2024/1773

25.6.2024

REGOLAMENTO DELEGATO (UE) 2024/1773 DELLA COMMISSIONE

del 13 marzo 2024

che integra il regolamento (UE) 2022/2554 del Parlamento europeo e del Consiglio per quanto riguarda le norme tecniche di regolamentazione che precisano il contenuto dettagliato della politica relativa agli accordi contrattuali per l'utilizzo di servizi TIC a supporto di funzioni essenziali o importanti prestati da fornitori terzi di servizi TIC

(Testo rilevante ai fini del SEE)

LA COMMISSIONE EUROPEA,

visto il trattato sul funzionamento dell'Unione europea,

visto 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 ([1]), in particolare l'articolo 28, paragrafo 10, terzo comma,

considerando quanto segue:

(1) Il quadro sulla resilienza operativa digitale per il settore finanziario istituito dal regolamento (UE) 2022/2554 prevede che le entità finanziarie stabiliscano alcuni principi fondamentali per la gestione 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.

(2) Le entità finanziarie, nel contesto del quadro per la gestione dei rischi informatici, sono tenute ad adottare, e a riesaminare periodicamente, una strategia per i rischi informatici derivanti da terzi. Ai sensi dell'articolo 28, paragrafo 2, del regolamento (UE) 2022/2554, tale strategia deve includere una politica per l'utilizzo dei servizi TIC a supporto di funzioni essenziali o importanti prestati da fornitori terzi. Essa si applica su base individuale e, se del caso, su base subconsolidata e consolidata.

(3) Le entità finanziarie variano notevolmente per dimensioni, struttura e organizzazione interna nonché per la natura e la complessità delle loro attività e operazioni. È necessario tenere conto di tale diversità, imponendo al contempo taluni requisiti normativi fondamentali che siano adeguati a tutte le entità finanziarie che elaborano la politica relativa agli accordi contrattuali per l'utilizzo di servizi TIC a supporto di funzioni essenziali o importanti prestati da fornitori terzi di servizi TIC («la politica»), e garantire che tali requisiti siano applicati in modo proporzionato.

(4) Nel caso in cui le entità finanziarie appartengano a un gruppo, l'impresa madre responsabile della redazione del bilancio consolidato o subconsolidato per il gruppo dovrebbe quindi garantire che la politica sia applicata in modo uniforme e coerente all'interno del gruppo.

(5) Nell'applicazione della politica è opportuno che i fornitori intragruppo di servizi TIC, compresi quelli interamente o collettivamente di proprietà di entità finanziarie nell'ambito dello stesso sistema di tutela istituzionale, siano considerati fornitori terzi di servizi TIC. I rischi posti dai fornitori intragruppo di servizi TIC possono essere diversi, ma le prescrizioni loro applicabili ai sensi del regolamento (UE) 2022/2554 sono le stesse. In modo analogo, la politica dovrebbe applicarsi ai subappaltatori che forniscono servizi TIC a supporto di funzioni essenziali o importanti o parti significative di essi a fornitori terzi di servizi TIC, laddove esista una catena di fornitori terzi di servizi TIC.

(6) La responsabilità finale dell'organo di gestione nell'affrontare i rischi informatici di un'entità finanziaria è un principio guida applicabile anche all'utilizzo di fornitori terzi di servizi TIC. Tale responsabilità dovrebbe tradursi nel costante coinvolgimento dell'organo di gestione nel controllo e nel monitoraggio della gestione dei rischi informatici, anche attraverso l'adozione e il riesame, almeno una volta all'anno, della politica.

([1]) GU L 333 del 27.12.2022, pag. 1, ELI: http://data.europa.eu/eli/reg/2022/2554/oj.

(7) Per garantire un'adeguata segnalazione all'organo di gestione la politica dovrebbe specificare e individuare chiaramente le responsabilità interne per l'approvazione, la gestione, il controllo e la documentazione degli accordi contrattuali per l'utilizzo di servizi TIC a supporto di funzioni essenziali o importanti prestati da fornitori terzi di servizi TIC («accordi contrattuali»), compresi i servizi TIC prestati nell'ambito degli accordi contrattuali di cui all'articolo 28, paragrafo 1, lettera a), del regolamento (UE) 2022/2554.

