sviluppare ulteriori componenti dei controlli sui diritti di gestione dell'accesso di cui all'articolo 9, 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 informatici mediante indicatori appropriati, compresi i modelli di utilizzo della rete, gli orari, l'attività informatica e i dispositivi sconosciuti;
- c) elaborare ulteriormente i meccanismi specificati all'articolo 10, paragrafo 1, in modo da consentire un'individuazione tempestiva delle attività anomale, e i criteri di cui all'articolo 10, paragrafo 2, per l'avvio dei processi di individuazione degli incidenti connessi alle TIC e di risposta agli stessi;

- d) specificare ulteriormente le componenti della politica di continuità operativa delle TIC di cui all'articolo 11, paragrafo 1;
- e) specificare ulteriormente i test sui piani di continuità operativa delle TIC di cui all'articolo 11, paragrafo 6, per garantire che tali test tengano debitamente conto degli scenari in cui la qualità dell'esercizio di una funzione essenziale 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 TIC e, se del caso, i rischi politici nelle giurisdizioni dei rispettivi fornitori;
- f) specificare ulteriormente le componenti dei piani di risposta e ripristino relativi alle TIC di cui all'articolo 11, paragrafo 3;
- g) specificare ulteriormente il contenuto e il formato della relazione sul riesame del quadro per la gestione dei rischi informatici di cui all'articolo 6, paragrafo 5.

All'atto dell'elaborazione di tali progetti di norme tecniche di regolamentazione, le AEV tengono conto delle dimensioni e del profilo di rischio complessivo dell'entità finanziaria, nonché della natura, della portata e della complessità dei suoi servizi, delle sue attività e delle sue operazioni, tenendo debitamente conto di eventuali caratteristiche specifiche derivanti dalla natura distinta delle attività nei diversi settori dei servizi finanziari.

Le AEV presentano tali progetti di norme tecniche di regolamentazione alla Commissione entro il 17 gennaio 2024.

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

## Articolo 16

### **Quadro semplificato per la gestione dei rischi informatici**

1. Gli articoli da 5 a 15 del presente regolamento non si applicano alle imprese di investimento piccole e non interconnesse e agli istituti di pagamento esentati a norma della direttiva (UE) 2015/2366; agli istituti esentati a norma della direttiva 2013/36/UE per i quali gli Stati membri hanno deciso di non applicare l'opzione di cui all'articolo 2, paragrafo 4, del presente regolamento; agli istituti di moneta elettronica esentati a norma della direttiva 2009/110/CE; e ai piccoli enti pensionistici aziendali o professionali.

Fermo restando il primo comma, le entità elencate al primo comma:

- a) pongono in essere e mantengono un solido e documentato quadro per la gestione dei rischi informatici che precisa i meccanismi e le misure finalizzate a una gestione rapida, efficiente e organica dei rischi informatici, anche ai fini della protezione delle pertinenti infrastrutture e componenti fisiche;
- b) monitorano costantemente la sicurezza e il funzionamento di tutti i sistemi di TIC;
- c) riducono al minimo l'impatto dei rischi informatici attraverso l'uso di sistemi, protocolli e strumenti di TIC solidi, resilienti e aggiornati e atti a supportare lo svolgimento delle loro attività e la fornitura di servizi e a proteggere adeguatamente la disponibilità, l'autenticità, l'integrità e la riservatezza dei dati nei sistemi informatici e di rete;
- d) provvedono a che le fonti di rischi informatici e le anomalie dei sistemi informatici e di rete siano tempestivamente individuate e rilevate e che gli incidenti connessi alle TIC siano trattati con rapidità;
- e) individuano le principali dipendenze da fornitori terzi di servizi TIC;
- f) garantiscono la continuità delle funzioni essenziali o importanti, attraverso piani di continuità operativa e misure di risposta e recupero, che comprendano almeno misure di back-up e ripristino;
- g) testano periodicamente i piani e le misure di cui alla lettera f) nonché l'efficacia dei controlli attuati in conformità delle lettere a) e c);



h) attuano, se del caso, le opportune conclusioni operative risultanti dai test di cui alla lettera g) e dall'analisi successiva all'incidente nel processo di valutazione dei rischi informatici ed elaborano, in funzione delle esigenze e del profilo dei rischi informatici, programmi di formazione e sensibilizzazione sulla sicurezza delle TIC per il personale e la dirigenza.

2. Il quadro per la gestione dei rischi informatici di cui al paragrafo 1, secondo comma, lettera a), è documentato e riesaminato periodicamente e al verificarsi di incidenti gravi connessi alle TIC conformemente alle istruzioni delle autorità di vigilanza. Il quadro è costantemente migliorato sulla base degli insegnamenti tratti dall'attuazione e dal monitoraggio. Su sua richiesta, è presentata all'autorità competente una relazione sul riesame del quadro per la gestione dei rischi informatici.

3. Tramite il comitato congiunto e in consultazione con l'ENISA, le AEV elaborano progetti di norme tecniche di regolamentazione comuni al fine di:

- a) specificare ulteriormente gli elementi da includere nel quadro per la gestione dei rischi informatici di cui al paragrafo 1, secondo comma, lettera a);
- b) specificare ulteriormente gli elementi relativi ai sistemi, ai protocolli e agli strumenti per ridurre al minimo l'impatto dei rischi informatici di cui al paragrafo 1, secondo comma, lettera c), allo scopo di garantire la sicurezza delle reti, introdurre salvaguardie adeguate contro le intrusioni e l'uso improprio dei dati e preservare la disponibilità, l'autenticità, l'integrità e la riservatezza dei dati;
- c) specificare ulteriormente le componenti dei piani di continuità operativa delle TIC di cui al paragrafo 1, secondo comma, lettera f);
- d) specificare ulteriormente le norme riguardanti i test sui piani di continuità operativa e assicurare l'efficacia dei controlli di cui al paragrafo 1, secondo comma, lettera g), e garantire che tali test tengano debitamente conto degli scenari in cui la qualità dell'esercizio di una funzione essenziale o importante si deteriora a un livello inaccettabile o viene meno;
- e) specificare ulteriormente il contenuto e il formato della relazione sul riesame del quadro per la gestione dei rischi informatici di cui al paragrafo 2.

All'atto dell'elaborazione di tali progetti di norme tecniche di regolamentazione, le AEV tengono conto delle dimensioni e del profilo di rischio complessivo dell'entità finanziaria, nonché della natura, della portata e della complessità dei suoi servizi, delle sue attività e delle sue operazioni.

Le AEV presentano tali progetti di norme tecniche di regolamentazione alla Commissione entro il 17 gennaio 2024.

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

### CAPO III

#### ***Gestione, classificazione e segnalazione degli incidenti informatici***

#### *Articolo 17*

#### **Processo di gestione degli incidenti connessi alle TIC**

1. Le entità finanziarie definiscono, stabiliscono e attuano un processo di gestione degli incidenti connessi alle TIC al fine di individuare, gestire e notificare tali incidenti.

2. Le entità finanziarie registrano tutti gli incidenti connessi alle TIC e le minacce informatiche significative. 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, documentare e affrontare le cause di fondo e prevenire il verificarsi di tali incidenti.

3. Il processo di gestione degli incidenti connessi alle TIC di cui al paragrafo 1:
  - a) predispone indicatori di allerta precoce;
  - b) stabilisce procedure per identificare, tracciare, registrare, categorizzare e classificare gli incidenti connessi alle TIC in base alla loro priorità e gravità e in base alla criticità dei servizi colpiti, conformemente ai criteri di cui all'articolo 18, paragrafo 1;
  - c) assegna i ruoli e le responsabilità che è necessario attivare per i diversi scenari e tipi di incidenti connessi alle TIC;
  - d) elabora piani per la comunicazione al personale, ai portatori di interessi esterni e ai mezzi di comunicazione conformemente all'articolo 14, nonché per la notifica ai clienti, per le procedure di attivazione dei livelli successivi di intervento, compresi i reclami dei clienti in materia di TIC, e per la comunicazione di informazioni alle entità finanziarie che agiscono da controparti, a seconda dei casi;
  - e) assicura la segnalazione almeno degli incidenti gravi connessi alle TIC agli alti dirigenti interessati e informa l'organo di gestione almeno in merito a detti incidenti, illustrandone l'impatto e la risposta e i controlli supplementari da introdurre;
  - f) stabilisce procedure di risposta agli incidenti connessi alle TIC per attenuarne l'impatto e garantisce tempestivamente l'operatività e la sicurezza dei servizi.

#### Articolo 18

##### **Classificazione degli incidenti connessi alle TIC e delle minacce informatiche**

1. Le entità finanziarie classificano gli incidenti connessi alle TIC e ne determinano l'impatto in base ai criteri seguenti:
  - a) il numero e/o la rilevanza di clienti o controparti finanziarie interessati e, ove applicabile, la quantità o il numero di transazioni interessate dall'incidente connesso alle TIC e il fatto che tale incidente abbia provocato o meno un impatto reputazionale;
  - b) la durata dell'incidente connesso alle TIC, compreso il periodo di inattività del servizio;
  - c) l'estensione geografica dell'incidente connesso alle TIC, con riferimento alle aree colpite, in particolare se interessa più di due Stati membri;
  - d) le perdite di dati derivanti dall'incidente connesso alle TIC, in relazione alla disponibilità, autenticità, integrità o riservatezza dei dati;
  - e) la criticità dei servizi colpiti, comprese le operazioni dell'entità finanziaria;
  - f) l'impatto economico dell'incidente connesso alle TIC — in particolare le perdite e i costi diretti e indiretti — in termini sia assoluti che relativi.
2. Le entità finanziarie classificano le minacce informatiche come significative in base alla criticità dei servizi a rischio, comprese le operazioni dell'entità finanziaria, il numero e/o la rilevanza di clienti o controparti finanziarie interessati e l'estensione geografica delle aree a rischio.
3. In consultazione con la BCE e l'ENISA, le AEV elaborano, tramite il comitato congiunto, progetti di norme tecniche di regolamentazione comuni che specificano ulteriormente gli aspetti seguenti:
  - a) i criteri di cui al paragrafo 1, comprese le soglie di rilevanza per la determinazione dei gravi incidenti TIC o, ove applicabile, dei gravi incidenti operativi o relativi alla sicurezza dei pagamenti, che sono oggetto dell'obbligo di segnalazione di cui all'articolo 19, paragrafo 1;
  - b) i criteri che le autorità competenti devono applicare per valutare la rilevanza degli gravi incidenti TIC o, ove applicabile, dei gravi incidenti operativi o relativi alla sicurezza dei pagamenti per le autorità competenti interessate in altri Stati membri, nonché i dettagli delle segnalazioni di incidenti gravi connessi alle TIC o, ove applicabile, di gravi incidenti operativi o di sicurezza dei pagamenti da condividere con altre autorità competenti ai sensi dell'articolo 19, paragrafi 6 e 7.
  - c) i criteri di cui al paragrafo 2 del presente articolo, comprese soglie di rilevanza elevate per la determinazione delle minacce informatiche significative.

4. All'atto dell'elaborazione dei progetti di norme tecniche di regolamentazione comuni di cui al paragrafo 3 del presente articolo, le AEV tengono conto dei criteri di cui all'articolo 4, paragrafo 2, come pure delle norme internazionali, degli orientamenti e delle specifiche elaborati e pubblicati dall'ENISA, tra cui, se del caso, le specifiche riguardanti altri settori economici. Ai fini dell'applicazione dei criteri di cui all'articolo 4, paragrafo 2, le AEV tengono debitamente conto della necessità delle microimprese e delle piccole e medie imprese di mobilitare risorse e capacità sufficienti per garantire una gestione rapida degli incidenti connessi alle TIC.

Le AEV presentano tali progetti di norme tecniche di regolamentazione comuni alla Commissione entro il 17 gennaio 2024.

Alla Commissione è delegato il potere di integrare il presente regolamento, adottando le norme tecniche di regolamentazione di cui al paragrafo 3 in conformità degli articoli da 0 a 14 dei regolamenti (UE) n. 1093/2010, (UE) n. 1094/2010 e (UE) n. 1095/2010.

#### Articolo 19

##### **Segnalazione dei gravi incidenti TIC e notifica volontaria delle minacce informatiche significative**

1. Le entità finanziarie segnalano gli gravi incidenti TIC all'autorità competente interessata di cui all'articolo 46 a norma del paragrafo 4 del presente articolo.

Se un'entità finanziaria è soggetta alla vigilanza di più di un'autorità nazionale competente di cui all'articolo 46, gli Stati membri designano un'unica autorità competente quale autorità competente interessata responsabile dell'espletamento delle funzioni e dei compiti di cui al presente articolo.

Gli enti creditizi classificati come significativi ai sensi dell'articolo 6, paragrafo 4, del regolamento (UE) n. 1024/2013 segnalano i gravi incidenti TIC all'autorità nazionale competente designata ai sensi dell'articolo 4 della direttiva 2013/36/UE, che trasmette immediatamente tale segnalazione alla BCE.

Ai fini del primo comma, le entità finanziarie redigono, dopo aver raccolto e analizzato tutte le informazioni pertinenti, la notifica iniziale e le relazioni di cui al paragrafo 4 del presente articolo utilizzando i modelli di cui all'articolo 20 e le trasmettono all'autorità competente. Qualora un impedimento tecnico non consenta la trasmissione della notifica iniziale utilizzando il modello, le entità finanziarie informano in merito l'autorità competente con mezzi alternativi.

La notifica iniziale e le relazioni di cui al paragrafo 4 contengono tutte le informazioni necessarie all'autorità competente per determinare la rilevanza dell'grave incidente TIC e valutarne i possibili impatti transfrontalieri.

Fatta salva la segnalazione a norma del primo comma da parte dell'entità finanziaria all'autorità competente interessata, gli Stati membri possono stabilire, in aggiunta, che alcune o tutte le entità finanziarie forniscano altresì la notifica iniziale e ciascuna relazione di cui al paragrafo 4 del presente articolo utilizzando i modelli di cui all'articolo 20 alle autorità competenti o ai gruppi di intervento per la sicurezza informatica in caso di incidente (*computer security incident response teams* — CSIRT) designati o istituiti a norma della direttiva (UE) 2022/2555.

2. Le entità finanziarie possono, su base volontaria, notificare le minacce informatiche significative all'autorità competente interessata 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 alle altre autorità pertinenti di cui al paragrafo 6.

Gli enti creditizi classificati come significativi ai sensi dell'articolo 6, paragrafo 4, del regolamento (UE) n. 1024/2013 possono notificare, su base volontaria, le minacce informatiche significative all'autorità nazionale competente, designata ai sensi dell'articolo 4 della direttiva 2013/36/UE, che trasmette immediatamente la notifica alla BCE.

Gli Stati membri possono stabilire che le entità finanziarie che procedono alla notifica su base volontaria e a norma del primo comma possano altresì trasmettere tale notifica ai CSIRT nazionali designati o istituiti a norma della direttiva (UE) 2022/2555.

3. Qualora si verifichi un grave incidente TIC che eserciti un impatto sugli interessi finanziari dei clienti, le entità finanziarie, senza indebito ritardo e non appena ne vengono a conoscenza, informano i loro clienti in merito a tale incidente e alle misure che sono state adottate per attenuare gli effetti avversi dell'incidente.

