

CC 2024 34

5 giugno 2024

Orientamenti congiunti

sulla stima dei costi e delle perdite annuali aggregati causati da gravi incidenti connessi alle TIC a norma del regolamento (UE) 2022/2554

I presenti orientamenti contengono riferimenti a regolamenti delegati e di esecuzione della Commissione europea non ancora pubblicati nella Gazzetta ufficiale dell'UE. Una volta che tali regolamenti saranno stati pubblicati nella Gazzetta ufficiale, i presenti orientamenti saranno integrati con i riferimenti pertinenti, che saranno inseriti nelle sezioni evidenziate in giallo.

La data di applicazione dei presenti orientamenti potrà essere determinata solo dopo il loro completamento. La data di applicazione prevista dei presenti orientamenti è il 17 gennaio 2025. In caso di ritardo nel completamento dei presenti orientamenti, il termine ultimo per l'applicazione sarà due mesi dopo la data di pubblicazione delle loro traduzioni in tutte le lingue ufficiali dell'UE.

Orientamenti congiunti sulla stima dei costi e delle perdite annuali aggregati causati da gravi incidenti connessi alle TIC

Status giuridico dei presenti orientamenti

Il presente documento contiene orientamenti congiunti emanati ai sensi dell'articolo 16 del regolamento (UE) n. 1093/2010 (¹), dell'articolo 16 del regolamento (UE) n. 1094/2010 (²) e dell'articolo 16 del regolamento (UE) n. 1095/2010 (³) (i «regolamenti delle AEV»). Conformemente all'articolo 16, paragrafo 3, dei regolamenti delle AEV pertinenti, le autorità competenti e gli istituti finanziari compiono ogni sforzo per conformarsi agli orientamenti.

Gli orientamenti congiunti definiscono il punto di vista delle AEV sulle prassi di vigilanza adeguate all'interno del Sistema europeo di vigilanza finanziaria o sulle modalità di applicazione del diritto dell'Unione in un determinato settore. Le autorità competenti cui si applicano gli orientamenti congiunti sono tenute a conformarsi a questi ultimi integrandoli opportunamente nelle rispettive prassi di vigilanza (per esempio modificando il proprio quadro giuridico o le proprie procedure di vigilanza), anche quando gli orientamenti congiunti sono diretti principalmente agli enti.

Obblighi di segnalazione

Entro il 19.05.2025 (due mesi dalla pubblicazione), ai sensi dell'articolo 16, paragrafo 3, dei regolamenti delle AEV, le autorità competenti devono comunicare alla rispettiva AEV se sono conformi o intendono conformarsi ai presenti orientamenti congiunti / alle presenti raccomandazioni congiunte oppure comunicare i motivi del mancato rispetto. Qualora entro il termine indicato non sia pervenuta alcuna comunicazione da parte delle autorità competenti, queste sono ritenute non conformi dalla rispettiva AEV. Le comunicazioni devono essere inviate a compliance@eba.europa.eu, compliance@eiopa.europa.eu e DORA@esma.europa.eu con il riferimento «JC/GL/2024/34». Sui siti web delle AEV è disponibile un modello per le comunicazioni. Le comunicazioni devono essere trasmesse da persone debitamente autorizzate a segnalare la conformità per conto delle rispettive autorità competenti.

Le comunicazioni sono pubblicate sui siti web delle AEV ai sensi dell'articolo 16, paragrafo 3.

(¹) 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).

(²) 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, pagg. 48–83).

(³) 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, pagg. 84–119).

Titolo I – Oggetto, ambito di applicazione e definizioni

Oggetto e ambito di applicazione

1. I presenti orientamenti sono destinati ad adempiere il mandato conferito alle AEV a norma dell'articolo 11, paragrafo 11, del regolamento (UE) 2022/2554 ⁽⁴⁾ di elaborare orientamenti congiunti sulla stima dei costi e delle perdite annuali aggregati causati da gravi incidenti connessi alle TIC di cui all'articolo 11, paragrafo 10, di tale regolamento. I presenti orientamenti specificano anche un modello comune per la presentazione dei costi e delle perdite annuali aggregati.

Destinatari

2. I presenti orientamenti sono rivolti alle autorità competenti di cui all'articolo 46 del regolamento (UE) 2022/2554 e agli istituti finanziari di cui all'articolo 4, paragrafo 1, del regolamento (UE) n. 1093/2010, all'articolo 4, paragrafo 1, del regolamento (UE) n. 1094/2010 e all'articolo 4, paragrafo 1, del regolamento (UE) n. 1095/2010.

Definizioni

3. I termini utilizzati e definiti nel regolamento (UE) 2022/2554 hanno lo stesso significato nei presenti orientamenti.

Titolo II – Attuazione

Data di applicazione

4. I presenti orientamenti si applicano a decorrere dal 19.05.2025.

⁽⁴⁾ 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, pagg. 1–79).