(8) Al fine di tenere conto di tutti i possibili rischi che possono sorgere quando si concludono contratti per la fornitura di servizi TIC a supporto di funzioni essenziali o importanti, la struttura della politica dovrebbe seguire tutti i passaggi di ciascuna fase principale del ciclo di vita degli accordi contrattuali con fornitori terzi.

(9) Per attenuare i rischi individuati la politica dovrebbe specificare la pianificazione degli accordi contrattuali, compresi la valutazione dei rischi, la dovuta diligenza e il processo di approvazione di nuovi accordi contrattuali o di modifiche sostanziali di tali accordi. Al fine di gestire i rischi che potrebbero insorgere prima di stipulare un accordo contrattuale con un fornitore terzo di servizi TIC, la politica dovrebbe specificare un processo adeguato e proporzionato per selezionare i potenziali fornitori terzi di servizi TIC e valutarne l'idoneità e prescrivere che l'entità finanziaria prenda in considerazione un elenco non esaustivo di elementi che i fornitori terzi di servizi TIC dovrebbero presentare. L'elenco dovrebbe includere elementi relativi alla reputazione commerciale dei fornitori di servizi, alle loro risorse finanziarie, umane e tecniche, alla loro sicurezza delle informazioni, alla loro struttura organizzativa, compresa la gestione dei rischi, e ai loro controlli interni.

(10) Per garantire una solida gestione dei rischi nella fornitura di servizi TIC a supporto di funzioni essenziali o importanti da parte di fornitori terzi di servizi TIC, la politica dovrebbe contenere informazioni sull'attuazione, sul monitoraggio e sulla gestione degli accordi contrattuali, anche a livello consolidato e subconsolidato, ove applicabile. Ciò include i requisiti relativi alle clausole contrattuali sugli obblighi reciproci delle entità finanziarie e dei fornitori terzi di servizi TIC, che è opportuno definire per iscritto. Per garantire una vigilanza efficace e promuovere la resilienza in caso di cambiamenti del modello o del contesto aziendale, la politica dovrebbe garantire il diritto delle entità finanziarie o di terze parti designate e delle autorità competenti di effettuare ispezioni e accedere alle informazioni, nonché specificare ulteriormente le strategie di uscita e i processi di risoluzione.

(11) Nella misura in cui i fornitori terzi di servizi TIC sono responsabili del trattamento dei dati personali, la politica e qualsiasi accordo contrattuale non pregiudicano e dovrebbero integrare gli obblighi previsti dal regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio ([2]), come ad esempio la stipula di un contratto scritto che descriva il trattamento dei dati personali, l'obbligo di garantire la sicurezza del trattamento dei dati personali e la definizione di tutti gli altri elementi previsti da tale regolamento.

([2]) 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, ELI: http://data.europa.eu/eli/reg/2016/679/oj).

(12) Il comitato congiunto delle autorità europee di vigilanza di cui all'articolo 54 del regolamento (UE) n. 1093/2010 del Parlamento europeo e del Consiglio ([3]), all'articolo 54 del regolamento (UE) n. 1094/2010 del Parlamento europeo e del Consiglio ([4]) e all'articolo 54 del regolamento (UE) n. 1095/2010 del Parlamento europeo e del Consiglio ([5]) ha condotto consultazioni pubbliche sul progetto di norme tecniche di regolamentazione su cui si basa il presente regolamento, ha analizzato i potenziali costi e benefici delle norme proposte e ha chiesto il parere del gruppo delle parti interessate nel settore bancario, istituito ai sensi dell'articolo 37 del regolamento (UE) n. 1093/2010, dei gruppi delle parti interessate nel settore dell'assicurazione e della riassicurazione e nel settore dei fondi pensionistici aziendali e professionali, istituiti ai sensi dell'articolo 37 del regolamento (UE) n. 1094/2010, e del gruppo delle parti interessate nel settore degli strumenti finanziari e dei mercati, istituito ai sensi dell'articolo 37 del regolamento (UE) n. 1095/2010.