In caso di minaccia informatica significativa, le entità finanziarie, se del caso, informano i loro clienti potenzialmente interessati in merito alle opportune misure di protezione che i clienti stessi possono prendere in considerazione.

4. Entro i termini da fissare a norma dell'articolo 20, primo comma, lettera a), punto ii), le entità finanziarie trasmettono all'autorità competente interessata:

- a) una notifica iniziale;
- b) una relazione intermedia dopo la notifica iniziale di cui alla lettera a), non appena lo stato originario dell'incidente cambia in maniera significativa o il trattamento dell'grave incidente TIC cambia alla luce delle nuove informazioni disponibili, 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 che hanno dato origine all'incidente 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.

5. Ai sensi del presente articolo, le entità finanziarie possono esternalizzare, conformemente al diritto settoriale dell'Unione e nazionale, gli obblighi di segnalazione a un fornitore terzo di servizi. In caso di esternalizzazione, l'entità finanziaria rimane pienamente responsabile di espletare gli obblighi di segnalazione degli incidenti.

6. Dopo aver ricevuto la notifica iniziale e ciascuna delle relazioni di cui al paragrafo 4, l'autorità competente trasmette tempestivamente i dettagli dell'grave incidente TIC ai seguenti destinatari sulla base, ove applicabile, delle rispettive competenze:

- a) all'ABE, all'ESMA o all'EIOPA;
- b) alla BCE, qualora siano coinvolte le entità finanziarie di cui all'articolo 2, paragrafo 1, lettere a), b) e d);
- c) alle autorità competenti, ai punti di contatto unici o ai CSIRT designati o istituiti conformemente alla direttiva (UE) 2022/2555;
- d) alle autorità di risoluzione di cui all'articolo 3 della direttiva 2014/59/UE e al Comitato di risoluzione unico (SRB) per quanto riguarda le entità di cui all'articolo 7, paragrafo 2, del regolamento (UE) n. 806/2014 del Parlamento europeo e del Consiglio <sup>(37)</sup> nonché le entità e i gruppi di cui all'articolo 7, paragrafo 4, lettera b), e all'articolo 7, paragrafo 5, del regolamento (UE) n. 806/2014, qualora tali dettagli riguardino incidenti che comportano un rischio per le funzioni essenziali definite all'articolo 2, paragrafo 1, punto 35), della direttiva 2014/59/UE; e
- e) ad altre pertinenti autorità pubbliche ai sensi del diritto nazionale.

7. Una volta ricevute le informazioni conformemente al paragrafo 6, l'ABE, l'ESMA o l'EIOPA e la BCE, in consultazione con l'ENISA e in collaborazione con l'autorità competente interessata, valutano la pertinenza dell'grave incidente TIC rispetto alle autorità competenti in altri Stati membri. A seguito di tale valutazione, l'ABE, l'ESMA o l'EIOPA inviano una notifica al riguardo il prima possibile alle autorità competenti interessate in altri Stati membri. 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.

---

<sup>(37)</sup> 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).

8. La notifica che l'ESMA deve effettuare a norma del paragrafo 7 del presente articolo lascia impregiudicata la responsabilità dell'autorità competente di trasmettere urgentemente i dettagli dell'grave incidente TIC all'autorità pertinente dello Stato membro ospitante, laddove uno dei depositari centrali di titoli svolga una cospicua attività transfrontaliera nello Stato membro ospitante, laddove l'incidente grave connesso alle TIC possa comportare serie conseguenze per i mercati finanziari dello Stato membro ospitante e laddove vi siano accordi di cooperazione tra le autorità competenti in relazione alla vigilanza delle entità finanziarie.

## Articolo 20

### Armonizzazione dei modelli e dei contenuti per la segnalazione

In consultazione con l'ENISA e la BCE, le AEV, tramite il comitato congiunto, elaborano quanto segue:

- a) progetti di norme tecniche di regolamentazione comuni per:
    - i) stabilire il contenuto delle segnalazioni relative agli incidenti gravi connessi alle TIC al fine di rispecchiare i criteri di cui all'articolo 18, paragrafo 1, e integrare ulteriori elementi, ad esempio i dettagli per stabilire la rilevanza delle segnalazioni per gli altri Stati membri e se si tratti o meno di un grave incidente operativo o di sicurezza dei pagamenti;
    - ii) stabilire i termini della notifica iniziale e di ciascuna relazione di cui all'articolo 19, paragrafo 4;
    - iii) stabilire il contenuto della notifica per le minacce informatiche significative.
- All'atto dell'elaborazione di tali progetti di norme tecniche di regolamentazione, le AEV tengono conto delle dimensioni e del profilo di rischio complessivo dell'entità finanziaria, nonché della natura, della portata e della complessità dei suoi servizi, delle sue attività e delle sue operazioni, in particolare al fine di garantire che, ai fini della lettera a), punto ii) del presente comma, termini differenti possano rispecchiare, se del caso, alcune specificità dei settori finanziari, fatto salvo il mantenimento di un approccio coerente alla segnalazione degli incidenti connessi alle TIC a norma del presente regolamento e della direttiva (UE) 2022/2555. Se del caso, le AEV forniscono una giustificazione quando si discostano dagli approcci adottati nel contesto di tale direttiva;
- 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 grave incidente TIC e notificare una minaccia informatica significativa.

Le AEV trasmettono alla Commissione i progetti di norme tecniche di regolamentazione comuni di cui al primo comma, lettera a), e i progetti di norme tecniche di attuazione comuni di cui al primo comma, lettera b), entro il 17 luglio 2024.

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

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

## Articolo 21

### Centralizzazione delle segnalazioni 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 congiunta 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 congiunta di cui al paragrafo 1 comprende almeno gli elementi seguenti:
  - a) prerequisiti per l'istituzione di un polo UE unico;
  - b) benefici, limiti e rischi, compresi i rischi associati all'elevata concentrazione di informazioni sensibili;
  - c) la necessaria capacità di garantire l'interoperabilità rispetto ad altri sistemi di segnalazione pertinenti;
  - d) elementi della gestione operativa;
  - e) condizioni di adesione;
  - f) modalità tecniche per l'accesso al polo UE unico da parte delle entità finanziarie e le autorità nazionali competenti;
  - g) una valutazione preliminare dei costi finanziari sostenuti per l'istituzione della piattaforma operativa su cui dovrà fondarsi il polo UE unico, comprese le richieste competenze.
3. Le AEV presentano la relazione di cui al paragrafo 1 al Parlamento europeo, al Consiglio e alla Commissione entro il 17 gennaio 2025.

## Articolo 22

### **Riscontri forniti dalle autorità di vigilanza**

1. Fatti salvi il contributo tecnico, la consulenza o i rimedi e il successivo seguito dato che possono essere forniti, ove applicabile, conformemente al diritto nazionale, dai CSIRT ai sensi della direttiva (UE) 2022/2555, l'autorità competente, dopo aver ricevuto la notifica iniziale e ciascuna delle relazioni di cui all'articolo 19, paragrafo 4, ne accusa ricevuta e può, ove fattibile, fornire tempestivamente all'entità finanziaria riscontri pertinenti e proporzionali o orientamenti di alto livello, in particolare rendendo disponibili le informazioni e i dati pertinenti anonimizzati su minacce analoghe, e può discutere rimedi applicati a livello di entità finanziaria e metodi per ridurre al minimo e attenuare gli effetti avversi nel settore finanziario. Fatti salvi i riscontri ricevuti dalle autorità di vigilanza, le entità finanziarie restano pienamente responsabili del trattamento e delle conseguenze degli incidenti connessi alle TIC segnalati a norma dell'articolo 19, paragrafo 1.
2. Le AEV, tramite il comitato congiunto, riferiscono con frequenza annuale, sulla base di dati anonimizzati e aggregati, in merito agli incidenti gravi connessi alle TIC, i cui dettagli sono forniti dalle autorità competenti a norma dell'articolo 19, paragrafo 6, indicando almeno il numero degli incidenti gravi connessi alle TIC, la natura, l'impatto sulle operazioni delle entità finanziarie o dei clienti, i costi sostenuti e le azioni di riparazione adottate.

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 23

### **Incidenti operativi o relativi alla sicurezza dei pagamenti riguardanti enti creditizi, istituti di pagamento, prestatori di servizi di informazione sui conti e istituti di moneta elettronica**

I requisiti contenuti nel presente capo si applicano anche agli incidenti operativi o relativi alla sicurezza dei pagamenti ovvero ai gravi incidenti operativi o relativi alla sicurezza dei pagamenti allorché riguardano enti creditizi, istituti di pagamento, prestatori di servizi di informazione sui conti e istituti di moneta elettronica.

## CAPO IV

**Test di resilienza operativa digitale**

## Articolo 24

**Requisiti generali per lo svolgimento dei test di resilienza operativa digitale**

1. Allo scopo di valutare la preparazione alla gestione degli incidenti connessi alle TIC, di identificare punti deboli, carenze e lacune della resilienza operativa digitale e di attuare tempestivamente misure correttive, le entità finanziarie diverse dalle microimprese, tenuto conto dei criteri di cui all'articolo 4, paragrafo 2, 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 informatici di cui all'articolo 6.
2. Il programma di test di resilienza operativa digitale comprende una serie di valutazioni, test, metodologie, pratiche e strumenti da applicare conformemente agli articoli 25 e 26.
3. Nello svolgimento del programma di test di resilienza operativa digitale di cui al paragrafo 1 del presente articolo, le entità finanziarie, diverse dalle microimprese, adottano un approccio basato sul rischio che prende in considerazione i criteri di cui all'articolo 4, paragrafo 2, tenendo debitamente conto del mutevole contesto dei rischi informatici, di eventuali rischi specifici cui l'entità finanziaria interessata è o potrebbe essere esposta, della criticità dei patrimoni informativi e dei servizi forniti, nonché di qualsiasi altro fattore giudicato rilevante dall'entità finanziaria stessa.
4. Le entità finanziarie, diverse dalle microimprese, assicurano che i test siano svolti da soggetti indipendenti, interni o esterni. Se i test sono svolti da un soggetto incaricato dello svolgimento dei test interno, le entità finanziarie dedicano risorse sufficienti e garantiscono che siano evitati conflitti d'interessi durante le fasi di progettazione ed esecuzione del test.
5. Le entità finanziarie, diverse dalle microimprese, definiscono procedure e politiche per dare un ordine di priorità ai problemi riscontrati durante lo svolgimento dei test, per classificarli e porvi rimedio; stabiliscono inoltre metodologie di convalida interne per accertare che tutti i punti deboli, le carenze o le lacune che sono stati individuati siano pienamente affrontati.
6. Le entità finanziarie, diverse dalle microimprese, provvedono affinché, con cadenza almeno annuale, siano eseguiti test adeguati su tutti i sistemi e le applicazioni di TIC a supporto di funzioni essenziali o importanti.

## Articolo 25

**Test di strumenti e sistemi di TIC**

1. Il programma di test di resilienza operativa digitale di cui all'articolo 24 prevede, conformemente ai criteri di cui all'articolo 4, paragrafo 2, l'esecuzione di test adeguati, tra cui valutazione e scansione delle vulnerabilità, analisi open source, valutazioni della sicurezza delle reti, analisi delle carenze, esami della sicurezza fisica, questionari e soluzioni di scansione del software, esami del codice sorgente, ove fattibile, test basati su scenari, test di compatibilità, test di prestazione, test end-to-end e test di penetrazione.
2. I depositari centrali di titoli e le controparti centrali effettuano valutazioni della vulnerabilità prima di ciascun rilascio o nuovo rilascio di nuovi o già esistenti applicazioni e componenti infrastrutturali, e servizi TIC a supporto delle funzioni essenziali o importanti dell'entità finanziaria.
3. Le microimprese eseguono i test di cui al paragrafo 1 combinando un approccio basato sul rischio con una pianificazione strategica dei test relativi alle TIC, tenendo debitamente conto della necessità di mantenere un approccio equilibrato tra l'entità delle risorse e il tempo da assegnare ai test relativi alle TIC di cui al presente articolo, da un lato, e l'urgenza, il tipo di rischio, la criticità dei patrimoni informativi e dei servizi forniti nonché qualsiasi altro fattore rilevante, compresa la capacità dell'entità finanziaria di assumere rischi calcolati, dall'altro.

## Articolo 26

**Test avanzati di strumenti, sistemi e processi di TIC basati su test di penetrazione guidati dalla minaccia (TLPT)**

1. Le entità finanziarie, diverse dalle entità di cui all'articolo 16, paragrafo 1, primo comma, e dalle microimprese, che sono identificate conformemente al paragrafo 8, terzo comma, del presente articolo, effettuano test avanzati sotto forma di test di penetrazione basati su minacce con cadenza almeno triennale. Sulla base del profilo di rischio dell'entità finanziaria e tenuto conto delle circostanze operative, l'autorità competente può, se necessario, chiedere all'entità finanziaria di ridurre o aumentare tale frequenza.

2. Ciascun test di penetrazione guidato dalla minaccia riguarda alcune o tutte le funzioni essenziali o importanti dell'entità finanziaria ed è effettuato sui sistemi attivi di produzione a supporto di tali funzioni.

Le entità finanziarie identificano tutti i sistemi, i processi e le tecnologie TIC sottostanti a supporto delle funzioni essenziali o importanti e tutti i pertinenti servizi TIC, compresi quelli a supporto di funzioni essenziali o importanti che sono stati esternalizzate o appaltate a fornitori terzi di servizi TIC.

Le entità finanziarie valutano quali funzioni essenziali o importanti debbano essere interessate dai TLPT. Il risultato della valutazione determina il preciso ambito di applicazione dei TLPT ed è convalidato dalle autorità competenti.

3. Qualora i fornitori terzi di servizi TIC rientrino nell'ambito di applicazione dei TLPT, l'entità finanziaria adotta le misure e le salvaguardie necessarie per garantire la partecipazione di tali fornitori terzi di servizi TIC ai TLPT ed è sempre pienamente responsabile di garantire il rispetto del presente regolamento.

4. Fatto salvo il paragrafo 2, primo e secondo comma, laddove si ritiene ragionevolmente che la partecipazione di un fornitore terzo di servizi TIC ai TLPT di cui al paragrafo 3 possa avere un impatto avverso sulla qualità o la sicurezza dei servizi offerti dal fornitore terzo di servizi TIC a clienti che sono entità non rientranti nell'ambito di applicazione del presente regolamento, ovvero sulla riservatezza dei dati relativi a tali servizi, l'entità finanziaria e il fornitore terzo di servizi TIC possono concordare per iscritto che il fornitore terzo di servizi TIC stipuli direttamente accordi contrattuali con un soggetto incaricato dello svolgimento dei test esterno, allo scopo di condurre, sotto la direzione di un'entità finanziaria designata, un TLPT congiunto che coinvolga diverse entità finanziarie (*pooled testing*) a cui il fornitore terzo di servizi TIC fornisce tali servizi.

Detto test congiunto riguarda la pertinente gamma di servizi TIC a supporto delle funzioni essenziali o importanti appaltate dalle entità finanziarie al rispettivo fornitore terzo di servizi TIC. I test congiunti sono considerati TLPT effettuati dalle entità finanziarie che partecipano ai test congiunti.

