BANCA D'ITALIA
EUROSISTEMA

Regolamento (UE) 2022/2554 del Parlamento europeo e del Consiglio del 14 dicembre 2022 relativo alla resilienza operativa digitale per il settore finanziario (Regolamento DORA)

Comunicazione della Banca d'Italia

Dicembre 2024

1. Premessa

Il 27 dicembre 2022 è stato pubblicato sulla Gazzetta Ufficiale dell'Unione Europea il Regolamento sulla resilienza operativa digitale del settore finanziario (*Digital Operational Resilience Act*, DORA), entrato in vigore il 16 gennaio 2023[1]. Il Regolamento DORA (o, nel prosieguo, Regolamento) mira a favorire l'armonizzazione dei requisiti di resilienza digitale per tutto il settore finanziario europeo e disciplina i seguenti profili:

1) gestione del rischio ICT: si introduce un *framework* armonizzato in materia di *governance* del rischio ICT, in continuità con gli Orientamenti dell'EBA sulla gestione dei rischi relativi alle tecnologie dell'informazione e della comunicazione (*Information and Communication Technology* - ICT) e di sicurezza (EBA/GL/2019/04) rivolti a banche, IP e IMEL e già recepiti nelle disposizioni di vigilanza della Banca d'Italia applicabili a questi intermediari[2];

2) ICT *incident reporting*: si introducono processi e criteri armonizzati per la classificazione, registrazione e gestione degli incidenti ICT e delle minacce informatiche, nonché obblighi di segnalazione degli incidenti ICT gravi e procedure per la notifica volontaria delle minacce informatiche significative;

3) test di resilienza operativa digitale: si rende obbligatorio lo svolgimento di prove avanzate di resilienza operativa dei sistemi ICT;

4) gestione del rischio di terze parti derivante dal ricorso ai *service provider* ICT: si sottopongono le entità finanziarie a presidi in linea con quelli previsti dagli Orientamenti dell'EBA in materia di esternalizzazione (EBA/GL/2019/02) e si introduce un regime europeo di *oversight* sui *provider* ICT critici;

5) *infosharing*: si promuovono meccanismi volontari di condivisione delle informazioni a livello dell'Unione, volti ad aiutare 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.

Il Regolamento DORA ha previsto inoltre una intensa attività tecnico-regolamentare di secondo livello da parte delle tre *European Supervisory Authorities* (ESAs), con la predisposizione di *Regulatory Technical Standards* (RTS), *Implementing Technical Standards* (ITS) e linee guida e/o rapporti. Alcuni di questi mandati sono già stati portati a termine dalle ESAs, per altri si è ancora in attesa dell'adozione dei regolamenti delegati da parte della Commissione europea.

Il 4 dicembre 2024 le ESAs hanno pubblicato uno *statement* nel quale si richiama l'attenzione del mercato sulla prima applicazione del Regolamento DORA[3].

---

[1] 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.

[2] Per le banche, Circolare della Banca d'Italia del 17 dicembre 2013, n. 285 (e successivi aggiornamenti); per gli IP e IMEL, Disposizioni di vigilanza per gli istituti di pagamento e gli istituti di moneta elettronica del 17 maggio 2016 (e successivi aggiornamenti).

[3] Cfr. JC 2024 99.

Ai sensi dell'articolo 64 del Regolamento DORA, le previsioni in esso contenute si applicano a decorrere dal **17 gennaio 2025**. Esse, come pure i relativi atti delegati, sono direttamente applicabili. Con l'avvio del nuovo regime si ritiene opportuno richiamare l'attenzione degli intermediari sottoposti alla vigilanza prudenziale della Banca d'Italia che rientrano nella definizione di "entità finanziaria" del Regolamento DORA (*i.e.*, banche, imprese di investimento, gestori, istituti di pagamento, istituti di moneta elettronica, emittenti di *token* collegati ad attività, prestatori di servizi per le cripto-attività, fornitori di servizi di *crowdfunding* – di seguito, "intermediari") su alcuni profili, rispetto ai quali si forniscono di seguito indicazioni per consentire un'applicazione uniforme del Regolamento DORA[4].

2. Profili di attenzione per l'applicazione del Regolamento DORA

2.1. Collocazione della funzione di controllo dei rischi ICT

Ai sensi del Regolamento DORA (articolo 6), le entità finanziarie sono tenute a predisporre, monitorare e aggiornare nel tempo un quadro per la gestione dei rischi informatici solido, esaustivo e adeguatamente documentato, che consenta di affrontare tali rischi in maniera rapida, efficiente ed esaustiva, attraverso una strategia di resilienza operativa digitale. Fermo restando quanto previsto dall'articolo 16, comma 1, del Regolamento DORA, le entità finanziarie diverse dalle microimprese[5] attribuiscono la responsabilità della gestione dei rischi informatici a una funzione di controllo (di seguito, "funzione di controllo ICT"), che deve avere un livello appropriato d'indipendenza, al fine di evitare conflitti d'interessi. Il Regolamento non definisce tuttavia specifiche regole sulla collocazione organizzativa di tale funzione, considerato che le diverse entità finanziarie hanno, in base alle discipline settoriali, meccanismi differenti di governo societario e di controlli interni.