(13) Conformemente all'articolo 42, paragrafo 1, del regolamento (UE) 2018/1725 del Parlamento europeo e del Consiglio ([6]), il Garante europeo della protezione dei dati è stato consultato e ha formulato il suo parere il 24 gennaio 2024,

HA ADOTTATO IL PRESENTE REGOLAMENTO:

Articolo 1

Profilo di rischio complessivo e complessità

La politica sull'utilizzo dei servizi TIC a supporto di funzioni essenziali o importanti prestati da fornitori terzi di servizi TIC (la «politica») tiene conto delle dimensioni e del profilo di rischio complessivo dell'entità finanziaria nonché della natura, della portata e degli elementi di maggiore o minore complessità dei suoi servizi, attività e operazioni, compresi gli elementi relativi a quanto segue:

a) il tipo di servizi TIC inclusi nell'accordo contrattuale per l'utilizzo di servizi TIC a supporto di funzioni essenziali o importanti prestati da fornitori terzi di servizi TIC (l'«accordo contrattuale») tra l'entità finanziaria e il fornitore terzo di servizi TIC;

b) la sede del fornitore terzo di servizi TIC o la sede della sua società madre;

c) se i servizi TIC a supporto di funzioni essenziali o importanti sono prestati da un fornitore terzo di servizi TIC situato all'interno di uno Stato membro o in un paese terzo, considerando anche il luogo da cui sono prestati i servizi TIC e il luogo in cui i dati sono trattati e conservati;

d) la natura dei dati condivisi con il fornitore terzo di servizi TIC;

e) se il fornitore terzo di servizi TIC fa parte dello stesso gruppo dell'entità finanziaria a cui sono prestati i servizi;

([3]) 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, ELI: http://data.europa.eu/eli/reg/2010/1093/oj).

([4]) 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, ELI: http://data.europa.eu/eli/reg/2010/1094/oj).

([5]) 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, ELI: http://data.europa.eu/eli/reg/2010/1095/oj).

([6]) 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, ELI: http://data.europa.eu/eli/reg/2018/1725/oj).

f) il ricorso a fornitori terzi di servizi TIC che sono autorizzati, registrati o soggetti a vigilanza o sorveglianza da parte di un'autorità competente in uno Stato membro o che sono soggetti al quadro di sorveglianza di cui al capo V, sezione II, del regolamento (UE) 2022/2554, e il ricorso a fornitori terzi di servizi TIC che non lo sono;

g) il ricorso a fornitori terzi di servizi TIC che sono autorizzati, registrati o soggetti a vigilanza o sorveglianza da parte di un'autorità di vigilanza in un paese terzo e il ricorso a fornitori terzi di servizi TIC che non lo sono;

h) se la fornitura di servizi TIC a supporto di funzioni essenziali o importanti è concentrata su un unico fornitore terzo di servizi TIC o su un numero ridotto di tali fornitori;

i) la trasferibilità dei servizi TIC a supporto di funzioni essenziali o importanti a un altro fornitore terzo di servizi TIC, anche in ragione di specificità tecnologiche;

j) il potenziale impatto di perturbazioni nella fornitura dei servizi TIC a supporto di funzioni essenziali o importanti sulla continuità delle attività dell'entità finanziaria e sulla disponibilità dei suoi servizi.

Articolo 2

Applicazione a livello di gruppo

Quando il presente regolamento si applica su base subconsolidata o consolidata, l'impresa madre responsabile della redazione del bilancio consolidato o subconsolidato del gruppo garantisce che la politica sia attuata in modo coerente in tutte le entità finanziarie che fanno parte del gruppo e sia adeguata per un'applicazione efficace del presente regolamento a tutti i livelli pertinenti del gruppo.

Articolo 3

Meccanismi di governance

1. L'organo di gestione riesamina la politica almeno una volta all'anno e la aggiorna se necessario. Le modifiche apportate alla politica sono attuate in modo tempestivo e non appena possibile nell'ambito degli accordi contrattuali pertinenti. L'entità finanziaria documenta la tempistica prevista per l'attuazione.

2. La politica stabilisce o fa riferimento a una metodologia per determinare quali sono i servizi TIC a supporto di funzioni essenziali o importanti. La politica specifica inoltre quando tale valutazione deve essere condotta e riesaminata.

3. La politica assegna chiaramente le responsabilità interne per l'approvazione, la gestione, il controllo e la documentazione dei pertinenti accordi contrattuali e assicura che all'interno dell'entità finanziaria siano mantenute le competenze, l'esperienza e le conoscenze adeguate a supervisionare efficacemente i pertinenti accordi contrattuali, compresi i servizi TIC forniti nell'ambito di tali accordi.