Il numero di entità finanziarie che partecipano ai test congiunti è debitamente calibrato tenendo conto della complessità e dei tipi di servizi interessati.

5. Le entità finanziarie, cooperando con i fornitori terzi di servizi TIC e altre parti coinvolte, inclusi i soggetti incaricati dello svolgimento dei test ma escluse le autorità competenti, applicano efficaci controlli di gestione del rischio per attenuare i rischi di potenziali impatti sui dati, danni alle attività e perturbazioni delle funzioni essenziali o importanti, delle operazioni o dei servizi delle entità finanziarie, delle loro controparti o del settore finanziario.

6. Alla fine dei test, dopo che le relazioni e i piani correttivi siano stati concordati, l'entità finanziaria e, ove applicabile, i soggetti incaricati dello svolgimento dei test esterni trasmettono all'autorità, designata conformemente al paragrafo 9 o 10, una sintesi delle pertinenti risultanze, i piani correttivi e la documentazione attestante che i TLPT sono stati svolti conformemente ai requisiti.

7. Le autorità forniscono alle entità finanziarie un attestato che conferma che i test sono stati svolti conformemente ai requisiti, come si evince dalla documentazione, in modo da consentire il riconoscimento reciproco dei TLPT tra le autorità competenti. L'entità finanziaria notifica all'autorità competente interessata l'attestato, la sintesi delle pertinenti risultanze e i piani correttivi.



Fatto salvo tale attestato, le entità finanziarie rimangono sempre pienamente responsabili degli impatti dei test di cui al paragrafo 4.

8. Per l'effettuazione dei TLPT, le entità finanziarie si avvalgono di soggetti incaricati dello svolgimento dei test in conformità dell'articolo 27. Quando ricorrono a soggetti incaricati dello svolgimento dei test interni per l'effettuazione di TLPT, le entità finanziarie si avvalgono di un soggetto incaricato dello svolgimento dei test esterno ogni tre test.

Gli enti creditizi classificati come significativi a norma dell'articolo 6, paragrafo 4, del regolamento (UE) n. 1024/2013, ricorrono esclusivamente a soggetto incaricato dello svolgimento dei test esterni conformemente all'articolo 27, paragrafo 1, lettere da a) a e).

Le autorità competenti identificano le entità finanziarie che hanno l'obbligo di svolgere TLPT tenendo conto dei criteri di cui all'articolo 4, paragrafo 2, sulla base della valutazione degli elementi seguenti:

- a) i fattori correlati all'impatto, in particolare la portata dell'impatto sul settore finanziario 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 di Unione o nazionale, a seconda dei casi;
- c) lo specifico profilo dei rischi informatici, il livello di maturità delle TIC dell'entità finanziaria o le caratteristiche tecnologiche in questione.

9. Gli Stati membri possono designare un'autorità pubblica unica nel settore finanziario responsabile delle questioni relative ai TLPT nel settore finanziario a livello nazionale e le affidano tutte le competenze e tutti i compiti a tal fine.

10. In assenza di una designazione a norma del paragrafo 9 del presente articolo e fatto salvo il potere di identificare le entità finanziarie tenute a svolgere TLPT, un'autorità competente può delegare l'esercizio di alcuni o di tutti i compiti di cui al presente articolo e all'articolo 27 a un'altra autorità nazionale nel settore finanziario.

11. Di concerto con la BCE, le AEV elaborano progetti di norme tecniche di regolamentazione comuni conformemente al quadro di riferimento TIBER-EU al fine di specificare ulteriormente quanto segue:

- a) i criteri utilizzati ai fini dell'applicazione del paragrafo 8, secondo comma;
- b) i requisiti e le norme che disciplinano il ricorso a soggetto incaricato dello svolgimento dei test interni;
- c) i requisiti concernenti:
  - i) l'ambito dei TLPT di cui al paragrafo 2;
  - ii) l'approccio e la metodologia da seguire per i test in ciascuna fase del relativo processo;
  - iii) i risultati, la chiusura e le fasi correttive dei test;
- d) il tipo di cooperazione di vigilanza e altri tipi di cooperazione pertinenti necessari per svolgere i TLPT e per la facilitazione del riconoscimento reciproco di tali test, nel contesto di entità finanziarie che operano in più di uno Stato membro, al fine di 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.

All'atto dell'elaborazione di tali progetti di norme tecniche di regolamentazione, le AEV tengono debitamente conto di eventuali caratteristiche specifiche derivanti dalla natura distinta delle attività nei diversi settori dei servizi finanziari.

Le AEV presentano tali progetti di norme tecniche di regolamentazione alla Commissione entro il 17 luglio 2024.

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

*Articolo 27***Requisiti per i soggetti incaricati dello svolgimento dei test per lo svolgimento dei TLPT**

1. Per lo svolgimento dei test di penetrazione basati su minacce, le entità finanziarie ricorrono unicamente a soggetto incaricato dello svolgimento dei test 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 analisi delle minacce, dei test di penetrazione e dei test red team;
  - c) siano certificati da un ente di accreditamento in uno Stato membro o rispettino codici formali di condotta o quadri etici;
  - d) forniscano una garanzia indipendente o una relazione di audit concernente la solida gestione dei rischi derivanti dallo svolgimento di TLPT, comprese la dovuta 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.
2. Quando ricorrono a soggetto incaricato dello svolgimento dei test interni, le entità finanziarie devono provvedere affinché, oltre all'obbligo di cui al paragrafo 1, siano soddisfatte le condizioni seguenti:
  - a) tale ricorso è stato approvato dall'autorità competente interessata o dall'autorità pubblica unica designata conformemente all'articolo 26, paragrafi 9 e 10;
  - b) l'autorità competente interessata ha verificato che l'entità finanziaria dispone di risorse dedicate sufficienti e che essa ha garantito che siano evitati conflitti d'interessi durante le fasi di progettazione ed esecuzione del test; e
  - c) il soggetto che fornisce analisi delle minacce è esterno all'entità finanziaria.
3. Le entità finanziarie garantiscono che i contratti conclusi con i soggetti incaricati dello svolgimento dei test esterni prevedano una solida gestione dei risultati dei TLPT e che qualsiasi trattamento dei dati, comprese la generazione, la conservazione, l'aggregazione, l'elaborazione, la segnalazione, la comunicazione o la distruzione, non comporti rischi per l'entità finanziaria.

*CAPO V****Gestione dei rischi informatici derivanti da terzi****Sezione I***Principi fondamentali di una solida gestione dei rischi informatici derivanti da terzi***Articolo 28***Principi generali**

1. Le entità finanziarie gestiscono i rischi informatici derivanti da terzi quali componenti integranti dei rischi informatici nel contesto del proprio quadro per la gestione di detti rischi di cui all'articolo 6, paragrafo 1, e conformemente ai principi indicati di seguito:
  - a) le entità finanziarie che hanno stipulato accordi contrattuali per l'utilizzo di servizi 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 normativa applicabile in materia di servizi finanziari;

- b) la gestione dei rischi informatici derivanti da terzi da parte delle entità finanziarie si svolge nel rispetto del principio di proporzionalità, tenendo conto:
  - i) della natura, della portata, della complessità e dell'importanza delle dipendenze connesse alle TIC;
  - ii) dei rischi derivanti dagli accordi contrattuali per l'utilizzo di servizi TIC conclusi con fornitori terzi di servizi TIC, tenendo conto della criticità o dell'importanza dei rispettivi servizi, processi o funzioni e del potenziale impatto sulla continuità e la disponibilità delle attività e dei servizi finanziari a livello individuale e di gruppo.

2. Nel contesto del quadro per la gestione dei rischi informatici TIC, le entità finanziarie diverse dalle entità di cui all'articolo 16, paragrafo 1, primo comma, e dalle microimprese adottano e riesaminano periodicamente una strategia per i rischi informatici derivanti da terzi, tenendo conto della strategia basata su una varietà di fornitori di cui all'articolo 6, paragrafo 9, ove applicabile. Tale strategia comprende una politica per l'utilizzo dei servizi TIC a supporto di funzioni essenziali o importanti prestati da fornitori terzi e si applica su base individuale e, se del caso, su base subconsolidata e consolidata. Sulla base di una valutazione del profilo di rischio complessivo dell'entità finanziaria e della portata e della complessità dei servizi operativi, l'organo di gestione riesamina periodicamente i rischi individuati in relazione agli accordi contrattuali per l'utilizzo di servizi TIC a supporto di funzioni essenziali o importanti.

3. Nel contesto del quadro per la gestione dei rischi informatici, 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 TIC prestati da fornitori terzi.

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

Le entità finanziarie comunicano almeno una volta all'anno alle autorità competenti il numero di nuovi accordi per l'utilizzo di servizi TIC, le categorie di fornitori terzi di servizi TIC, il tipo di accordi contrattuali e le funzioni e i servizi TIC 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 in merito a eventuali accordi contrattuali previsti per l'utilizzo di servizi TIC a supporto di funzioni essenziali o importanti, nonché del momento in cui una funzione diventa essenziale o importante.

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

- a) valutano se l'accordo contrattuale riguardi l'utilizzo di servizi TIC a supporto di una funzione essenziale 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 tale accordo contrattuale possa aggravare il rischio di concentrazione delle TIC di cui all'articolo 29;
- d) effettuano controlli di dovuta diligenza (*due diligence*) sui potenziali fornitori terzi di servizi TIC e ne garantiscono l'idoneità lungo tutto il processo di selezione e valutazione;
- e) individuano e valutano i conflitti d'interessi che possano derivare dall'accordo contrattuale.

5. Le entità finanziarie possono stipulare accordi contrattuali soltanto con fornitori terzi di servizi TIC che soddisfano standard appropriati in materia di sicurezza delle informazioni. Laddove tali accordi contrattuali riguardino funzioni essenziali o importanti, le entità finanziarie, prima di concludere detti accordi, prendono in debita considerazione l'utilizzo da parte dei fornitori terzi di servizi TIC degli standard di qualità più aggiornati ed elevati in materia di sicurezza delle informazioni.

6. Nell'esercizio dei diritti di accesso, ispezione e audit nei confronti del fornitore terzo di servizi TIC, le entità finanziarie predeterminano, sulla base di un approccio basato sul rischio, la frequenza delle verifiche di audit e delle ispezioni nonché i settori da sottoporre ad audit, aderendo a standard di audit comunemente accettate in conformità di eventuali indicazioni di vigilanza sull'uso e l'integrazione di tali standard di audit.

Laddove gli accordi contrattuali conclusi con fornitori terzi di servizi TIC per l'utilizzo di servizi TIC comportino un'elevata complessità tecnica, l'entità finanziaria verifica che i revisori, indipendentemente dal fatto che siano revisori interni o esterni o siano un gruppo di revisori, possiedano competenze e conoscenze adeguate per svolgere efficacemente gli audit e le valutazioni del caso.

7. Le entità finanziarie stabiliscono clausole che consentano la risoluzione degli accordi contrattuali per l'utilizzo di servizi TIC in una qualsiasi delle circostanze seguenti:

- a) rilevante violazione, da parte del fornitore terzo di servizi TIC, di leggi, regolamenti o condizioni contrattuali applicabili;
- b) circostanze, identificate nel corso del monitoraggio dei rischi informatici 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 TIC;
- c) punti deboli del fornitore terzo di servizi TIC emersi riguardo alla sua gestione complessiva dei rischi informatici e, in particolare, nel modo in cui il fornitore garantisce la disponibilità, autenticità, integrità e riservatezza dei dati, siano essi dati personali o altrimenti sensibili, oppure dei dati non personali;
- d) laddove l'autorità competente non sia più in grado di vigilare efficacemente sull'entità finanziaria per via delle condizioni dell'accordo contrattuale in questione o delle circostanze ivi afferenti.

8. Per i servizi TIC a supporto di funzioni essenziali o importanti, le entità finanziarie predispongono strategie di uscita. Tali strategie tengono conto dei rischi che possono emergere a livello dei fornitori terzi di servizi TIC, in particolare possibili disfunzioni dei fornitori stessi, il deterioramento della qualità dei servizi TIC forniti, una perturbazione dell'attività commerciale conseguente a una fornitura di servizi TIC inadeguata o carente, oppure gravi rischi connessi all'adeguatezza e alla continuità dell'esercizio del rispettivo servizio TIC oppure la risoluzione di accordi contrattuali con fornitori terzi di servizi TIC in una delle circostanze di cui al paragrafo 7.

Le entità finanziarie garantiscono di poter porre termine agli accordi contrattuali senza:

- a) perturbare le proprie attività commerciali;
- b) limitare il rispetto dei requisiti normativi;
- c) pregiudicare la continuità e la qualità dei servizi forniti ai clienti.

I piani di uscita sono esaustivi, documentati e, conformemente ai criteri di cui all'articolo 4, paragrafo 2, sottoposti a test adeguati e riesaminati periodicamente.

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

Le entità finanziarie dispongono di misure di emergenza idonee per mantenere la continuità operativa qualora si verificano le circostanze di cui al primo comma.

9. Le AEV, tramite il comitato congiunto, elaborano progetti di norme tecniche di attuazione per definire modelli standard in relazione al registro delle informazioni di cui al paragrafo 3, comprese le informazioni comuni a tutti gli accordi contrattuali per l'utilizzo di servizi TIC. Le AEV presentano tali progetti di norme tecniche di attuazione alla Commissione entro il 17 gennaio 2024.

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

10. Le AEV, tramite il comitato congiunto, elaborano progetti di norme tecniche di regolamentazione per precisare ulteriormente il contenuto dettagliato della politica di cui al paragrafo 2, in relazione agli accordi contrattuali per l'utilizzo di servizi TIC a supporto di funzioni essenziali o importanti prestati da fornitori terzi di servizi TIC.

All'atto dell'elaborazione di tali progetti di norme tecniche di regolamentazione, le AEV tengono conto delle dimensioni e del profilo di rischio complessivo dell'entità finanziaria, nonché della natura, della portata e della complessità dei suoi servizi, delle sue attività e delle sue operazioni. Le AEV presentano detti progetti di norme tecniche di regolamentazione alla Commissione 17 gennaio 2024.

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

#### *Articolo 29*

#### **Valutazione preliminare del rischio di concentrazione delle TIC a livello di entità**

1. All'atto dell'identificazione e della valutazione dei rischi di cui all'articolo 28, paragrafo 4, lettera c), le entità finanziarie tengono conto altresì dell'eventualità che la prevista conclusione di un accordo contrattuale relativo a servizi TIC a supporto di funzioni essenziali o importanti possa avere una delle seguenti conseguenze:

- a) la conclusione di un contratto con un fornitore terzo di servizi TIC non facilmente sostituibile; o
- b) la presenza di molteplici accordi contrattuali relativi alla prestazione di servizi TIC a supporto di funzioni essenziali 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 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 gli accordi contrattuali per l'utilizzo di servizi TIC a supporto di funzioni essenziali o importanti prevedano la possibilità che un fornitore terzo di servizi TIC subappalti a sua volta servizi TIC a supporto di una funzione essenziale o importante ad altri fornitori terzi di servizi TIC, le entità finanziarie vagliano i benefici e i rischi che possono derivare da tale subappalto, in particolare nel caso di un subappaltatore di TIC stabilito in un paese terzo.