In assenza – allo stato – di diverse indicazioni nella complessiva disciplina europea, si ritiene, nel rispetto dei principi di proporzionalità e di neutralità organizzativa, che sia compatibile con il Regolamento DORA che gli intermediari facciano leva sul modello di *governance* e sul sistema dei controlli interni adottati ai sensi della propria disciplina settoriale, opportunamente integrati per tenere conto di tutte le nuove previsioni del Regolamento.

In particolare, gli intermediari potranno valutare se istituire o confermare un'autonoma funzione di controllo ICT, avente i requisiti delle funzioni aziendali di controllo di secondo livello, oppure attribuire i compiti della funzione di controllo ICT alla funzione di *risk management* e a quella di *compliance*, ove istituite, in relazione ai ruoli, alle responsabilità e alle competenze proprie delle due funzioni, oppure affidare lo svolgimento della funzione di controllo ICT alla struttura che svolge la funzione di *risk management* o a quella che svolge la funzione di *compliance*. Nei casi in cui le funzioni di *risk management* e di *compliance* siano affidate a un'unica struttura, anche la funzione di controllo ICT può essere affidata a quest'ultima.

---

[4] Nella "Legge di delegazione europea 2022-2023" (legge 21 febbraio 2024, n. 15, come emendata dalla legge 28 giugno 2024, n. 90, recante disposizioni in materia di rafforzamento della cybersicurezza nazionale e di reati informatici) è incluso un criterio di delega specifico per individuare idonei presidi di resilienza operativa digitale, in linea con gli obiettivi del Regolamento DORA, per gli intermediari finanziari *ex* articolo 106 del TUB e per Poste Italiane S.p.A. per l'attività del Patrimonio Bancoposta, che non sono direttamente ricompresi nel campo di applicazione del Regolamento.

[5] Ai sensi del Regolamento DORA (art. 3, punto 60), per "microimpresa" si intende "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 euro."

In ogni caso, la scelta sulla collocazione organizzativa della funzione di controllo ICT non deve pregiudicare l'efficace svolgimento di tutti i compiti ad essa attribuiti per la gestione e la supervisione dei rischi ICT previsti dal *framework* DORA.

La funzione di controllo ICT non può in ogni caso essere affidata alla struttura che svolge la funzione di *internal audit*.

2.2. Comunicazione all'autorità competente di eventuali accordi contrattuali previsti per l'utilizzo di servizi ICT a supporto di funzioni essenziali o importanti

Ai sensi del Regolamento DORA (articolo 28), le entità finanziarie informano tempestivamente l'autorità competente in merito a eventuali accordi contrattuali previsti (*planned*) per l'utilizzo di servizi ICT a supporto di funzioni essenziali o importanti (FEI)[6], nonché del momento in cui una funzione diventa essenziale o importante. Il Regolamento non specifica le tempistiche di questa informativa preventiva, né prevede un potere di autorizzazione/nulla osta da parte dell'autorità competente. L'informativa è funzionale allo svolgimento da parte dell'autorità competente dell'attività di vigilanza *on-going* sull'entità finanziaria che si avvale del servizio ICT prestato dal fornitore terzo.

L'esternalizzazione di funzioni in ambito ICT è stata finora disciplinata dalle normative settoriali sull'esternalizzazione applicabili agli intermediari soggetti al Regolamento DORA. Con l'avvio dell'applicazione del Regolamento, all'utilizzo da parte degli intermediari di servizi ICT prestati da fornitori terzi non troveranno più applicazione le discipline settoriali in materia di esternalizzazione. Si pone pertanto l'esigenza di fornire indicazioni in merito ai procedimenti amministrativi previsti da tali discipline settoriali.

A partire dal 17 gennaio 2025, non devono ritenersi più applicabili i seguenti procedimenti amministrativi di divieto dell'esternalizzazione previsti dalla normativa secondaria della Banca d'Italia, ove aventi ad oggetto l'esternalizzazione di servizi ICT a supporto di FEI:

- divieto di esternalizzare funzioni aziendali operative essenziali o importanti (Regolamento della Banca d'Italia di attuazione degli articoli 4-*undecies* e 6, comma 1, lett. b) e c-*bis*), del TUF: articolo 50, comma 3);
- divieto di esternalizzazione di funzioni aziendali operative essenziali o importanti a fornitori di servizi *cloud* (Regolamento della Banca d'Italia di attuazione degli articoli 4-*undecies* e 6, comma 1, lett. b) e c-*bis*), del TUF: articolo 18, comma 4);
- divieto di esternalizzare, in tutto o in parte, funzioni operative importanti e di controllo a un soggetto esterno o nell'ambito del gruppo di appartenenza per IP e IMEL (Disposizioni di vigilanza per gli istituti di pagamento e gli istituti di moneta elettronica: Capitolo VI, Sezione II).

[6] Ai sensi del Regolamento DORA (art. 3, punto 22), per "funzione essenziale o importante" si intende 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".