4. Fatta salva la responsabilità finale dell'entità finanziaria di supervisionare efficacemente gli accordi contrattuali pertinenti, la politica impone di valutare se il fornitore terzo di servizi TIC dispone di risorse sufficienti a garantire il rispetto da parte dell'entità finanziaria di tutti i requisiti di natura legale e regolamentare relativi ai servizi TIC a supporto di funzioni essenziali o importanti che sono prestati.

5. La politica individua chiaramente il ruolo o il dirigente di rango elevato responsabile del monitoraggio degli accordi contrattuali pertinenti. La politica specifica le modalità di collaborazione tra il ruolo o il dirigente di rango elevato e le funzioni di controllo, salvo nel caso in cui ne faccia parte, e definisce le linee gerarchiche di comunicazione all'organo di gestione, compresi la natura delle informazioni da comunicare e i documenti da fornire. Essa stabilisce altresì la frequenza di tale comunicazione.

6. La politica garantisce che gli accordi contrattuali siano coerenti con:

a) il quadro per la gestione dei rischi informatici di cui all'articolo 6 del regolamento (UE) 2022/2554;

b) la politica di sicurezza dell'informazione di cui all'articolo 9, paragrafo 4, del regolamento (UE) 2022/2554;

c) la politica di continuità operativa delle TIC di cui all'articolo 11 del regolamento (UE) 2022/2554;

d) gli obblighi di segnalazione degli incidenti di cui all'articolo 19 del regolamento (UE) 2022/2554.

7. La politica impone che i servizi TIC a supporto di funzioni essenziali o importanti prestati da fornitori terzi di servizi TIC siano soggetti a un riesame indipendente e siano inclusi nel piano di audit.

8. La politica specifica esplicitamente che gli accordi contrattuali:

a) non sollevano l'entità finanziaria e il suo organo di gestione dagli obblighi regolamentari e dalle responsabilità nei confronti dei clienti;

b) non devono impedire l'efficace vigilanza dell'entità finanziaria e non devono contravvenire a eventuali restrizioni di vigilanza sui servizi e sulle attività;

c) devono prescrivere che i fornitori terzi di servizi TIC collaborino con le autorità competenti;

d) devono prescrivere che l'entità finanziaria, i suoi revisori e le autorità competenti abbiano effettivo accesso ai dati e ai locali connessi all'utilizzo dei servizi TIC a supporto di funzioni essenziali o importanti.

Articolo 4

Fasi principali del ciclo di vita degli accordi contrattuali

La politica specifica le prescrizioni, compresi le regole, le responsabilità e i processi, per ciascuna fase principale del ciclo di vita dell'accordo contrattuale, riguardanti almeno gli aspetti seguenti:

a) le responsabilità dell'organo di gestione, compreso il suo coinvolgimento, se del caso, nel processo decisionale sull'utilizzo di servizi TIC a supporto di funzioni essenziali o importanti prestati da fornitori terzi di servizi TIC;

b) la pianificazione degli accordi contrattuali, tra cui la valutazione dei rischi, la dovuta diligenza di cui agli articoli 5 e 6 e il processo di approvazione di nuovi accordi o di modifiche sostanziali di tali accordi di cui all'articolo 8, paragrafo 4;

c) il coinvolgimento delle unità aziendali, dei controlli interni e di altre unità pertinenti in relazione agli accordi contrattuali;

d) l'attuazione, il monitoraggio e la gestione degli accordi contrattuali di cui agli articoli 7, 8 e 9, anche a livello consolidato e subconsolidato, ove applicabile;

e) la documentazione e la tenuta dei registri, tenendo conto degli obblighi relativi al registro di informazioni di cui all'articolo 28, paragrafo 3, del regolamento (UE) 2022/2554;

f) le strategie di uscita e i processi di risoluzione di cui all'articolo 10.

Articolo 5

Valutazione dei rischi ex ante

1. La politica prevede che le esigenze aziendali dell'entità finanziaria siano definite prima della conclusione di un accordo contrattuale.