Qualora gli accordi contrattuali riguardino servizi TIC a supporto delle funzioni essenziali o importanti, le entità finanziarie tengono in debita considerazione le disposizioni del diritto fallimentare applicabili in caso di fallimento del fornitore terzo di servizi TIC come pure eventuali restrizioni relative all'urgente ripristino dei dati dell'entità finanziaria.

Qualora gli accordi contrattuali per l'utilizzo di servizi TIC a supporto di funzioni essenziali o importanti siano conclusi con un fornitore terzo di servizi TIC stabilito in un paese terzo, le entità finanziarie, in aggiunta alle considerazioni di cui al secondo comma, tengono conto altresì del rispetto delle norme dell'UE sulla protezione dei dati e dell'effettiva applicazione della legge in tale paese terzo.

Qualora gli accordi contrattuali per l'utilizzo di servizi TIC a supporto di funzioni essenziali o importanti prevedano un subappalto, le entità finanziarie valutano se e come catene di subappalti potenzialmente lunghe e complesse possano incidere sulla loro capacità di monitorare pienamente le funzioni appaltate e sulla capacità dell'autorità competente di vigilare efficacemente, a tal proposito, sull'entità finanziaria.

*Articolo 30***Principali disposizioni contrattuali**

1. I diritti e gli obblighi dell'entità finanziaria e del fornitore terzo di servizi TIC sono attribuiti chiaramente e definiti per iscritto. Il testo integrale del contratto comprende gli accordi sul livello dei servizi ed è contenuto in un documento scritto disponibile alle parti in formato cartaceo oppure in un documento in altro formato scaricabile, durevole e accessibile.
2. Gli accordi contrattuali per l'utilizzo di servizi TIC comprendono almeno gli elementi seguenti:
  - a) la descrizione chiara e completa di tutte le funzioni che il fornitore terzo di servizi TIC deve svolgere e tutti i servizi TIC che deve prestare, comprese l'indicazione dell'eventuale autorizzazione a subappaltare un servizio TIC a sostegno di una funzione essenziale 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 svolgere le funzioni e prestare i servizi 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 TIC, di segnalare in anticipo all'entità finanziaria l'intenzione di cambiare tale o tali località;
  - c) le disposizioni in materia di disponibilità, autenticità, integrità e riservatezza in relazione alla protezione dei dati, compresi i dati personali;
  - d) 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 TIC o in caso di risoluzione degli accordi commerciali;
  - e) le descrizioni dei livelli di servizio, compresi relativi aggiornamenti e revisioni;
  - f) l'obbligo per il fornitore terzo di servizi TIC di prestare assistenza all'entità finanziaria senza costi aggiuntivi o a un costo stabilito ex ante, qualora si verifichi un incidente connesso alle TIC relativo al servizio TIC fornito all'entità finanziaria;
  - g) l'obbligo per il fornitore terzo di servizi di TIC di operare senza riserve con le autorità competenti e con le autorità di risoluzione dell'entità finanziaria, comprese le persone da queste nominate;
  - h) i diritti di risoluzione e il relativo termine minimo di preavviso per la risoluzione degli accordi contrattuali, conformemente alle attese delle autorità competenti e delle autorità di risoluzione;
  - i) le condizioni riguardanti la partecipazione dei fornitori terzi di servizi TIC ai programmi di sensibilizzazione sulla sicurezza delle TIC e alle attività di formazione sulla resilienza operativa digitale delle entità finanziarie conformemente all'articolo 13, paragrafo 6.
3. Gli accordi contrattuali per l'utilizzo di servizi TIC a supporto di funzioni essenziali o importanti comprendono, in aggiunta agli elementi di cui al paragrafo 2, almeno quanto segue:
  - a) la descrizione completa dei livelli di servizio, comprendente i relativi aggiornamenti e revisioni con precisi obiettivi quantitativi e qualitativi, in termini di prestazioni, nell'ambito dei livelli di servizio concordati, in modo da consentire un monitoraggio efficace da parte dell'entità finanziaria dei servizi TIC e l'applicazione, senza indebito ritardo, di opportune azioni correttive qualora i livelli di servizio concordati non siano rispettati;
  - b) termini di preavviso e obblighi di segnalazione per il fornitore terzo di servizi TIC nei confronti dell'entità finanziaria, tra cui la notifica di eventuali sviluppi che potrebbero esercitare un impatto significativo sulla capacità del fornitore terzo di servizi TIC di prestare servizi a supporto di funzioni essenziali o importanti efficacemente, in linea con i livelli di servizio concordati;
  - c) l'obbligo per il fornitore terzo di servizi 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 sicurezza per la fornitura dei servizi da parte dell'entità finanziaria, in linea con il proprio quadro normativo;
  - d) l'obbligo per il fornitore terzo di servizi TIC di partecipare e cooperare pienamente al TLPT dell'entità finanziaria di cui agli articoli 26 e 27;
  - e) il diritto di monitorare costantemente le prestazioni del fornitore terzo di servizi TIC, che comporta quanto segue:

- i) diritti incondizionati di accesso, ispezione e audit da parte dell'entità finanziaria — o di un terzo designato a tal fine — e dell'autorità competente nonché il diritto di ottenere copia della documentazione pertinente in loco, se di importanza critica per le operazioni del fornitore terzo di servizi TIC, il cui effettivo esercizio non sia impedito o limitato da altri accordi contrattuali o politiche di attuazione;
  - ii) il diritto di concordare livelli di garanzia alternativi, qualora siano interessati i diritti di altri clienti;
  - iii) l'obbligo per il fornitore terzo di servizi TIC di cooperare senza riserve nel corso delle ispezioni e degli audit in loco svolti dalle autorità competenti, dall'autorità di sorveglianza capofila, dall'entità finanziaria o da un terzo designato; e
  - iv) l'obbligo di fornire dettagli sull'ambito di applicazione, sulle procedure da seguire e sulla frequenza di tali ispezioni e audit;
- f) le strategie di uscita, in particolare la definizione di un adeguato periodo di transizione obbligatorio:
- i) durante il quale il fornitore terzo di servizi TIC continuerà a prestare i suoi servizi TIC o 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;
  - ii) che permetta all'entità finanziaria di migrare verso un altro fornitore terzo di servizi TIC oppure di adottare soluzioni interne coerenti con la complessità del servizio prestato.

In deroga alla lettera e), il fornitore terzo di servizi TIC e l'entità finanziaria che è una microimpresa possono convenire che i diritti di accesso, ispezione e audit dell'entità finanziaria possano essere delegati a un terzo indipendente, nominato dal fornitore terzo di servizi TIC, e che l'entità finanziaria possa richiedere in qualsiasi momento al terzo informazioni e garanzie sulle prestazioni del fornitore terzo di servizi TIC.

4. All'atto della negoziazione degli accordi contrattuali, le entità finanziarie e i fornitori terzi di servizi TIC prendono in considerazione il ricorso a clausole contrattuali standard elaborate dalle autorità pubbliche per servizi specifici.

5. Le AEV, tramite il comitato congiunto, elaborano progetti di norme tecniche di regolamentazione per specificare ulteriormente gli elementi di cui al paragrafo 2, lettera a), che l'entità finanziaria deve determinare e valutare quando subappalta servizi TIC a supporto di funzioni essenziali o importanti.

All'atto dell'elaborazione di tali progetti di norme tecniche di regolamentazione, le AEV tengono conto delle dimensioni e del profilo di rischio complessivo dell'entità finanziaria, nonché della natura, della portata e della complessità dei suoi servizi, delle sue attività e delle sue operazioni.

Le AEV presentano tali progetti di norme tecniche di regolamentazione alla Commissione entro il 17 luglio 2024.

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

## Sezione II

### **Quadro di sorveglianza dei fornitori terzi critici di servizi TIC**

#### *Articolo 31*

#### **Designazione dei fornitori terzi critici di servizi TIC**

1. Le AEV, tramite il comitato congiunto e su raccomandazione del forum di sorveglianza istituito ai sensi dell'articolo 32, paragrafo 1:

- a) designano i fornitori terzi di servizi TIC che sono critici per le entità finanziarie, a seguito di una valutazione che tiene conto dei criteri di cui al paragrafo 2;

- b) nominano quale autorità di sorveglianza capofila di ciascun fornitore terzo critico di servizi TIC la AEV che è responsabile, a norma dei regolamenti (UE) n. 1093/2010, (UE) n. 1094/2010 o (UE) n. 1095/2010, delle entità finanziarie che possiedono complessivamente la quota maggiore delle attività totali rispetto al valore delle attività totali di tutte le entità finanziarie che utilizzano i servizi del pertinente fornitore terzo critico di servizi TIC, secondo quanto risulta dalla somma dei singoli bilanci di quelle entità finanziarie.

2. La designazione di cui al paragrafo 1, lettera a), si fonda su tutti i criteri indicati di seguito in relazione ai servizi TIC prestati da un fornitore terzo di servizi TIC:

- a) l'impatto sistemico sulla stabilità, la continuità o la qualità della fornitura di servizi finanziari qualora il fornitore terzo di servizi 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 e del valore totale delle attività delle entità finanziarie cui quel fornitore terzo di servizi TIC presta servizi;
- b) il carattere sistemico o l'importanza delle entità finanziarie che dipendono da quel fornitore terzo di servizi 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 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 TIC in rapporto alle funzioni essenziali o importanti delle entità finanziarie che in ultima analisi coinvolgono quel medesimo fornitore terzo di servizi 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 TIC, prendendo in considerazione i parametri seguenti:
- i) la mancanza di alternative reali, anche parziali, dovuta al limitato numero di fornitori terzi di servizi TIC attivi su un mercato specifico, alla quota di mercato del fornitore terzo di servizi 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 TIC;
- ii) difficoltà inerenti alla migrazione, totale o parziale, dei dati e dei carichi di lavoro dal fornitore terzo di servizi TIC pertinente a un altro, a causa dei cospicui costi finanziari, del tempo o di altre risorse che possono essere necessarie per il processo di migrazione, oppure dei maggiori rischi informatici o di altri rischi operativi cui l'entità finanziaria può esporsi a causa di tale migrazione.

3. Laddove il fornitore terzo di servizi TIC appartenga a un gruppo, i criteri di cui al paragrafo 2 sono presi in considerazione in relazione ai servizi TIC prestati dal gruppo nel suo insieme.

4. I fornitori terzi critici di servizi TIC che fanno parte di un gruppo designano una persona giuridica come punto di coordinamento per garantire un'adeguata rappresentanza e la comunicazione con l'autorità di sorveglianza capofila.

5. L'autorità di sorveglianza capofila informa il fornitore terzo di servizi TIC in merito all'esito della valutazione che ha portato alla designazione di cui al paragrafo 1, lettera a). Entro sei settimane dalla data della notifica, il fornitore terzo di servizi TIC può presentare all'autorità di sorveglianza capofila una dichiarazione motivata contenente tutte le informazioni pertinenti ai fini della valutazione. L'autorità di sorveglianza capofila esamina la dichiarazione motivata e può richiedere ulteriori informazioni da presentare entro 30 giorni di calendario dal ricevimento di detta dichiarazione.



Dopo aver designato un fornitore terzo di servizi TIC come critico, le AEV, tramite il comitato congiunto, notificano al fornitore terzo di servizi TIC tale designazione e la data di inizio a partire dalla quale sarà effettivamente soggetto ad attività di sorveglianza. La data di inizio è fissata a non più di un mese dall'avvenuta notifica. Il fornitore terzo di servizi TIC notifica alle entità finanziarie a cui presta servizi la propria designazione come critico.

6. Alla Commissione è conferito il potere di adottare un atto delegato, conformemente all'articolo 57, per integrare il presente regolamento specificando ulteriormente i criteri di cui al paragrafo 2 del presente articolo, entro il 17 luglio 2024.

7. 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 6.

8. Il meccanismo di designazione di cui al paragrafo 1, lettera a), non si applica:

- i) alle entità finanziarie che forniscono servizi TIC ad altre entità finanziarie;
- ii) ai fornitori terzi di servizi 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;
- iii) ai fornitori intragruppo di servizi TIC;
- iv) ai fornitori terzi di servizi TIC che prestano servizi TIC unicamente in uno Stato membro a entità finanziarie attive solo in tale Stato membro.

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

10. Ai fini del paragrafo 1, lettera a), le autorità competenti, con cadenza annuale e in forma aggregata, trasmettono le relazioni di cui all'articolo 28, paragrafo 3, terzo comma, al forum di sorveglianza istituito ai sensi dell'articolo 32. Il forum di sorveglianza valuta la dipendenza delle entità finanziarie da terzi nel settore delle TIC sulla base delle informazioni ricevute dalle autorità competenti.

11. I fornitori terzi di servizi TIC che non sono inseriti nell'elenco di cui al paragrafo 9 possono chiedere di essere designati come critici conformemente al paragrafo 1, lettera a).

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

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

12. Le entità finanziarie ricorrono ai servizi di un fornitore terzo di servizi TIC stabilito in un paese terzo e che è stato designato come critico conformemente al paragrafo 1, lettera a), soltanto se detto fornitore ha istituito un'impresa figlia nell'Unione entro 12 mesi dalla designazione.

13. Il fornitore terzo critico di servizi TIC di cui al paragrafo 12 notifica all'autorità di sorveglianza capofila eventuali cambiamenti nella struttura gestionale dell'impresa istituita nell'Unione.

## Articolo 32

### Struttura del quadro di sorveglianza

1. Il comitato congiunto, in conformità dell'articolo 57, paragrafo 1, dei regolamenti (UE) n. 1093/2010, (UE) n. 1094/2010 o (UE) n. 1095/2010, istituisce il forum di sorveglianza come sottocomitato incaricato di coadiuvare il lavoro del comitato congiunto e dell'autorità di sorveglianza capofila di cui all'articolo 31, paragrafo 1, lettera b), per quanto concerne i rischi informatici derivanti da terzi in tutti i settori finanziari. Il forum di sorveglianza prepara i progetti di posizioni comuni e atti comuni del comitato congiunto in tale ambito.

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

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

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

4. Il forum di sorveglianza è composto da:

- a) i presidenti delle AEV;
- b) un rappresentante di alto livello del personale in servizio dell'autorità competente interessata di cui all'articolo 46 di ciascuno Stato membro;
- c) i direttori esecutivi di ciascuna AEV e un rappresentante della Commissione, del CERS, della BCE e dell'ENISA in qualità di osservatori;
- d) se del caso, un rappresentante supplementare di un'autorità competente di cui all'articolo 46 di ciascuno Stato membro in qualità di osservatore;
- e) ove applicabile, un rappresentante delle autorità competenti designate o istituite in conformità della direttiva (UE) 2022/2555 responsabile della vigilanza di un soggetto essenziale o importante ai sensi di tale direttiva, che è stato designato come un fornitore terzo di servizi TIC critici in qualità di osservatore.

Il forum di sorveglianza può, se del caso, chiedere il parere di esperti indipendenti nominati a norma del paragrafo 6.

