



- *Dora's Journey 17 Gennaio 2025*

- *Atto del Governo n. 242 Gennaio 2025*

- *DORA & NIS 2*

- *Quadro Normativo*

- *DORA - governance contrattuale e societaria / sicurezza e gestione di rischi ICT*

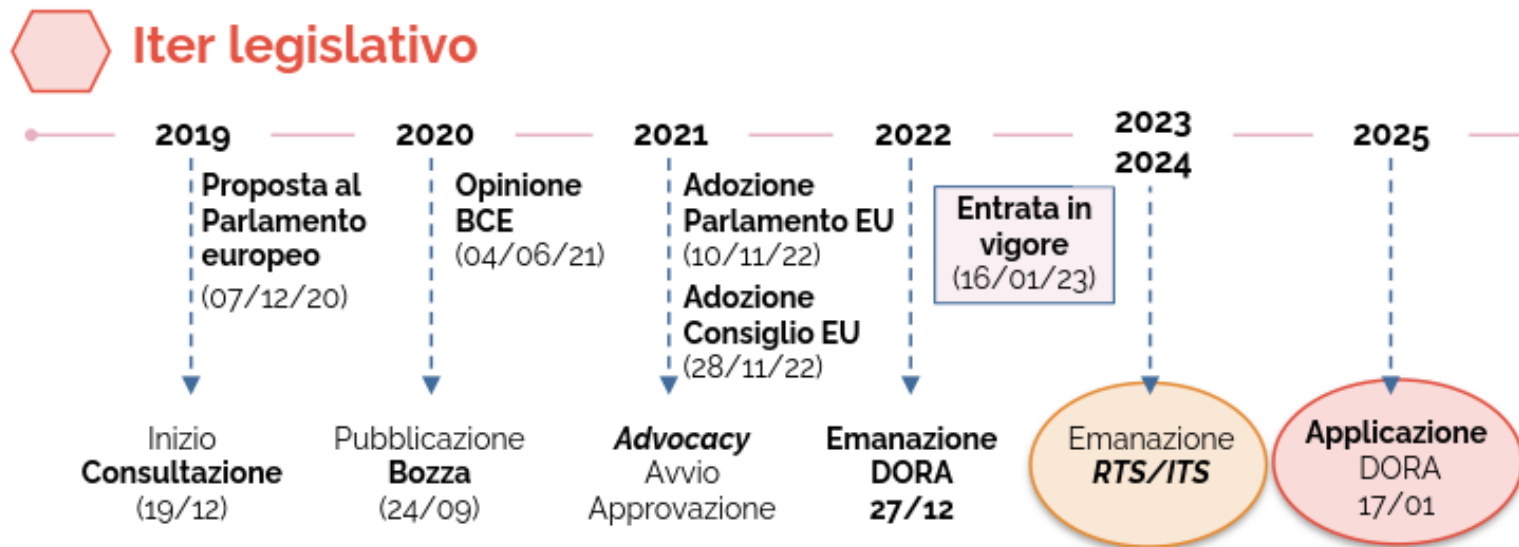
- *DORA'S GOALS and BUILDING BLOCKS*

- *DORA - norme tecniche: RTS e ITS*

- *DORA - una compliance integrata*

- *DORA - approccio di Generalfinance*

- *Ciclo di incontri di approfondimento 2025*



- **Approvazione Formale:** Novembre 2022
- **Entrata in Vigore:** La normativa è entrata formalmente in vigore il 16 gennaio 2023, venti giorni dopo la pubblicazione nella Gazzetta Ufficiale dell'Unione Europea
- **Applicazione:** Le disposizioni di DORA saranno applicabili a partire da 24 mesi dopo la data di entrata in vigore, quindi **dal 17 gennaio 2025**



dossier

XIX Legislatura

Gennaio 2025

Schema di decreto legislativo recante disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2022/2554, 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, e per il recepimento della direttiva (UE) 2022/2556, che modifica le direttive 2009/65/CE, 2009/138/CE, 2011/61/CE, 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

Atto del Governo n. 242

CAPO VI DISPOSIZIONI FINALI

Articoli 16 e 17

(Clausola di invarianza finanziaria (Art.16); Entrata in vigore (Art. 17))

L'articolo 16 reca la clausola di invarianza finanziaria, disponendo che dal decreto in esame non devono derivare nuovi o maggiori oneri a carico della finanza pubblica e che le amministrazioni competenti e le istituzioni pubbliche coinvolte provvedono all'attuazione delle disposizioni di cui al decreto con le risorse umane, strumentali e finanziarie previste a legislazione vigente.