2. La politica prevede che prima della conclusione di un accordo contrattuale sia effettuata una valutazione dei rischi a livello di entità finanziaria e, ove applicabile, a livello consolidato e subconsolidato.

La valutazione dei rischi tiene conto di tutti i pertinenti requisiti stabiliti dal regolamento (UE) 2022/2554 e dalla legislazione settoriale dell'Unione applicabile. Essa considera, in particolare, l'impatto della fornitura di servizi TIC a supporto di funzioni essenziali o importanti da parte di fornitori terzi di servizi TIC sull'entità finanziaria e tutti i rischi posti dalla fornitura di tali servizi TIC a supporto di funzioni essenziali o importanti da parte di fornitori terzi di servizi TIC, tra cui:

a) i rischi operativi;

b) i rischi giuridici;

c) i rischi informatici;

d) i rischi reputazionali;

e) i rischi legati alla protezione dei dati riservati o personali;

f) i rischi legati alla disponibilità dei dati;

g) i rischi legati al luogo in cui i dati sono trattati e conservati;

h) i rischi legati alla località in cui si trova il fornitore terzo di servizi TIC;

i) i rischi di concentrazione delle TIC a livello di entità.

Articolo 6

Dovuta diligenza

1. La politica definisce un processo adeguato e proporzionato per la selezione e la valutazione dei potenziali fornitori terzi di servizi TIC, che consideri se il fornitore terzo di servizi TIC sia o no un fornitore di servizi TIC infragruppo, e prevede che l'entità finanziaria valuti, prima di concludere un accordo contrattuale, se il fornitore terzo di servizi TIC:

a) gode della reputazione commerciale, possiede sufficienti capacità e competenze nonché adeguate risorse finanziarie, umane e tecniche, è dotato di standard in materia di sicurezza dell'informazione e di una struttura organizzativa adeguata, attua la gestione dei rischi e i controlli interni e, se del caso, dispone delle necessarie autorizzazioni o registrazioni per fornire i servizi TIC a supporto della funzione essenziale o importante in modo affidabile e professionale;

b) possiede la capacità di monitorare i pertinenti sviluppi tecnologici e di individuare le pratiche di punta in materia di sicurezza delle TIC e di attuarle, ove opportuno, per disporre di un quadro di resilienza operativa digitale efficace e solido;

c) ricorre o intende ricorrere a subappaltatori TIC per l'esecuzione dei servizi TIC a supporto di funzioni essenziali o importanti o di parti significative di essi;

d) è situato in un paese terzo oppure tratta o conserva i dati in un paese terzo e, in tal caso, se tale pratica incide sul livello dei rischi operativi o reputazionali o sul rischio di incorrere in misure restrittive, inclusi embarghi e sanzioni, che potrebbero influire sulla capacità del fornitore terzo di servizi TIC di prestare i servizi TIC o dell'entità finanziaria di ricevere tali servizi TIC;

e) aderisce ad accordi contrattuali che garantiscono all'entità finanziaria stessa, a terze parti designate e alle autorità competenti l'effettiva possibilità di effettuare audit presso il fornitore terzo di servizi TIC, anche in loco;

f) agisce in modo etico e socialmente responsabile, rispetta i diritti umani e i diritti dei minori, compreso il divieto di lavoro minorile, rispetta i principi applicabili in materia di tutela ambientale e garantisce condizioni di lavoro adeguate.

2. La politica specifica il livello di garanzia richiesto in merito all'efficacia del quadro per la gestione dei rischi dei fornitori terzi di servizi TIC per i servizi TIC a supporto di funzioni essenziali o importanti che devono essere prestati da un fornitore terzo. La politica prevede che il processo di dovuta diligenza includa una valutazione dell'esistenza, presso il fornitore terzo di servizi TIC, di misure di attenuazione dei rischi e di continuità operativa e delle modalità per garantirne il funzionamento.

3. La politica stabilisce il processo di dovuta diligenza per la selezione e la valutazione dei potenziali fornitori terzi di servizi TIC e indica quali degli elementi seguenti devono essere utilizzati per il livello di garanzia richiesto in merito alle prestazioni del fornitore terzo di servizi TIC:

a) audit o valutazioni indipendenti effettuati dall'entità finanziaria stessa o per suo conto;

b) relazioni di audit indipendenti redatte su richiesta del fornitore terzo di servizi TIC;

c) relazioni di audit effettuate dalla funzione di audit interno del fornitore terzo di servizi TIC;

d) idonee certificazioni di terze parti;

e) altre informazioni pertinenti a disposizione dell'entità finanziaria o altre informazioni provenienti dal fornitore terzo di servizi TIC.