5. Ciascuno Stato membro designa l'autorità competente interessata il cui membro del personale è il rappresentante di alto livello di cui al paragrafo 4, primo comma, lettera b), e ne informa l'autorità di sorveglianza capofila.

Le AEV pubblicano sul loro sito web l'elenco dei rappresentanti di alto livello dell'attuale personale della pertinente autorità competente designati dagli Stati membri.

6. Gli esperti indipendenti di cui al paragrafo 4, secondo comma, sono nominati dal forum di sorveglianza e provengono da un gruppo di esperti selezionati al termine di una procedura di candidatura pubblica e trasparente. Gli esperti indipendenti sono nominati sulla base dell'esperienza maturata in settori quali la stabilità finanziaria, la resilienza operativa digitale e le questioni di sicurezza delle TIC.

Agiscono 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.

7. Ai sensi dell'articolo 16 dei regolamenti (UE) n. 1093/2010, (UE) n. 1094/2010 e (UE) n. 1095/2010, le AEV, entro il 17 luglio 2024, formulano, ai fini della presente sezione, orientamenti sulla cooperazione tra le AEV e le autorità competenti concernenti le procedure e le condizioni dettagliate per la ripartizione e l'esecuzione dei compiti tra le autorità competenti e le AEV, nonché forniscono dettagli sugli scambi di informazioni necessari alle autorità competenti per garantire il seguito da dare alle raccomandazioni a norma dell'articolo 35, paragrafo 1, lettera d) rivolte ai fornitori terzi critici di servizi TIC.

8. I requisiti di cui alla presente sezione non pregiudicano l'applicazione della direttiva (UE) 2022/2555 né di altre norme dell'Unione in materia di sorveglianza applicabili ai fornitori di servizi di cloud computing.

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

*Articolo 33***Compiti dell'autorità di sorveglianza capofila**

1. L'autorità di sorveglianza capofila, nominata conformemente all'articolo 31, paragrafo 1, lettera b), effettua la sorveglianza dei fornitori terzi critici di servizi TIC assegnati e, ai fini di tutte le questioni relative alla sorveglianza, è il principale punto di contatto per tali fornitori terzi critici di servizi TIC.

2. Ai fini del paragrafo 1, l'autorità di sorveglianza capofila valuta se ciascun fornitore terzo critico di servizi TIC abbia predisposto norme, procedure, meccanismi e accordi esaustivi, solidi ed efficaci per gestire i rischi informatici cui esso può esporre le entità finanziarie.

La valutazione di cui al primo comma si concentra principalmente sui servizi TIC forniti dal fornitore terzo critico di servizi TIC a supporto di funzioni essenziali o importanti delle entità finanziarie. Se necessario per affrontare tutti i rischi pertinenti, tale valutazione si estende ai servizi TIC a supporto di funzioni diverse da quelle essenziali o importanti.

3. La valutazione di cui al paragrafo 2 riguarda:

- a) requisiti in materia di TIC atti a garantire, in particolare, la sicurezza, la disponibilità, la continuità, la scalabilità e la qualità dei servizi che il fornitore terzo critico di servizi TIC presta alle entità finanziarie, nonché la capacità di mantenere standard di, disponibilità, autenticità, integrità o riservatezza 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 di elaborazione dati;
- c) i processi di gestione del rischio, comprese le politiche di gestione dei rischi informatici, la politica di continuità operativa delle TIC e i piani di risposta e ripristino relativi alle TIC;
- d) i meccanismi 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 informatici;
- e) l'identificazione, il monitoraggio e la tempestiva segnalazione alle entità finanziarie di incidenti significativi 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 e l'interoperabilità delle applicazioni, per assicurare un effettivo esercizio dei diritti di risoluzione da parte delle entità finanziarie;
- g) i test su sistemi, infrastrutture e controlli relativi alle TIC;
- h) gli audit in materia di TIC;
- i) l'utilizzo dei pertinenti standard nazionali e internazionali applicabili alla fornitura dei servizi TIC alle entità finanziarie.

4. Sulla base della valutazione di cui al paragrafo 2, e in coordinamento con la rete di sorveglianza comune di cui all'articolo 34, paragrafo 1, l'autorità di sorveglianza capofila adotta un piano di sorveglianza individuale chiaro, dettagliato e motivato che descrive gli obiettivi annuali in materia di sorveglianza e le principali azioni di sorveglianza previste per ciascun fornitore terzo critico di servizi TIC. Tale piano è comunicato annualmente al fornitore terzo critico di servizi TIC.

Prima dell'adozione del piano di sorveglianza, l'autorità di sorveglianza capofila comunica il progetto di piano di sorveglianza al fornitore terzo critico di servizi TIC.

Al ricevimento del progetto di piano di sorveglianza, il fornitore terzo critico di servizi TIC può presentare, entro 15 giorni di calendario, una dichiarazione motivata che dimostri l'impatto previsto sui clienti che sono entità che non rientrano nell'ambito di applicazione del presente regolamento e, se del caso, formuli soluzioni per attenuare i rischi.

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

*Articolo 34***Coordinamento operativo tra autorità di sorveglianza capofila**

1. Per garantire un approccio coerente alle attività di sorveglianza e al fine di consentire strategie di sorveglianza generale coordinate e approcci operativi e metodologie di lavoro coerenti, le tre autorità di sorveglianza capofila nominate a norma dell'articolo 31, paragrafo 1, lettera b), istituiscono una rete di sorveglianza comune per coordinarsi tra loro nelle fasi preparatorie e coordinare lo svolgimento delle attività di sorveglianza sui rispettivi fornitori terzi critici di servizi TIC sottoposti a sorveglianza, nonché nello svolgimento di qualsiasi azione eventualmente necessaria a norma dell'articolo 42.
2. Ai fini del paragrafo 1, le autorità di sorveglianza capofila elaborano un protocollo comune di sorveglianza che specifica le procedure dettagliate da seguire per effettuare il coordinamento quotidiano e garantire scambi e reazioni rapidi. Il protocollo è riveduto periodicamente per tener conto delle esigenze operative, in particolare dell'evoluzione delle modalità pratiche di sorveglianza.
3. Le autorità di sorveglianza capofila possono, a seconda dei casi, chiedere alla BCE e all'ENISA di fornire consulenza tecnica, condividere esperienze pratiche o partecipare a specifiche riunioni di coordinamento della rete di sorveglianza comune.

*Articolo 35***Poteri dell'autorità di sorveglianza capofila**

1. Ai fini dello svolgimento dei compiti previsti dalla presente sezione, all'autorità di sorveglianza capofila sono conferiti i poteri indicati di seguito riguardo ai fornitori terzi critici di servizi TIC:
  - a) richiedere tutte le informazioni e la documentazione pertinenti ai sensi dell'articolo 37;
  - b) condurre indagini e ispezioni di carattere generale ai sensi degli articoli 38 e 39 rispettivamente;
  - c) richiedere, dopo il completamento delle attività di sorveglianza, relazioni in cui si specifichino le azioni adottate o i rimedi applicati da parte dei fornitori terzi critici di servizi TIC in relazione alle raccomandazioni di cui alla lettera d) del presente paragrafo;
  - d) formulare raccomandazioni concernenti i settori di cui all'articolo 33, paragrafo 3, in particolare per quanto riguarda gli elementi indicati di seguito:
    - i) l'impiego di specifici processi o requisiti di sicurezza e qualità delle TIC, segnatamente per il rilascio di correzioni, aggiornamenti, cifratura e altre misure di sicurezza che l'autorità di sorveglianza capofila giudichi pertinenti per garantire la sicurezza delle 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 critici di servizi TIC prestano servizi TIC alle entità finanziarie, che l'autorità di sorveglianza capofila giudichi importanti per prevenire il prodursi di singoli punti di vulnerabilità (*points of failure*), 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) eventuali subappalti previsti, ove l'autorità di sorveglianza capofila ritenga che ulteriori subappalti, compresi gli accordi di subappalto che i fornitori terzi critici di servizi TIC intendano stipulare con fornitori terzi di servizi TIC o con subappaltatori di TIC stabiliti in un paese terzo, possano produrre rischi per la fornitura di servizi da parte dell'entità finanziaria o rischi per la stabilità finanziaria, sulla base dell'esame delle informazioni raccolte a norma degli articoli 37 e 38;
    - 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 TIC oppure un subappaltatore di TIC stabilito in un paese terzo;
      - il subappalto riguarda funzioni essenziali o importanti dell'entità finanziaria; nonché

- l'autorità di sorveglianza capofila ritiene che il ricorso a tale subappalto rappresenti un rischio grave e chiaro per la stabilità finanziaria dell'Unione o per le entità finanziarie, anche per quanto riguarda la capacità delle entità finanziarie di rispettare i requisiti in materia di sorveglianza.

Ai fini del punto iv) della presente lettera, i fornitori terzi di servizi TIC trasmettono all'autorità di sorveglianza capofila, utilizzando il modello di cui all'articolo 41, paragrafo 1, lettera b), le informazioni relative al subappalto.

2. Nell'esercizio dei poteri di cui al presente articolo, l'autorità di sorveglianza capofila:
  - a) assicura un coordinamento regolare all'interno della rete di sorveglianza comune e, in particolare, persegue approcci coerenti, se del caso, per quanto riguarda la sorveglianza dei fornitori terzi critici di servizi TIC;
  - b) tiene debitamente conto del quadro istituito dalla direttiva (UE) 2022/2555 e, se necessario, consulta le autorità competenti interessate designate o istituite in conformità di tale direttiva, al fine di evitare duplicazioni delle misure tecniche e organizzative che potrebbero applicarsi ai fornitori terzi critici di servizi TIC ai sensi di tale direttiva;
  - c) si adopera per ridurre al minimo, nella misura del possibile, il rischio di perturbazione dei servizi forniti da fornitori terzi critici di servizi TIC a clienti che sono entità non rientranti nell'ambito di applicazione del presente regolamento.
3. L'autorità di sorveglianza capofila consulta il forum di sorveglianza prima di esercitare i poteri di cui al paragrafo 1.

Prima di formulare raccomandazioni a norma del paragrafo 1, lettera d), l'autorità di sorveglianza capofila dà al fornitore terzo di servizi TIC la possibilità di fornire entro 30 giorni di calendario informazioni pertinenti che dimostrino l'impatto previsto sui clienti che sono entità che non rientrano nell'ambito di applicazione del presente regolamento e, se del caso, formulino soluzioni per attenuare i rischi.

4. L'autorità di sorveglianza capofila informa la rete di sorveglianza comune dell'esito dell'esercizio dei poteri di cui al paragrafo 1, lettere a) e b). L'autorità di sorveglianza capofila trasmette, senza indebito ritardo, le relazioni di cui al paragrafo 1, lettera c), alla rete di sorveglianza comune e alle autorità competenti delle entità finanziarie che utilizzano i servizi TIC di tale fornitore terzo critico di servizi TIC.

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

6. In caso di inosservanza totale o parziale delle misure che devono essere adottate ai sensi dell'esercizio dei poteri di cui al paragrafo 1, lettere a), b) e c), e dopo la scadenza di un periodo di almeno 30 giorni di calendario dalla data in cui il fornitore terzo critico di servizi TIC ha ricevuto la notifica delle rispettive misure, l'autorità di sorveglianza capofila adotta una decisione che impone una penalità di mora al fine di costringere il fornitore terzo critico di servizi TIC a conformarsi a tali misure.

7. La penalità di mora, di cui al paragrafo 6, è imposta su base giornaliera fino al conseguimento della conformità e per un periodo non superiore a sei mesi dalla notifica della decisione che impone una penalità di mora al fornitore terzo critico di servizi TIC.

8. 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 dal fornitore terzo critico di servizi TIC nel precedente esercizio. Nel determinare l'importo della penalità, l'autorità di sorveglianza capofila tiene conto dei seguenti criteri per quanto riguarda l'inosservanza delle misure di cui al paragrafo 6:

- a) la gravità e la durata dell'inosservanza;
- b) se l'inosservanza sia stata commessa intenzionalmente o per negligenza;
- c) il livello di cooperazione del fornitore terzo di servizi TIC con l'autorità di sorveglianza capofila.

Ai fini del primo comma, per garantire un approccio coerente, l'autorità di sorveglianza capofila avvia consultazioni nell'ambito della rete di sorveglianza comune.

9. 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.

10. L'autorità di sorveglianza capofila comunica 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.

11. Prima di imporre una penalità di mora ai sensi del paragrafo 6, l'autorità di sorveglianza capofila concede ai rappresentanti del fornitore terzo critico di servizi TIC oggetto del procedimento l'opportunità di essere sentiti in merito alle risultanze, e fonda le proprie decisioni unicamente sulle risultanze in merito alle quali il fornitore terzo critico di servizi TIC 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. Il fornitore terzo critico di servizi TIC oggetto del procedimento ha 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 36*

### **Esercizio dei poteri dell'autorità di sorveglianza capofila al di fuori dell'Unione**

1. Qualora gli obiettivi di sorveglianza non possano essere conseguiti interagendo con l'impresa figlia istituita ai fini dell'articolo 31, paragrafo 12, o esercitando attività di sorveglianza in locali situati nell'Unione, l'autorità di sorveglianza capofila può esercitare i poteri, di cui alle disposizioni seguenti, in qualsiasi locale situato in un paese terzo che sia posseduto, o utilizzato in qualsiasi modo, ai fini della fornitura di servizi a entità finanziarie dell'Unione da parte di un fornitore terzo critico di servizi di TIC, riguardo alle relative operazioni commerciali, funzioni o servizi, compresi eventuali uffici amministrativi, commerciali o operativi, locali, terreni, edifici o altre proprietà:

- a) articolo 35, paragrafo 1, lettera a); e
- b) articolo 35, paragrafo 1, lettera b), conformemente all'articolo 38, paragrafo 2, lettere a), b) e d), e all'articolo 39, paragrafi 1 e 2, lettera a).

I poteri di cui al primo comma possono essere esercitati alle condizioni seguenti:

- i) lo svolgimento di un'ispezione in un paese terzo è ritenuto necessario dall'autorità di sorveglianza capofila per consentirle di svolgere pienamente ed efficacemente i propri compiti ai sensi del presente regolamento;
- ii) l'ispezione in un paese terzo è direttamente connessa alla fornitura di servizi TIC a entità finanziarie nell'Unione;
- iii) il fornitore terzo critico di servizi TIC interessato acconsente allo svolgimento di un'ispezione in un paese terzo; nonché
- iv) l'autorità pertinente del paese terzo interessato è stata ufficialmente informata dall'autorità di sorveglianza capofila e non ha sollevato obiezioni al riguardo.

2. Fatte salve le rispettive competenze delle istituzioni dell'Unione e degli Stati membri, ai fini del paragrafo 1, l'ABE, l'ESMA o l'EIOPA concludono accordi di cooperazione amministrativa con l'autorità pertinente del paese terzo al fine di consentire il regolare svolgimento delle ispezioni nel paese terzo interessato da parte dell'autorità di sorveglianza capofila e del gruppo designato per la sua missione in tale paese terzo. Tali accordi di cooperazione non creano obblighi giuridici per l'Unione e i suoi Stati membri, né impediscono agli Stati membri e alle loro autorità competenti di concludere accordi bilaterali o multilaterali con tali paesi terzi e le loro autorità pertinenti.