Titolo III – Disposizioni sulla stima dei costi e delle perdite annuali aggregati causati da gravi incidenti connessi alle TIC

5. Le entità finanziarie dovrebbero stimare i costi e le perdite annuali aggregati causati da gravi incidenti connessi alle TIC aggregando i costi e le perdite causati da gravi incidenti connessi alle TIC che rientrano nell'anno di riferimento per il quale l'autorità competente ha richiesto la stima. L'entità finanziaria può decidere se l'anno di riferimento debba corrispondere all'anno civile concluso o all'esercizio contabile concluso dell'entità finanziaria per il quale quest'ultima ha ultimato i suoi rendiconti finanziari. Una volta che l'entità finanziaria ha deciso se fornire la stima sulla base dell'anno civile o del suo esercizio contabile, tale decisione dovrebbe essere applicata alle stime future dei costi e delle perdite annuali aggregati. L'entità finanziaria può modificare tale decisione dandone notifica all'autorità competente e a condizione che quest'ultima non sollevi obiezioni entro due mesi dal ricevimento della notifica. Le entità finanziarie non dovrebbero includere i costi e le perdite causati dagli incidenti che si verificano prima o dopo l'anno di riferimento.
6. Le entità finanziarie dovrebbero includere nella stima tutti gli incidenti connessi alle TIC che, indipendentemente dal motivo, sono stati classificati come gravi conformemente al regolamento delegato della Commissione [OJ L, 2024/1772, 25.6.2024]⁵ sulla classificazione degli incidenti e
 - (a) per i quali l'entità finanziaria ha presentato una relazione finale a norma dell'articolo 19, paragrafo 4, lettera c), del regolamento (UE) 2022/2554 nell'anno di riferimento pertinente, o
 - (b) qualsiasi incidente per il quale l'entità finanziaria ha presentato negli anni di riferimento precedenti una relazione finale a norma dell'articolo 19, paragrafo 4, lettera c), del regolamento (UE) 2022/2554 che ha avuto un impatto finanziario quantificabile sull'entità finanziaria nell'anno di riferimento pertinente.
7. Le entità finanziarie dovrebbero stimare i costi e le perdite annuali aggregati applicando le seguenti fasi in sequenza:
 - (a) stimare singolarmente i costi e le perdite causati da ciascun grave incidente connesso alle TIC di cui al paragrafo 6. Tali stime dovrebbero produrre i costi e le perdite lordi tenendo conto dei tipi di costi e perdite di cui all'articolo 7, paragrafi 1 e 2, del regolamento delegato della Commissione [OJ L, 2024/1772, 25.6.2024];

⁵ Regolamento delegato (UE) 2024/1772 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 specificano i criteri per la classificazione degli incidenti connessi alle TIC e delle minacce informatiche, stabiliscono le soglie di rilevanza e specificano i dettagli delle segnalazioni di gravi incidenti, [OJ L, 2024/1772, 25.6.2024, ELI: http://data.europa.eu/eli/reg_del/2024/1772/oj]

- (b) per ciascun grave incidente connesso alle TIC, le entità finanziarie dovrebbero stimare anche i recuperi finanziari come specificato nell'allegato II del regolamento di esecuzione della Commissione [OJ L, 2025/302, 20.2.2025]⁶;
- (c) le entità finanziarie dovrebbero aggregare i costi e le perdite lordi e i recuperi finanziari relativi a tutti i gravi incidenti connessi alle TIC.
8. Come base per le stime, le entità finanziarie dovrebbero fare riferimento ai costi, alle perdite e ai recuperi finanziari indicati nei loro rendiconti finanziari, come il conto profitti e perdite o, se del caso, nelle loro segnalazioni a fini di vigilanza dell'anno di riferimento pertinente. Le entità finanziarie dovrebbero includere nella stima anche gli accantonamenti contabili indicati nei loro rendiconti finanziari, come il conto profitti e perdite dell'anno di riferimento pertinente. Qualora non siano disponibili dati accurati, le entità finanziarie dovrebbero basare la stima, per quanto possibile, su altri dati e informazioni disponibili.
9. Le entità finanziarie dovrebbero includere gli adeguamenti dei costi e delle perdite di una stima presentata per un anno precedente nella stima dell'anno di riferimento pertinente in cui gli adeguamenti sono effettuati.
10. Le entità finanziarie dovrebbero includere nella relazione della stima dei costi e delle perdite annuali aggregati anche la scomposizione dei costi e delle perdite lordi e dei recuperi finanziari per ciascun grave incidente connesso alle TIC incluso nell'aggregazione.
11. Le entità finanziarie dovrebbero utilizzare il modello di cui all'allegato per trasmettere all'autorità competente la stima dei costi e delle perdite annuali aggregati per l'anno di riferimento. Per ciascuna voce di cui ai paragrafi 6 e 9 inclusa nella stima dell'anno di riferimento, le entità finanziarie dovrebbero utilizzare gli stessi codici di riferimento per gli incidenti forniti dall'entità finanziaria stessa utilizzati nella relazione finale trasmessa ai sensi dell'articolo 19, paragrafo 4, lettera c), del regolamento (UE) 2022/2554.

⁶Regolamento di esecuzione (UE) 2025/302 della Commissione, del 23 ottobre 2024, che stabilisce norme tecniche di attuazione per l'applicazione del regolamento (UE) 2022/2554 del Parlamento europeo e del Consiglio per quanto riguarda i formati, i modelli e le procedure standard con cui le entità finanziarie devono segnalare un incidente grave connesso alle TIC e notificare una minaccia informatica significativa, [OJ L, 2025/302, 20.2.2025, ELI: http://data.europa.eu/eli/reg_impl/2025/302/oj]

Allegato: modello per la comunicazione dei costi e delle perdite lordi e dei recuperi finanziari in un anno di riferimento

Nome dell'entità finanziaria				
Identificativo dell'entità giuridica				
Data di inizio e di fine dell'anno di riferimento dell'entità finanziaria				
Valuta				
Numero di incidente	Data di trasmissione della relazione finale sull'incidente	Numero di riferimento dell'incidente	Costi e perdite lordi causati dall'incidente nell'anno di riferimento (migliaia di unità)	Recuperi dell'incidente nell'anno di riferimento (migliaia di unità)
1				
2				
...				
Totale per l'anno di riferimento	-----	-----		