4. Le entità finanziarie assicurano un livello adeguato di garanzia in merito alle prestazioni del fornitore terzo di servizi TIC, tenendo conto degli elementi elencati al paragrafo 3, lettere da a) a e). Ove opportuno, si utilizza più di un elemento elencato alle lettere di cui sopra.

Articolo 7

Conflitti di interessi

1. La politica specifica le opportune misure per individuare, prevenire e gestire i conflitti di interessi effettivi o potenziali derivanti dal ricorso a fornitori terzi di servizi TIC, da adottare prima di concludere gli accordi contrattuali pertinenti, e prevede un monitoraggio continuo di tali conflitti di interessi.

2. Qualora i servizi TIC a supporto di funzioni essenziali o importanti siano prestati da fornitori intragruppo di servizi TIC, la politica specifica che le decisioni sulle condizioni, comprese quelle finanziarie, per i servizi TIC devono essere prese in modo obiettivo.

Articolo 8

Clausole contrattuali

1. La politica specifica che gli accordi contrattuali pertinenti devono essere in forma scritta e devono includere tutti gli elementi di cui all'articolo 30, paragrafi 2 e 3, del regolamento (UE) 2022/2554. La politica comprende anche elementi relativi agli obblighi di cui all'articolo 1, paragrafo 1, lettera a), del regolamento (UE) 2022/2554 nonché ad altre normative nazionali e dell'Unione pertinenti, a seconda dei casi.

2. La politica specifica che gli accordi contrattuali pertinenti devono includere il diritto dell'entità finanziaria di accedere alle informazioni, di effettuare ispezioni e audit e di eseguire test sulle TIC. A tal fine, fatta salva la responsabilità finale dell'entità finanziaria, la politica prevede che l'entità finanziaria utilizzi i metodi seguenti:

a) il proprio audit interno o un audit condotto da una terza parte designata;

b) se del caso, audit e test TIC congiunti, compresi i test di penetrazione guidati dalla minaccia, organizzati congiuntamente con altre entità finanziarie o imprese contraenti che utilizzano i servizi TIC dello stesso fornitore terzo di servizi TIC e che sono eseguiti da tali entità finanziarie o imprese contraenti o da una terza parte da loro designata;

c) se del caso, certificazioni di terze parti;

d) se del caso, relazioni di audit interni o di terze parti rese disponibili dal fornitore terzo di servizi TIC.

3. Nel tempo l'entità finanziaria non si affida esclusivamente alle certificazioni di cui al paragrafo 2, lettera c), o alle relazioni di audit di cui alla lettera d) del medesimo paragrafo. La politica consente l'utilizzo dei metodi di cui al paragrafo 2, lettere c) e d), solo se l'entità finanziaria:

a) è soddisfatta del piano di audit del fornitore terzo di servizi TIC per gli accordi contrattuali pertinenti;

b) si assicura che le certificazioni o le relazioni di audit coprono i sistemi e i controlli essenziali da essa individuati e garantisce la conformità ai requisiti regolamentari pertinenti;

c) valuta in modo accurato il contenuto delle certificazioni o delle relazioni di audit su base continuativa e verifica che le relazioni o le certificazioni non siano obsolete;

d) si assicura che i sistemi e i controlli essenziali siano coperti nelle versioni future della certificazione o della relazione di audit;

e) è soddisfatta dell'idoneità del soggetto incaricato della certificazione o dell'audit;

f) è certa che le certificazioni siano rilasciate e che gli audit siano eseguiti sulla base di norme professionali pertinenti ampiamente riconosciute e includano un test dell'efficacia operativa dei controlli essenziali in essere;

g) ha il diritto contrattuale di richiedere, con una frequenza ragionevole e legittima dal punto di vista della gestione dei rischi, che l'ambito delle certificazioni o delle relazioni di audit sia modificato per ricomprendere altri sistemi e controlli pertinenti;

h) ha il diritto contrattuale di eseguire audit individuali e congiunti a sua discrezione in relazione agli accordi contrattuali e di esercitare tali diritti in linea con la frequenza concordata.