L'articolo 17 disciplina l'entrata in vigore, disponendo un'applicazione differita al 1° gennaio 2027 per quanto riguarda la disciplina relativa alla resilienza operativa digitale applicabile agli intermediari finanziari (contenuta nell'articolo 6, commi 1 e 2, del decreto).

CAPO III DISPOSIZIONI APPLICABILI A INTERMEDIARI FINANZIARI E BANCOPOSTA

Articoli 6 e 7 *(Disposizioni applicabili agli intermediari finanziari (Art. 6); Disposizioni applicabili a Bancoposta (Art. 7))*

L'articolo 6 individua le disposizioni del regolamento (UE) 2022/2554 applicabili agli intermediari finanziari iscritti all'albo di cui all'articolo 106 del TUB.

L'articolo 7 individua le disposizioni dello stesso regolamento applicabili a Bancoposta. In ossequio al principio di proporzionalità richiamato nei criteri di delega, si rende applicabile la medesima disciplina applicata per le banche.

La RT rileva che gli articoli 6 e 7 chiariscono quali disposizioni del regolamento DORA si applichino, a seconda della complessità del soggetto e del livello di rischio ICT dell'attività svolta, a intermediari finanziari e Bancoposta.

In linea con il principio di proporzionalità richiamato nei criteri di delega, l'articolo 6, comma 3, rimette alla potestà regolamentare della Banca d'Italia l'eventuale individuazione di una categoria di intermediari finanziari da considerarsi «significativi» (anche per tipologia di attività svolte), a cui applicare l'ICT *risk management framework* completo, in luogo di quello semplificato.

La Banca d'Italia ha, ai sensi degli articoli 131 e 282 del TFUE, un bilancio autonomo e gode della più ampia indipendenza finanziaria. Pertanto, la Banca d'Italia provvede all'attuazione dei compiti di vigilanza disciplinati dal Capo III con le risorse umane, strumentali e finanziarie disponibili a legislazione vigente e, comunque, senza nuovi o maggiori oneri a carico della finanza pubblica.

NIS 2 (Network and Information Security) è una direttiva dell'UE che impone agli Stati membri di proteggere infrastrutture critiche (come energia, sanità e trasporti) da cyberattacchi, stabilendo standard minimi di sicurezza e obblighi di notifica degli incidenti per migliorare la resilienza informatica in tutta l'Unione Europea.

Esclusione dalla Direttiva NIS2 per le Entità Soggette al Regolamento DORA

Le entità finanziarie regolamentate dal DORA sono esentate dalla Direttiva NIS2 per evitare duplicazioni normative (Art. 32), poiché DORA già soddisfa pienamente i requisiti di resilienza operativa digitale necessari, permettendo loro di concentrarsi specificamente sulle misure di sicurezza previste da DORA.



Gli operatori economici soggetti al Regolamento DORA (Regolamento (UE) 2022/2554) dovranno implementare, entro il 17 gennaio 2025, gli obblighi previsti dalla normativa europea in merito alla gestione dei rischi informatici, tenendo altresì in considerazione, in tale processo di adeguamento, **gli standard tecnici definiti nel frattempo dalle Autorità Europee di Vigilanza, ossia le ITS (Implementing Technical Standard) e le RTS (Regulatory Technical Standard)**, che chiariscono e specificano alcuni obblighi di cui al Regolamento DORA.