Tali accordi di cooperazione specificano almeno gli elementi seguenti:

- a) le procedure per il coordinamento delle attività di sorveglianza svolte a norma del presente regolamento e qualsiasi analogo monitoraggio dei rischi informatici derivanti da terzi nel settore finanziario esercitato dall'autorità pertinente del paese terzo interessato, comprese le modalità di trasmissione dell'accordo di quest'ultimo al fine di consentire all'autorità di sorveglianza capofila e al suo gruppo designato di svolgere le indagini generali e le ispezioni in loco di cui al paragrafo 1, primo comma, nel territorio sotto la sua giurisdizione;
  - b) il meccanismo per la trasmissione di tutte le informazioni pertinenti tra l'ABE, l'ESMA o l'EIOPA e l'autorità pertinente del paese terzo interessato, in particolare in relazione alle informazioni che possono essere richieste dall'autorità di sorveglianza capofila a norma dell'articolo 37;
  - c) i meccanismi per la tempestiva notifica, da parte dell'autorità pertinente del paese terzo interessato all'ABE, all'ESMA o all'EIOPA, dei casi in cui si ritiene che un fornitore terzo di servizi TIC stabilito in un paese terzo e designato come critico ai sensi dell'articolo 31, paragrafo 1, lettera a), abbia violato gli obblighi ai quali è tenuto a norma del diritto applicabile del paese terzo interessato quando fornisce servizi a enti finanziari in tale paese terzo, nonché i mezzi di ricorso e le penalità applicate;
  - d) la trasmissione periodica di aggiornamenti sugli sviluppi normativi o di vigilanza sul monitoraggio dei rischi informatici derivanti da terzi degli enti finanziari nel paese terzo interessato;
  - e) i dettagli per consentire, se necessario, la partecipazione di un rappresentante dell'autorità pertinente del paese terzo alle ispezioni condotte dall'autorità di sorveglianza capofila e dal gruppo designato.
3. Quando l'autorità di sorveglianza capofila non è in grado di svolgere le attività di sorveglianza, al di fuori dell'Unione, di cui ai paragrafi 1 e 2, l'autorità di sorveglianza capofila:
- a) esercita i poteri di cui all'articolo 35 sulla base di tutti i fatti e di tutti i documenti di cui dispone;
  - b) documenta e spiega le eventuali conseguenze della sua incapacità di svolgere le attività di sorveglianza previste di cui al presente articolo.

Le potenziali conseguenze di cui alla lettera b) del presente comma sono prese in considerazione nelle raccomandazioni dell'autorità di sorveglianza capofila emesse a norma dell'articolo 35, paragrafo 1, lettera d).

#### *Articolo 37*

#### **Richiesta di informazioni**

1. L'autorità di sorveglianza capofila può, con semplice richiesta o mediante decisione, imporre ai fornitori terzi critici di servizi TIC 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 informatici, nonché qualsiasi informazione relativa ai soggetti cui il fornitore terzo critico di servizi TIC ha esternalizzato attività o funzioni operative.

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

- a) fa riferimento al presente articolo quale base giuridica della richiesta;
- b) dichiara la finalità della richiesta;
- c) specifica le informazioni richieste;
- d) stabilisce un termine entro il quale tali informazioni devono pervenirle;

- e) informa il rappresentante critico del fornitore terzo di servizi TIC cui sono richieste le informazioni che non è tenuto a fornirle, ma 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 entro il quale tali informazioni devono pervenirle;
  - e) indica le penalità di mora di cui all'articolo 35, paragrafo 6, laddove le informazioni fornite siano incomplete o quando tali informazioni non siano fornite entro il termine indicato alla lettera d) del presente paragrafo;
  - 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») in conformità degli articoli 60 e 61 dei regolamenti (UE) n. 1093/2010, (UE) n. 1094/2010 e (UE) n. 1095/2010.
4. I rappresentanti dei fornitori terzi critici di servizi TIC forniscono le informazioni richieste. Gli avvocati debitamente incaricati possono fornire le informazioni richieste a nome dei loro clienti. I fornitori terzi critici di servizi TIC sono pienamente responsabili qualora le informazioni fornite siano incomplete, inesatte o fuorvianti.
5. L'autorità di sorveglianza capofila trasmette senza ritardo copia della decisione di fornire informazioni alle autorità competenti delle entità finanziarie che utilizzano i servizi dei fornitori terzi interessati di servizi TIC critici e alla rete di sorveglianza comune.

#### Articolo 38

#### **Indagini generali**

1. Per adempiere i propri compiti ai sensi del presente regolamento, l'autorità di sorveglianza capofila, coadiuvata dal gruppo di esaminatori congiunto di cui all'articolo 40, paragrafo 1, può, se necessario, svolgere le indagini sui fornitori terzi critici di servizi TIC.
2. L'autorità di sorveglianza capofila ha il potere di:
- a) esaminare registri, dati, procedure e qualsiasi altro materiale pertinente per l'esecuzione dei compiti di sua competenza, su qualsiasi forma di supporto;
  - b) fare od ottenere copie certificate o estratti di tali registri, dati, procedure documentate e di ogni altro materiale;
  - c) convocare rappresentanti del fornitore terzo critico di servizi 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 35, paragrafo 6, qualora i registri, i dati, le procedure documentate o qualsiasi altro materiale richiesto, oppure le risposte alle domande poste ai rappresentanti del fornitore terzo di servizi TIC, siano incompleti o non siano forniti affatto.



4. I rappresentanti dei fornitori terzi critici di servizi 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 35, paragrafo 6, 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 avverso la decisione.

5. In tempo utile prima dell'avvio dell'indagine, l'autorità di sorveglianza capofila informa le autorità competenti delle entità finanziarie che si avvalgono dei servizi TIC del fornitore terzo critico di servizi TIC in questione in merito all'indagine prevista e all'identità delle persone autorizzate.

L'autorità di sorveglianza capofila comunica alla rete di sorveglianza comune tutte le informazioni trasmesse a norma del primo comma.

### Articolo 39

#### Ispezioni

1. Per adempiere i propri compiti ai sensi del presente regolamento, l'autorità di sorveglianza capofila può, coadiuvata dai gruppi di esaminatori congiunti di cui all'articolo 40, paragrafo 1, accedere a locali commerciali, immobili o proprietà dei fornitori terzi di servizi TIC, come sedi centrali, centri operativi, sedi secondarie, per condurvi tutte le necessarie ispezioni in loco; può inoltre effettuare ispezioni extra loco.

Ai fini dell'esercizio dei poteri di cui al primo comma, l'autorità di sorveglianza capofila consulta la rete di sorveglianza comune.

2. I funzionari e altre persone autorizzate dall'autorità di sorveglianza capofila a effettuare l'ispezione in loco hanno il potere di:

- a) accedere ai suddetti locali commerciali, immobili o proprietà; e
- b) sigillare i suddetti locali, libri o registri, per il periodo dell'ispezione e nella misura necessaria per effettuarla.

I funzionari e altre persone autorizzate dall'autorità di sorveglianza capofila 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 35, paragrafo 6, qualora i rappresentanti dei fornitori terzi critici di servizi TIC interessati non si sottopongano all'ispezione.

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

4. Le ispezioni si estendono all'intera gamma di sistemi, reti, dispositivi, informazioni e dati in materia di TIC utilizzati per la fornitura di servizi TIC 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 critici di servizi TIC, 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 critico di servizi TIC si sottopone alle ispezioni in loco ordinate con decisione dell'autorità di sorveglianza capofila. La decisione specifica l'oggetto e le finalità dell'ispezione, fissa la data d'inizio dell'ispezione indica le penalità di mora di cui all'articolo 35, paragrafo 6, 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 presentare ricorso dinanzi alla Corte di giustizia avverso la decisione.

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

*Articolo 40***Sorveglianza nel continuo**

1. Nello svolgimento di attività di sorveglianza, in particolare indagini generali o ispezioni, l'autorità di sorveglianza capofila è coadiuvata da un gruppo di esaminatori congiunto istituito per ciascun fornitore terzo critico di servizi TIC.
2. Il gruppo di esaminatori congiunto di cui al paragrafo 1 è composto da membri del personale appartenenti:
  - a) alle AEV;
  - b) alle autorità competenti interessate che vigilano sulle entità finanziarie cui il fornitore terzo critico di servizi TIC presta servizi TIC;
  - c) all'autorità nazionale competente di cui all'articolo 32, paragrafo 4, lettera e), su base volontaria;
  - d) a un'autorità nazionale competente dello Stato membro in cui è stabilito il fornitore terzo critico di servizi TIC, su base volontaria.

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'autorità di sorveglianza capofila designato a tale scopo («coordinatore dell'autorità di sorveglianza capofila»).

3. Entro tre mesi dal completamento dell'indagine o dell'ispezione, l'autorità di sorveglianza capofila, dopo essersi consultata con il forum di sorveglianza, adotta le raccomandazioni da inviare al fornitore terzo critico di servizi TIC in forza dei poteri che le sono stati conferiti ai sensi dell'articolo 35.
4. Le raccomandazioni di cui al paragrafo 3 sono comunicate immediatamente al fornitore terzo critico di servizi TIC e alle autorità competenti delle entità finanziarie cui il fornitore in questione presta i suoi servizi TIC.

Per l'espletamento delle attività di sorveglianza, l'autorità di sorveglianza capofila può tener conto di qualsiasi pertinente 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 critico di servizi TIC.

*Articolo 41***Armonizzazione delle condizioni che consentono lo svolgimento delle attività di 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 TIC deve fornire nella domanda di designazione volontaria quale fornitore critico a norma dell'articolo 31, paragrafo 11;
  - b) il contenuto, la struttura e il formato delle informazioni da trasmettere, diffondere o segnalare da parte dei fornitori terzi di servizi TIC ai sensi dell'articolo 35, paragrafo 1, compreso il modello per fornire informazioni relative agli accordi di subappalto;
  - c) i criteri per determinare la composizione del gruppo di esaminatori congiunto, garantendo una partecipazione equilibrata dei membri del personale delle AEV e delle autorità competenti interessate, la loro nomina, i compiti e le modalità di lavoro.
  - d) i dettagli della valutazione, da parte delle autorità competenti, delle misure adottate dai fornitori terzi critici di servizi TIC sulla base delle raccomandazioni dell'autorità di sorveglianza capofila ai sensi dell'articolo 42, paragrafo 3.
2. Le AEV presentano tali progetti di norme tecniche di regolamentazione alla Commissione entro il 17 luglio 2024.

Alla Commissione è delegato il potere di integrare il presente regolamento, adottando le norme tecniche di regolamentazione di cui al paragrafo 1, in conformità 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 42***Seguito dato dalle autorità competenti**

1. Entro 60 giorni di calendario dalla ricezione delle raccomandazioni formulate dall'autorità di sorveglianza capofila ai sensi dell'articolo 35, paragrafo 1, lettera d), i fornitori terzi critici di servizi TIC comunicano all'autorità di sorveglianza capofila la loro intenzione di attenersi alle raccomandazioni o forniscono una spiegazione articolata del motivo per cui non lo faranno. L'autorità di sorveglianza capofila trasmette immediatamente le informazioni alle autorità competenti delle entità finanziarie interessate.

2. L'autorità di sorveglianza capofila rende pubblici i casi in cui un fornitore terzo critico di servizi TIC non dà notizia all'autorità di sorveglianza capofila conformemente al paragrafo 1 o se la spiegazione fornita dal fornitore terzo critico di servizi TIC non è ritenuta sufficiente. Le informazioni pubblicate rivelano l'identità del fornitore terzo critico di servizi TIC nonché informazioni sul tipo e la natura dell'inosservanza. Tali informazioni sono limitate a quanto è pertinente e proporzionato al fine di assicurare la sensibilizzazione del pubblico, salvo il caso in cui la pubblicazione possa arrecare un danno sproporzionato alle parti coinvolte o mettere gravemente a rischio il regolare funzionamento e l'integrità dei mercati finanziari o la stabilità dell'intero sistema finanziario dell'Unione o di parte di esso.

L'autorità di sorveglianza capofila informa il fornitore terzo di servizi TIC di tale divulgazione al pubblico.

3. Le autorità competenti informano le entità finanziarie interessate dei rischi individuati nelle raccomandazioni inviate ai fornitori terzi critici di servizi TIC conformemente all'articolo 35, paragrafo 1, lettera d).

Nella gestione dei rischi informatici derivanti da terzi, le entità finanziarie tengono conto dei rischi di cui al primo comma.

4. Qualora un'autorità competente ritenga che un'entità finanziaria non tenga conto dei rischi specifici individuati nelle raccomandazioni, o non li affronti in misura sufficiente, nell'ambito della sua gestione dei rischi informatici derivanti da terzi, essa notifica all'entità finanziaria la possibilità di adottare una decisione, entro 60 giorni di calendario dal ricevimento di tale notifica, a norma del paragrafo 6, in assenza di adeguati accordi contrattuali volti a far fronte a tali rischi.

5. Dopo aver ricevuto le relazioni di cui all'articolo 35, paragrafo 1, lettera c), e prima di adottare una decisione di cui al paragrafo 6 del presente articolo, le autorità competenti possono, su base volontaria, consultare le autorità competenti designate o istituite in conformità della direttiva (UE) 2022/2555 responsabili della vigilanza di un soggetto essenziale o importante ai sensi di tale direttiva, che è stato designato come fornitore terzo critico di servizi TIC.

6. A norma dell'articolo 50, le autorità competenti possono adottare, come misura di ultima istanza, a seguito della notifica e, se del caso, della consultazione di cui ai paragrafi 4 e 5 del presente articolo, una decisione che impone alle entità finanziarie di sospendere temporaneamente, in tutto o in parte, l'utilizzo o l'introduzione di un servizio prestato dal fornitore terzo critico di servizi TIC, fino a quando non siano stati affrontati i rischi identificati nelle raccomandazioni trasmesse ai fornitori terzi critici di servizi TIC. Laddove si renda necessario, le autorità competenti possono chiedere alle entità finanziarie di risolvere, in tutto o in parte, gli accordi contrattuali pertinenti stipulati con i fornitori terzi critici di servizi TIC.

7. Qualora un fornitore terzo critico di servizi TIC rifiuti di accogliere raccomandazioni basandosi su un approccio diverso da quello raccomandato dall'autorità di sorveglianza capofila e qualora tale approccio diverso possa avere un impatto negativo su un numero considerevole di entità finanziarie, o su una parte significativa del settore finanziario, e le singole segnalazioni emesse dalle autorità competenti non abbiano dato luogo ad approcci coerenti che attenuino il rischio potenziale per la stabilità finanziaria, l'autorità di sorveglianza capofila può, previa consultazione del forum di sorveglianza, emettere pareri non vincolanti e non pubblici alle autorità competenti, al fine di promuovere, se del caso, misure di follow-up coerenti e convergenti in materia di vigilanza.