Pertanto, a partire dal 17 gennaio 2025, prima di dare corso a eventuali accordi contrattuali previsti per l'utilizzo di servizi ICT a supporto di FEI, gli intermediari informano tempestivamente la Banca d'Italia.

Restano in ogni caso fermi i poteri di intervento della Banca d'Italia anche con riguardo alle politiche e agli accordi con i fornitori terzi di servizi ICT, qualora questi dovessero risultare pregiudizievoli per la sana e prudente gestione degli intermediari.

I procedimenti amministrativi di divieto di esternalizzazione di FEI previsti nelle richiamate disposizioni di vigilanza della Banca d'Italia continuano a trovare applicazione in caso di esternalizzazione di servizi non-ICT.

2.3. Segnalazione dei gravi incidenti ICT e delle minacce informatiche significative

In applicazione del Regolamento DORA (articolo 19), gli intermediari segnalano i gravi incidenti ICT[7] e, su base volontaria, le minacce informatiche significative alla Banca d'Italia. A partire dal 17 gennaio 2025 la disciplina vigente in materia sarà abrogata e sostituita dallo schema di notifica disciplinato dal nuovo Regolamento e dagli atti delegati (RTS e ITS) previsti dallo stesso. Al riguardo, gli intermediari:

- classificano gli incidenti ICT e le minacce informatiche secondo quanto previsto dal regolamento delegato (UE) 2024/1772[8];
- segnalano alla Banca d'Italia, utilizzando la piattaforma Infostat[9], gli incidenti ICT attraverso la rilevazione denominata "DORA – Segnalazione gravi incidenti ICT (DORAI)" e, su base volontaria, le minacce informatiche significative attraverso la rilevazione denominata "DORA – Segnalazione minacce informatiche significative (DORAM)", tenendo conto dell'atto adottato dalla Commissione europea il 23 ottobre 2024[10] che specifica il contenuto e le tempistiche per la segnalazione;
- utilizzano, ai fini della segnalazione di cui al punto precedente, il modulo in formato ".xlsx" disponibile sul sito Internet della Banca d'Italia[11], compilandolo secondo le modalità previste dall'atto adottato dalla Commissione europea il 23 ottobre 2024 che stabilisce i formati, i modelli e le procedure standard per la segnalazione dei gravi incidenti ICT e delle

[7] Tali obblighi sono estesi anche agli incidenti operativi o di sicurezza dei pagamenti riguardanti enti creditizi, istituti di pagamento e istituti di moneta elettronica. Nel seguito del documento con "incidenti ICT" si intendono anche tali fattispecie.

[8] Cfr. https://eur-lex.europa.eu/eli/reg_del/2024/1772/oj.

[9] Per maggiori dettagli sulla piattaforma Infostat si rimanda alla sezione dedicata nel sito Internet istituzionale https://www.bancaditalia.it/statistiche/raccolta-dati/informazioni-generali/raccolta-internet/index.html

[10] Regolamento delegato sulle norme tecniche di regolamentazione che specificano il contenuto e i termini della notifica iniziale, della relazione intermedia e della relazione finale per gli incidenti gravi connessi alle TIC nonché il contenuto della notifica volontaria per le minacce informatiche significative (https://webgate.ec.europa.eu/regdel/#/delegatedActs/2503).

[11] Cfr. https://www.bancaditalia.it/compiti/vigilanza/dora-incidenti/index.html (raggiungibile anche attraverso l'attuale pagina dedicata agli incidenti https://www.bancaditalia.it/compiti/vigilanza/incidenti-operativi/index.html).

minacce informatiche significative[12] e tenendo conto delle istruzioni operative pubblicate nella medesima pagina del sito[13].

2.4. Test avanzati di penetrazione basati sulle minacce (Threat-Led Penetration Test)

In applicazione del Regolamento DORA (Articolo 26), gli intermediari identificati secondo i criteri definiti dall'apposito atto delegato in corso di adozione, sono tenuti ad effettuare test avanzati di penetrazione basati su minacce (*Threat-Led Penetration Test - TLPT*) con cadenza almeno triennale[14].

Alla luce delle previsioni del Regolamento, tali test rientrano tra gli strumenti utilizzati dalla Vigilanza, i cui esiti saranno incorporati nei processi di supervisione.

Per quanto riguarda gli intermediari vigilati direttamente dalla Banca d'Italia, il processo di identificazione di cui sopra è ancora in corso e una volta concluso si procederà ad informare i soggetti interessati nonché a definire, successivamente, una pianificazione per l'esecuzione dei test.

* * *

Si fa infine presente che le Disposizioni di vigilanza della Banca d'Italia potranno essere modificate al fine di assicurare il riordino della complessiva disciplina di vigilanza alla luce delle previsioni del Regolamento DORA, in un'ottica di chiarezza del complessivo quadro normativo.

[12] Regolamento di esecuzione riguardante 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. https://ec.europa.eu/transparency/documents-register/detail?ref=C(2024)7277&lang=en

[13] Le istruzioni operative saranno aggiornate una volta finalizzato l'iter regolamentare europeo.

[14] Tale frequenza può essere ridotta o aumentata dalla Banca d'Italia sulla base del profilo di rischio dell'intermediario e tenuto conto delle circostanze operative.