Il **17 gennaio 2024** le Autorità di Vigilanza Europee hanno pubblicato le bozze finali del primo set di ITS e RTS, recentemente pubblicate in GU dopo il vaglio della Commissione Europea. Il secondo set di norme tecniche sarà finalizzato e presentato alla Commissione Europea **entro il 17 luglio 2024**.

Dal 17 gennaio 2025 le entità finanziarie dovranno prevedere e riesaminare periodicamente una **strategia per la gestione dei rischi informatici derivanti da tutti i fornitori di servizi ICT**. Il Regolamento, infatti, amplia considerevolmente il perimetro dei soggetti rispetto ai quali le entità finanziarie debbono disciplinare adeguatamente i propri rapporti: non più solo i fornitori di servizi informatici a cui le entità finanziarie abbiano esternalizzato funzioni essenziali o importanti, bensì tutti i fornitori di servizi ICT.

Nonostante lo sforzo di armonizzare la disciplina, **permane la necessità di raccordare gli obblighi previsti** da un quadro normativo complesso:

Linee guida EBA
Outsourcing

40.mo aggiornamento
della Circolare 285/2013

Orientamenti ESMA sui
servizi cloud

DORA

Orientamenti EBA
in materia di
esternalizzazione

285/2013 – 40° agg.
Elementi di novità

DORA
Capo V - Gestione dei
rischi ICT derivanti da
terzi

⇒ EBA copre i **servizi in outsourcing**, inclusi i servizi **Cloud**.

Banca d'Italia ha introdotto:

- L'applicazione degli orientamenti EBA (Sez. 1.2.3) sulla gestione dei rischi ICT e di sicurezza ai servizi ICT diversi dall'esternalizzazione forniti dai soggetti terzi (EBA/GL/2019/04).

⇒ DORA copre tutti gli accordi di servizi ICT con le terze parti. E' introdotto il ruolo del fornitore ICT critico il quale sarà nominato dall'AEV.

Alcuni principi comuni alle normative:

- Principio di proporzionalità
- Registro delle informazioni per accordi contrattuali con fornitori di servizi ICT
- **Valutazione preliminare del rischio dell'accordo e due diligence sul fornitore**
- Conflitti di interesse
- Diritti di accesso e di recesso
- **Exit Strategy**

Conclusione: il modello di governance ai sensi del Reg. Dora deve evolvere e non deve ripartire da zero!

Osservati:

- il massiccio ricorso all'utilizzo delle tecnologie dell'informazione e della comunicazione (Servizi TIC) nell'ambito del settore finanziario, anche (e soprattutto) prestate da fornitori terzi (esternalizzazioni) (tale opzione ha determinato un maggiore livello di **efficienza dei processi e dei presidi** anche in termini di **costi** da sostenere, migliorando altresì la specializzazione e la **qualità** dei servizi resi al mercato di riferimento)
- le travolgenti trasformazioni digitali che coinvolgono l'operatività di tutti i players che operano nel mercato finanziario;

elementi che, amplificano notevolmente l'esposizione al rischio derivante da potenziali incidenti informatici (c.d. "Rischi ICT"), potenzialmente suscettibile di coinvolgere l'intero il sistema finanziario, minandone la stabilità.

Il Regolamento DORA, attraverso il rafforzamento e l'armonizzazione della normativa applicabile, mira ad accrescere la consapevolezza circa i Rischi ICT sulla solidità degli intermediari finanziari, anche mediante l'implementazione di mirate **MISURE** di:

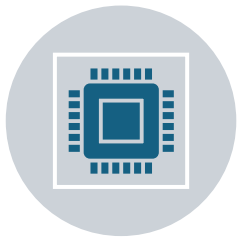
**governance contrattuale e
societaria**

**sicurezza e gestione di rischi
ICT e segnalazioni di incidenti**

L'obiettivo della norma, pertanto, è raggiungere un adeguato **livello di mitigazione dei Rischi ICT**, assicurando l'integrità degli intermediari finanziari nelle ipotesi di eventuali attacchi informatici e/o altri disallineamenti operativi derivanti dall'operatività delle terze parti in materia cyber.



creazione di un quadro regolamentare orientato a garantire la **stabilità** del mercato di riferimento, attraverso il rafforzamento dei **presidi di vigilanza** connessi al coinvolgimento delle **terze parti** nei processi di business degli intermediari vigilati.
Tale rafforzamento sembra attuarsi mediante la definizione di un perimetro normativo volto a identificare i "nuovi" rischi emergenti, legati al coinvolgimento delle terze parti nonché alle ulteriori innovazioni che impattano sulle attività degli intermediari vigilati.