8. Dopo aver ricevuto le relazioni di cui all'articolo 35, paragrafo 1, lettera c), le autorità competenti tengono conto, al momento di adottare le decisioni di cui al paragrafo 6 del presente articolo, del tipo e delle dimensioni del rischio che non è stato affrontato dal fornitore terzo critico di servizi TIC, 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 critico di servizi TIC;
- c) se l'inosservanza abbia favorito o generato un reato finanziario o se tale reato sia in qualche misura attribuibile all'inosservanza;
- d) se l'inosservanza sia stata commessa intenzionalmente o per negligenza;
- e) se la sospensione o la risoluzione degli accordi contrattuali comporti un rischio per la continuità delle operazioni commerciali dell'entità finanziaria malgrado gli sforzi dell'entità finanziaria per evitare perturbazioni nella fornitura dei suoi servizi;
- f) se del caso, il parere, richiesto su base volontaria conformemente al paragrafo 5 del presente articolo, delle autorità competenti designate o istituite a norma della direttiva (UE) 2022/2555 responsabili della vigilanza di un soggetto essenziale o importante ai sensi di tale direttiva, che è stato designato come fornitore terzo critico di servizi TIC.

Le autorità competenti concedono alle entità finanziarie il periodo di tempo necessario per consentire loro di adeguare gli accordi contrattuali con i fornitori terzi critici di servizi TIC al fine di evitare effetti negativi sulla loro resilienza operativa digitale e di consentire loro di attuare le strategie di uscita e i piani di transizione di cui all'articolo 28.

9. La decisione di cui al paragrafo 6 del presente articolo è notificata ai membri del forum di sorveglianza di cui all'articolo 32, paragrafo 4, lettere a), b) e c), e alla rete di sorveglianza comune.

I fornitori terzi critici di servizi TIC interessati dalle decisioni di cui al paragrafo 6 cooperano pienamente con le entità finanziarie colpite, in particolare nel contesto del processo di sospensione o risoluzione dei loro accordi contrattuali.

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

11. L'autorità di sorveglianza capofila può, su richiesta, fornire ulteriori chiarimenti sulle raccomandazioni formulate per orientare le autorità competenti sulle misure di follow-up.

#### Articolo 43

### Commissioni per le attività di sorveglianza

1. L'autorità di sorveglianza capofila addebita, conformemente all'atto delegato di cui al paragrafo 2 del presente articolo, ai fornitori terzi critici di servizi TIC commissioni che coprono completamente le spese necessarie sostenute dall'autorità di sorveglianza capofila 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 dal gruppo di esaminatori congiunto di cui all'articolo 40, nonché i costi della consulenza fornita dagli esperti indipendenti di cui all'articolo 32, paragrafo 4, secondo comma, in relazione a questioni che rientrano nell'ambito delle attività di sorveglianza diretta.

L'importo della commissione addebitata al fornitore terzo critico di servizi TIC copre tutti i costi derivanti dall'esecuzione dei compiti di cui alla presente sezione ed è proporzionato al fatturato del fornitore.

2. Alla Commissione è conferito il potere di adottare un atto delegato, conformemente all'articolo 57, per integrare il presente regolamento determinando l'importo delle commissioni e le relative modalità di pagamento entro il 17 luglio 2024.

*Articolo 44***Cooperazione internazionale**

1. Fatto salvo l'articolo 36, ai sensi, rispettivamente, dell'articolo 33 dei regolamenti (UE) n. 1093/2010, (UE) n. 1095/2010 e (UE) n. 1094/2010, 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 informatici 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 informatici 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 pertinenti tenute con le autorità dei paesi terzi di cui al paragrafo 1, con particolare attenzione all'evoluzione dei rischi informatici derivanti da terzi e alle implicazioni per la stabilità finanziaria, l'integrità del mercato, la protezione degli investitori e il funzionamento del mercato interno.

**CAPO VI*****Meccanismi di condivisione delle informazioni****Articolo 45***Meccanismi di condivisione delle informazioni e delle analisi delle minacce informatiche**

1. Le entità finanziarie possono scambiarsi reciprocamente informazioni e analisi delle minacce informatiche, tra cui indicatori di compromissione, tattiche, tecniche e procedure, segnali di allarme per la cibersicurezza e strumenti di configurazione, nella misura in cui tale condivisione di informazioni e dati:
  - a) mira a potenziare la resilienza operativa digitale delle entità finanziarie, in particolare aumentando la consapevolezza in merito alle minacce informatiche, contenendo o inibendo la capacità di diffusione delle minacce informatiche, sostenendo le capacità di difesa, le tecniche di individuazione delle minacce, le politiche di mitigazione o le fasi di risposta e ripristino;
  - b) si svolge entro comunità fidate di entità finanziarie;
  - c) si realizza mediante meccanismi di condivisione delle informazioni che tutelano la natura potenzialmente sensibile delle informazioni condivise e sono disciplinati da norme di condotta pienamente rispettose della riservatezza dell'attività economica, della protezione dei dati personali ai sensi del regolamento (UE) 2016/679 e delle linee guida sulla politica in materia di concorrenza.
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 concernenti il coinvolgimento delle autorità pubbliche e la veste in cui queste possono partecipare ai meccanismi di condivisione delle informazioni, il coinvolgimento dei fornitori terzi di servizi TIC, nonché gli elementi operativi tra cui l'utilizzo di piattaforme informatiche apposite.
3. Le entità finanziarie notificano alle autorità competenti la propria partecipazione ai meccanismi di condivisione delle informazioni di cui al paragrafo 1, al momento della convalida della propria adesione o, se del caso, della cessazione dell'adesione, quando quest'ultima abbia effetto.

## CAPO VII

**Autorità competenti**

## Articolo 46

**Autorità competenti**

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

- a) per gli enti creditizi e per gli enti esentati a norma della direttiva 2013/36/UE: l'autorità competente designata in conformità dell'articolo 4 di tale direttiva; e per gli enti creditizi classificati come significativi ai sensi dell'articolo 6, paragrafo 4, del regolamento (UE) n. 1024/2013: la BCE conformemente ai poteri e ai compiti conferiti da tale regolamento;
- b) per gli istituti di pagamento, compresi quelli esentati a norma della direttiva (UE) 2015/2366, gli istituti di moneta elettronica, compresi quelli esentati a norma della direttiva 2009/110/CE, e i prestatori di servizi di informazione sui conti di cui all'articolo 33, paragrafo 1, della direttiva (UE) 2015/2366: l'autorità competente designata in conformità dell'articolo 22 della direttiva (UE) 2015/2366;
- c) per le imprese di investimento: l'autorità competente designata in conformità dell'articolo 4 della direttiva (UE) 2019/2034 del Parlamento europeo e del Consiglio <sup>(38)</sup>;
- d) per i fornitori di servizi per le cripto-attività quali autorizzati ai sensi del regolamento sui mercati delle cripto-attività e gli emittenti di token collegati ad attività: l'autorità competente designata in conformità delle pertinenti disposizioni di tale regolamento;
- e) per i depositari centrali di titoli: l'autorità competente designata in conformità dell'articolo 11 del regolamento (UE) n. 909/2014;
- f) per le controparti centrali: l'autorità competente designata in conformità dell'articolo 22 del regolamento (UE) n. 648/2012;
- g) 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 e l'autorità competente quale definita all'articolo 2, paragrafo 1, punto 18), del regolamento (UE) n. 600/2014;
- h) per i repertori di dati sulle negoziazioni: l'autorità competente designata in conformità dell'articolo 22 del regolamento (UE) n. 648/2012;
- i) per i gestori di fondi di investimento alternativi: l'autorità competente designata in conformità dell'articolo 44 della direttiva 2011/61/UE;
- j) per le società di gestione: l'autorità competente designata in conformità dell'articolo 97 della direttiva 2009/65/CE;
- k) per le imprese di assicurazione e di riassicurazione: l'autorità competente designata in conformità dell'articolo 30 della direttiva 2009/138/CE;
- l) 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;
- m) per gli enti pensionistici aziendali o professionali: l'autorità competente designata a norma dell'articolo 47 della direttiva (UE) 2016/2341;
- n) per le agenzie di rating del credito: l'autorità competente designata in conformità dell'articolo 21 del regolamento (CE) n. 1060/2009;
- o) per gli amministratori di indici di riferimento critici: l'autorità competente designata in conformità degli articoli 40 e 41 del regolamento (UE) 2016/1011;

<sup>(38)</sup> Direttiva (UE) 2019/2034 del Parlamento europeo e del Consiglio, del 27 novembre 2019, relativa alla vigilanza prudenziale sulle imprese di investimento e recante modifica delle direttive 2002/87/CE, 2009/65/CE, 2011/61/UE, 2013/36/UE, 2014/59/UE e 2014/65/UE (GU L 314 del 5.12.2019, pag. 64).

- p) per i fornitori di servizi di crowdfunding: l'autorità competente designata in conformità dell'articolo 29 del regolamento (UE) 2020/1503;
- q) 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 47

### **Cooperazione con le strutture e le autorità istituite dalla direttiva (UE) 2022/2555**

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 14 della direttiva (UE) 2022/2555, le AEV e le autorità competenti possono partecipare alle attività del gruppo di cooperazione per le questioni che riguardano le loro attività di vigilanza in relazione alle entità finanziarie. Le AEV e le autorità competenti possono chiedere di essere invitate a partecipare alle attività del gruppo di cooperazione per questioni relative alle entità essenziali o importanti ai sensi della direttiva (UE) 2022/2555 che sono anch'esse state designate come fornitori terzi critici di servizi TIC a norma dell'articolo 31 del presente regolamento.
2. Le autorità competenti possono consultare, se del caso, i punti di contatto unici e i CSIRT designati o istituiti in conformità della direttiva (UE) 2022/2555, e scambiare informazioni con essi.
3. Se del caso, le autorità competenti possono richiedere qualsiasi consulenza e assistenza tecnica pertinenti alle autorità competenti designate o istituite a norma della direttiva (UE) 2022/2555 e stabilire accordi di cooperazione per consentire l'istituzione di meccanismi di coordinamento efficaci e di risposta rapida.
4. Gli accordi di cui al paragrafo 3 del presente articolo possono, tra l'altro, specificare le procedure per il coordinamento delle attività di vigilanza e di sorveglianza, rispettivamente, in relazione a soggetti essenziali o importanti ai sensi della direttiva (UE) 2022/2555 che sono stati designati come fornitori terzi critici di servizi TIC a norma dell'articolo 31 del presente regolamento, anche per lo svolgimento, conformemente al diritto nazionale, di indagini e ispezioni in loco, nonché per i meccanismi per lo scambio di informazioni tra le autorità competenti ai sensi del presente regolamento e le autorità competenti designate o istituite a norma di tale direttiva, il che comprende l'accesso alle informazioni richieste da tali ultime autorità.

#### Articolo 48

### **Cooperazione tra autorità**

1. Le autorità competenti cooperano strettamente tra loro e, se del caso, con l'autorità di sorveglianza capofila.
2. Le autorità competenti e l'autorità di sorveglianza capofila si scambiano tempestivamente tutte le informazioni pertinenti riguardanti i fornitori terzi critici di servizi TIC che sono necessarie per svolgere i rispettivi compiti ai sensi del presente regolamento, in particolare in relazione ai rischi individuati, agli approcci e alle misure adottate nell'ambito dei compiti di sorveglianza dell'autorità di sorveglianza capofila.

#### Articolo 49

### **Comunicazione, cooperazione e attività finanziarie intersettoriali**

1. Le AEV, tramite il comitato congiunto e in collaborazione con le autorità competenti, le autorità di risoluzione di cui all'articolo 3 della direttiva 2014/59/UE, la BCE, il Comitato di risoluzione unico per quanto riguarda le informazioni relative alle entità che rientrano nell'ambito di applicazione del regolamento (UE) n. 806/2014, il CERS e l'ENISA, se del caso, 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'Unione nel caso di grave incidente transfrontaliero connesso alle TIC o relativa minaccia aventi un impatto sistemico sull'intero settore finanziario dell'Unione.

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

2. Le autorità competenti, le AEV e la BCE cooperano strettamente tra loro e si scambiano informazioni per svolgere i compiti di cui agli articoli da 47 a 54. Realizzano uno stretto coordinamento dell'attività di vigilanza per rilevare e correggere le violazioni del presente regolamento, sviluppare e promuovere migliori prassi, agevolare la collaborazione, promuovere la coerenza dell'interpretazione e formulare valutazioni transgiurisdizionali in caso di disaccordo.

#### Articolo 50

#### **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 i poteri seguenti:
  - a) l'avere accesso a qualsiasi documento o dato, detenuto in qualsiasi forma, che l'autorità competente consideri pertinente per lo svolgimento dei propri compiti e la possibilità di riceverne o farne una copia;
  - b) lo svolgere ispezioni o indagini in loco comprendenti tra l'altro:
    - i) la convocazione di rappresentanti delle entità finanziarie per ottenere spiegazioni scritte od orali su fatti o documenti relativi all'oggetto e alle finalità dell'indagine e registrarne le risposte;
    - ii) l'audizione di persone fisiche o giuridiche consenzienti allo scopo di raccogliere informazioni pertinenti all'oggetto dell'indagine;
  - c) il richiedere l'applicazione di misure correttive e di riparazione per le violazioni dei requisiti del presente regolamento.
3. Fatto salvo il diritto degli Stati membri di imporre sanzioni penali in conformità dell'articolo 52, 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 violazione del presente regolamento e di astenersi dal ripeterlo;
  - b) richiedere la cessazione temporanea o permanente di qualsiasi pratica o comportamento che le autorità competenti considerino contrari alle disposizioni del presente regolamento e prevenirne la reiterazione;
  - c) adottare qualsiasi tipo di misura, anche di natura pecuniaria, per assicurare che le entità finanziarie continuino a rispettare i requisiti 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; nonché
  - e) pubblicare comunicazioni pubbliche, comprese dichiarazioni pubbliche, indicanti l'identità della persona fisica o giuridica e la natura della violazione.



5. Qualora il paragrafo 2, lettera c), e il 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 51*

### **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 50 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; oppure
- 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 50, 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 o 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 persona fisica o giuridica;
- g) le precedenti violazioni commesse dalla persona fisica o giuridica responsabile.

#### *Articolo 52*

### **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 53***Obblighi di notifica**

Gli Stati membri notificano alla Commissione, all'ESMA, all'ABE e all'EIOPA le disposizioni legislative, regolamentari e amministrative adottate in attuazione del presente capo, incluse le eventuali norme di diritto penale pertinenti, entro il 17 gennaio 2025. Gli Stati membri notificano senza indebito ritardo alla Commissione, all'ESMA, all'ABE e all'EIOPA tutte le successive modifiche.

*Articolo 54***Pubblicazione delle sanzioni amministrative**

1. Le autorità competenti pubblicano senza indebito ritardo sul proprio sito web ufficiale qualsiasi decisione di imporre sanzioni amministrative contro la quale non vi sia diritto di ricorso, dopo la notifica al destinatario.
2. La pubblicazione di cui al paragrafo 1 comprende informazioni sul tipo e la natura della violazione, l'identità delle persone responsabili e le sanzioni imposte.
3. Qualora, in seguito a una valutazione caso per caso, ritenga che la pubblicazione dell'identità, nel caso di persone giuridiche, o dell'identità e dei dati personali, nel caso di persone fisiche, sarebbe sproporzionata, ivi compresi rischi inerenti alla protezione dei dati personali, metterebbe a repentaglio la stabilità dei mercati finanziari o lo svolgimento di un'indagine penale in corso, oppure provocherebbe, 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; oppure
  - 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 unicamente per il periodo necessario ai fini dell'applicazione del presente articolo. Tale periodo non è superiore ai cinque anni dalla sua pubblicazione.