4. La politica garantisce che le modifiche sostanziali dell'accordo contrattuale siano formalizzate in un documento scritto recante la data e la firma di tutte le parti e specifica il processo di rinnovo degli accordi contrattuali.

Articolo 9

Monitoraggio degli accordi contrattuali

1. La politica prescrive che gli accordi contrattuali specifichino le misure e gli indicatori chiave per monitorare, su base continuativa, le prestazioni dei fornitori terzi di servizi TIC, comprese le misure per monitorare la conformità ai requisiti di riservatezza, disponibilità, integrità e autenticità dei dati e delle informazioni, e la conformità dei fornitori terzi di servizi TIC alle politiche e alle procedure pertinenti dell'entità finanziaria. La politica specifica anche le misure applicabili in caso di mancato rispetto degli accordi sul livello dei servizi, comprese le penali contrattuali, se del caso.

2. La politica specifica le modalità con cui l'entità finanziaria è tenuta a valutare se i fornitori terzi di servizi TIC utilizzati per i servizi TIC a supporto di funzioni essenziali o importanti soddisfano standard di prestazione e di qualità adeguati, in linea con l'accordo contrattuale e con le politiche dell'entità finanziaria stessa. La politica garantisce in particolare:

a) che i fornitori terzi di servizi TIC forniscano all'entità finanziaria relazioni adeguate sulle loro attività e sui loro servizi, tra cui relazioni periodiche, relazioni sugli incidenti, relazioni sull'erogazione dei servizi, relazioni sulla sicurezza delle TIC e relazioni sulle misure e sui test di continuità operativa;

b) che le prestazioni dei fornitori terzi di servizi TIC siano valutate mediante indicatori chiave di prestazione, indicatori chiave di controllo, audit, autocertificazioni e revisioni indipendenti in linea con il quadro per la gestione dei rischi informatici dell'entità finanziaria;

c) che l'entità finanziaria riceva altre informazioni pertinenti dai fornitori terzi di servizi TIC;

d) che all'entità finanziaria siano notificati, se del caso, gli incidenti connessi alle TIC e gli incidenti operativi o di sicurezza dei pagamenti;

e) che si proceda a revisioni e audit indipendenti che verifichino la conformità alle politiche e ai requisiti di natura legale e regolamentare.

3. La politica specifica che la valutazione di cui al paragrafo 2 deve essere documentata e i suoi risultati devono essere utilizzati per aggiornare la valutazione dei rischi dell'entità finanziaria di cui all'articolo 6.

4. La politica stabilisce le opportune misure che l'entità finanziaria deve adottare se individua carenze dei fornitori terzi di servizi TIC, compresi gli incidenti connessi alle TIC e gli incidenti operativi o di sicurezza dei pagamenti, nella fornitura di servizi TIC a supporto di funzioni essenziali o importanti o nel rispetto degli accordi contrattuali o dei requisiti di natura legale. Essa specifica inoltre le modalità di monitoraggio dell'attuazione di tali misure, al fine di garantirne l'effettiva osservanza entro un periodo di tempo definito, tenendo conto della rilevanza delle carenze.

Articolo 10

Uscita dagli accordi contrattuali e risoluzione degli stessi

La politica contiene prescrizioni per un piano di uscita documentato per ciascun accordo contrattuale e per la revisione e i test periodici del piano di uscita documentato. Nel definire il piano di uscita, si tiene conto degli aspetti seguenti:

a) interruzioni del servizio impreviste e persistenti;

b) inadeguata o mancata erogazione dei servizi;

c) risoluzione inattesa dell'accordo contrattuale.

Il piano di uscita è realistico, fattibile, basato su scenari plausibili e ipotesi ragionevoli e prevede un calendario di attuazione compatibile con le condizioni di uscita e di risoluzione stabilite negli accordi contrattuali.

Articolo 11

Entrata in vigore

Il presente regolamento entra in vigore il ventesimo giorno successivo alla pubblicazione nella *Gazzetta ufficiale dell'Unione europea*.

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

Fatto a Bruxelles, il 13 marzo 2024

Per la Commissione
La presidente
Ursula VON DER LEYEN