*Articolo 55***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, ivi compreso lo scambio di informazioni tra le autorità competenti ai sensi del presente regolamento e le autorità competenti designate o istituite a norma della direttiva (UE) 2022/2555, non sono 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.

#### *Articolo 56*

### **Protezione dei dati**

1. Le AEV e le autorità competenti sono autorizzate a trattare i dati personali solo se necessario ai fini dell'adempimento dei rispettivi obblighi e doveri ai sensi del presente regolamento, in particolare per quanto riguarda le indagini, le ispezioni, la richiesta di informazioni, la comunicazione, la pubblicazione, le valutazioni, la verifica e la stesura dei piani di sorveglianza. I dati personali sono trattati a norma del regolamento (UE) 2016/679 o del regolamento (UE) 2018/1725, a seconda dei casi.

2. Salvo nel caso in cui sia altrimenti disposto in altri atti settoriali, i dati personali di cui al paragrafo 1 sono conservati fino all'espletamento degli obblighi di vigilanza applicabili e, in ogni caso, per un periodo massimo di 15 anni, salvo in caso di procedimenti giudiziari in corso che richiedono un'ulteriore conservazione di tali dati.

#### *CAPO VIII*

### **Atti delegati**

#### *Articolo 57*

### **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 31, paragrafo 6, e all'articolo 43, paragrafo 2, è conferito alla Commissione per un periodo di cinque anni a decorrere dal 17 gennaio 2024. 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 31, paragrafo 6, e all'articolo 43, paragrafo 2, può essere revocata in qualsiasi momento dal Parlamento europeo o dal Consiglio. La decisione di revoca pone fine alla delega di potere ivi specificata. Gli effetti della decisione decorrono dal giorno successivo alla pubblicazione della decisione nella *Gazzetta ufficiale dell'Unione europea* o da una data successiva ivi specificata. Essa non pregiudica la validità degli atti delegati già in vigore.

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

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

6. L'atto delegato adottato ai sensi dell'articolo 31, paragrafo 6, e dell'articolo 43, 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 58

### **Clausola di riesame**

1. Entro il 17 gennaio 2028, la Commissione, dopo aver consultato le AEV 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. Il riesame comprende almeno:

- a) i criteri per la designazione dei fornitori terzi critici di servizi TIC, di cui all'articolo 31, paragrafo 2;
- b) il carattere volontario della notifica di minacce informatiche significative di cui all'articolo 19;
- c) il regime di cui all'articolo 31, paragrafo 12, e i poteri dell'autorità di sorveglianza capofila di cui all'articolo 35, paragrafo 1, lettera d), punto iv), primo trattino, al fine di valutare l'efficacia di tali disposizioni per quanto riguarda la garanzia di una sorveglianza efficace dei fornitori terzi critici di servizi TIC stabiliti in un paese terzo e la necessità di istituire un'impresa figlia nell'Unione.

Ai fini del primo comma della presente lettera, il riesame comprende un'analisi del regime di cui all'articolo 31, paragrafo 12, comprese le condizioni di accesso delle entità finanziarie dell'Unione ai servizi di paesi terzi e la disponibilità di tali servizi sul mercato dell'Unione, e tiene conto degli ulteriori sviluppi nei mercati dei servizi disciplinati dal presente regolamento, dell'esperienza pratica delle entità finanziarie e delle autorità di vigilanza finanziaria per quanto riguarda l'applicazione e, rispettivamente, la vigilanza di tale regime e di eventuali sviluppi pertinenti in materia di regolamentazione e vigilanza a livello internazionale;

- d) se sia opportuno includere nell'ambito di applicazione del presente regolamento le entità finanziarie di cui all'articolo 2, paragrafo 3, lettera e), che utilizzano sistemi di vendita automatizzata, alla luce dei futuri sviluppi del mercato sull'uso di tali sistemi;
- e) il funzionamento e l'efficacia della rete di sorveglianza comune in termini di sostegno alla coerenza della sorveglianza e all'efficienza dello scambio di informazioni nell'ambito del quadro di sorveglianza.

2. Nel contesto del riesame della direttiva (UE) 2015/2366, la Commissione valuta la necessità di una maggiore ciberresilienza dei sistemi di pagamento e delle attività di trattamento dei pagamenti e se sia opportuno ampliare l'ambito di applicazione del presente regolamento agli operatori dei sistemi di pagamento e alle entità coinvolte nelle attività di trattamento dei pagamenti. Alla luce di tale valutazione, la Commissione presenta, nell'ambito del riesame della direttiva (UE) 2015/2366, una relazione al Parlamento europeo e al Consiglio e entro il 17 luglio 2023.

Sulla base di tale relazione di riesame e previa consultazione delle AEV, della BCE e del CERS, la Commissione può presentare, se del caso e nell'ambito della proposta legislativa che può adottare a norma dell'articolo 108, secondo comma, della direttiva (UE) 2015/2366, una proposta volta a garantire che tutti gli operatori dei sistemi di pagamento e le entità coinvolte nelle attività di trattamento dei pagamenti siano soggetti a un'adeguata sorveglianza, tenendo conto nel contempo dell'esistente sorveglianza da parte delle banche centrali.

3. Entro il 17 gennaio 2026, la Commissione, dopo aver consultato le AEV e il comitato degli organismi europei di controllo delle attività di revisione contabile, effettua un riesame e presenta al Parlamento europeo e al Consiglio una relazione accompagnata, se del caso, da una proposta legislativa sull'opportunità di rafforzare i requisiti per i revisori legali e le imprese di revisione contabile per quanto riguarda la resilienza operativa digitale, mediante l'inclusione dei revisori legali e delle imprese di revisione contabile nell'ambito di applicazione del presente regolamento o mediante modifiche della direttiva 2006/43/CE del Parlamento europeo e del Consiglio <sup>(39)</sup>.

## Sezione II

### Modifiche

#### Articolo 59

#### Modifiche del regolamento (CE) n. 1060/2009

Il regolamento (CE) n. 1060/2009 è così modificato:

- 1) nell'allegato I, sezione A, punto 4, il primo comma è sostituito dal 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) 2022/2554 del Parlamento europeo e del Consiglio (\*).

(\*) Regolamento (UE) 2022/2554 del Parlamento europeo e del Consiglio, del 14 dicembre 2022, 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, (UE) n. 909/2014 e (UE) 2016/1011 (GU L 333 del 27.12.2022, pag. 1).»;

- 2) nell'allegato III, il punto 12) è sostituito dal seguente:

«12) L'agenzia di rating del credito viola l'articolo 6, paragrafo 2, in combinato disposto con l'allegato I, sezione A, punto 4, quando non dispone di procedure amministrative o contabili solide, di meccanismi di controllo interno, di procedure efficaci per la valutazione del rischio o di meccanismi efficaci di controllo e protezione per la gestione dei sistemi di TIC in conformità del regolamento (UE) 2022/2554, o non instaurando, né mantenendo le procedure di adozione di decisione o le strutture organizzative richieste dal predetto punto.».

#### Articolo 60

#### 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, tra cui sistemi di TIC gestiti in conformità del regolamento (UE) 2022/2554 del Parlamento europeo e del Consiglio (\*).

(\*) Regolamento (UE) 2022/2554 del Parlamento europeo e del Consiglio, del 14 dicembre 2022, 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, (UE) n. 909/2014 e (UE) 2016/1011 (GU L 333 del 27.12.2022, pag. 1).»;

<sup>(39)</sup> Direttiva 2006/43/CE del Parlamento europeo e del Consiglio, del 17 maggio 2006, relativa alle revisioni legali dei conti annuali e dei conti consolidati, che modifica le direttive 78/660/CEE e 83/349/CEE del Consiglio e abroga la direttiva 84/253/CEE del Consiglio (GU L 157 del 9.6.2006, pag. 87).

- 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 una politica di continuità operativa delle TIC e piani di risposta e ripristino relativi alle TIC predisposti e attuati in conformità del regolamento (UE) 2022/2554, miranti ad assicurare il mantenimento delle funzioni, la ripresa tempestiva delle attività e l'adempimento degli obblighi della CCP.»;
- b) al paragrafo 3, il primo comma è sostituito dal seguente:
- «3. 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 della politica di continuità operativa delle TIC e dei piani di risposta e ripristino relativi alle TIC.»;
- 3) all'articolo 56, paragrafo 3, il primo comma 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 i requisiti in materia di gestione dei rischi informatici, 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) 2022/2554.
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 una politica di continuità operativa delle TIC e piani di risposta e ripristino relativi alle TIC istituiti in conformità del regolamento (UE) 2022/2554, miranti ad assicurare il mantenimento delle loro funzioni, la ripresa tempestiva delle attività e l'adempimento degli obblighi assunti.»;
- 5) all'articolo 80, il paragrafo 1 è soppresso;
- 6) nell'allegato I, la sezione II è così modificata:
- a) le lettere a) e b) sono sostituite dalle seguenti:
- «a) un repertorio di dati sulle negoziazioni viola l'articolo 79, paragrafo 1, allorché non individua le fonti di rischio operativo o non limita al massimo tali rischi sviluppando sistemi, controlli e procedure adeguati, tra cui sistemi di TIC gestiti ai sensi del regolamento (UE) 2022/2554;
- b) un repertorio di dati sulle negoziazioni viola l'articolo 79, paragrafo 2, allorché non stabilisce, non attua o non mantiene una politica adeguata di continuità operativa e un piano di ripristino in caso di disastro, istituiti in conformità del regolamento (UE) 2022/2554, miranti ad assicurare il mantenimento delle proprie funzioni, la ripresa tempestiva delle attività e l'adempimento degli obblighi assunti.»;
- b) la lettera c) è soppressa;
- 7) l'allegato III è così modificato:
- a) La sezione II è così modificata:
- i) la lettera c) è sostituita dalla seguente:
- «c) una CCP di classe 2 viola l'articolo 26, paragrafo 3, allorché non mantiene o non gestisce una struttura organizzativa che assicuri la continuità e il regolare funzionamento della prestazione dei propri servizi e dell'esercizio delle attività, o allorché non utilizza sistemi, risorse o procedure adeguati e proporzionati, tra cui sistemi di TIC gestiti conformemente al regolamento (UE) 2022/2554»;
- ii) la lettera f) è soppressa;

b) nella sezione III, la lettera a) è sostituita dalla seguente:

- «a) una CCP di classe 2 viola l'articolo 34, paragrafo 1, allorché non stabilisce, non attua o non mantiene una politica adeguata di continuità operativa e un piano di ripristino in caso di disastro, istituiti in conformità del regolamento (UE) 2022/2554, miranti ad assicurare il mantenimento delle proprie funzioni, la ripresa tempestiva delle attività e l'adempimento degli obblighi assunti dalla CCP; tale piano prevede almeno la ripresa di tutte le operazioni in corso al momento della perturbazione in modo da permettere alla CCP di continuare a funzionare con certezza e di completare il regolamento alla data prevista;».

#### Articolo 61

### 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) 2022/2554 del Parlamento europeo e del Consiglio (\*), 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) 2022/2554 del Parlamento europeo e del Consiglio, del 14 dicembre 2022, 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, (UE) n. 909/2014 e (UE) 2016/1011 (GU L 333 del 27.12.2022, pag. 1).»;

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 operato, i CSD stabiliscono, attuano e mantengono una politica adeguata di continuità operativa e un piano di ripristino in caso di disastro, comprendente una politica di continuità operativa delle TIC e piani di risposta e ripristino relativi alle TIC istituiti ai sensi del regolamento (UE) 2022/2554, 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 12, paragrafi 5 e 7, del regolamento (UE) 2022/2554.»;

4) il paragrafo 6 è sostituito dal seguente:

- «6. I CSD individuano, controllano e gestiscono i rischi ai quali i principali partecipanti ai sistemi di regolamento titoli da essi operati nonché i fornitori di servizi e utenze, e altri CSD o altre infrastrutture di mercato possono esporre le loro attività. Su richiesta, forniscono alle autorità competenti e alle autorità rilevanti informazioni su ogni rischio siffatto individuato. Informano inoltre senza ritardo l'autorità competente e le autorità rilevanti in merito a eventuali incidenti operativi causati da tali rischi, tranne che in relazione ai rischi informatici.»;

5) al paragrafo 7, il primo comma è sostituito dal seguente:

- «7. L'ESMA, in stretta cooperazione con i membri del SEBC, elabora progetti di norme tecniche di regolamentazione per specificare i rischi operativi di cui ai paragrafi 1 e 6, tranne che in relazione ai rischi informatici, i metodi per testare, gestire o ridurre al minimo tali rischi, ivi compresi le politiche di continuità operativa e i piani di ripristino in caso di disastro di cui ai paragrafi 3 e 4, nonché i metodi di valutazione degli stessi.».

## Articolo 62

**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 sostituito dal seguente:

«4. Gli APA rispettano i requisiti in materia di sicurezza dei sistemi informatici e di rete di cui al regolamento (UE) 2022/2554 del Parlamento europeo e del Consiglio (\*).

(\*) Regolamento (UE) 2022/2554 del Parlamento europeo e del Consiglio, del 14 dicembre 2022, 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, (UE) n. 909/2014 e (UE) 2016/1011 (GU L 333 del 27.12.2022, pag. 1).»;

b) al paragrafo 8, la lettera c) è sostituita dalla seguente:

«c) i requisiti organizzativi concreti di cui ai paragrafi 3 e 5.»;

2) l'articolo 27 *nonies* è così modificato:

a) il paragrafo 5 è sostituito dal seguente:

«5. I CTP rispettano i requisiti in materia di sicurezza dei sistemi informatici e di rete di cui al regolamento (UE) 2022/2554.»;

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 sostituito dal seguente:

«3. Gli ARM rispettano i requisiti in materia di sicurezza dei sistemi informatici e di rete di cui al regolamento (UE) 2022/2554.»;

b) al paragrafo 5, la lettera b) è sostituita dalla seguente:

«b) i requisiti organizzativi concreti di cui ai paragrafi 2 e 4.».

## Articolo 63

**Modifiche del regolamento (UE) 2016/1011**

All'articolo 6 del regolamento (UE) 2016/1011 è aggiunto il paragrafo seguente:

«6. Per gli indici di riferimento critici, un amministratore 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) 2022/2554 del Parlamento europeo e del Consiglio (\*).

(\*) Regolamento (UE) 2022/2554 del Parlamento europeo e del Consiglio, del 14 dicembre 2022, 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, (UE) n. 909/2014 e (UE) 2016/1011 (GU L 333 del 27.12.2022, pag. 1).»;



*Articolo 64***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 17 gennaio 2025.

Il presente regolamento è obbligatorio in tutti i suoi elementi e direttamente applicabile in ciascuno degli Stati membri.

Fatto a Strasburgo, il 14 dicembre 2022

*Per il Parlamento europeo*

*La presidente*

R. METSOLA

*Per il Consiglio*

*Il presidente*

M. BEK

---