INTRODUCE E DEFINISCE IL
CONCETTO DI STRATEGIA DI
RESILIENZA OPERATIVA DIGITALE



OTTENERE UN ELEVATO
LIVELLO DI
CYBERSICUREZZA FRA GLI
STATI MEMBRI



RAPPRESENTA UN QUADRO NORMATIVO
ARMONIZZATO PER LA SICUREZZA
INFORMATICA DEI PRODOTTI



SI PONE L'OBIETTIVO DI ARMONIZZARE E
UNIFORMARE A LIVELLO DI UNIONE
EUROPEA GLI ELEMENTI ESSENZIALI DEI
CONTRATTI CHE DISCIPLINANO LA
PRESTAZIONE DI SERVIZI ICT E I
RAPPORTI CON I FORNITORI TERZI.

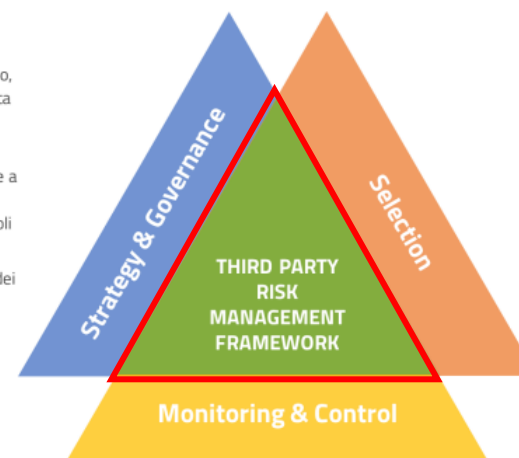
Le norme tecniche DORA sono dunque finalizzate a migliorare la resilienza operativa digitale del settore finanziario dell'UE, rafforzando le tecnologie dell'informazione e della comunicazione (ITC) e i quadri di gestione del rischio di terzi e di segnalazione degli incidenti delle entità finanziarie.

L'obiettivo è garantire che le entità finanziarie mantengano il controllo dei propri rischi operativi, della sicurezza delle informazioni e della continuità operativa durante l'intero ciclo di vita degli accordi contrattuali con tali fornitori terzi di servizi ICT.

- norme tecniche di regolamentazione (RTS) sul quadro di gestione del rischio ICT e sul quadro semplificato di gestione del rischio ICT;
- RTS sui criteri per la classificazione degli incidenti legati alle ICT, che specificano:
 - I **criteri** e l'approccio per la classificazione degli **incidenti gravi legati alle ICT**;
 - Le **soglie di rilevanza** di ciascun **criterio di classificazione**;
 - I criteri e le soglie di rilevanza per determinare le **minacce informatiche significative**;
 - I criteri per la valutazione da parte delle autorità competenti della **rilevanza degli incidenti e i dettagli degli incidenti da condividere**.
- RTS relativi alla politica sui servizi ICT che supportino funzioni critiche o importanti forniti da fornitori di servizi ICT di terze parti (TPP), contenenti **disposizioni di governance**, della **gestione del rischio** e del **quadro di controllo interno che le entità finanziarie dovrebbero adottare in merito all'utilizzo di fornitori terzi di servizi ICT**.
- norme tecniche di attuazione (ITS) per stabilire i **modelli per il registro delle informazioni sugli accordi contrattuali con i fornitori di servizi ICT terzi**: il registro sarà utilizzato dalle autorità competenti e dalle autorità di vigilanza europee per supervisionare la conformità delle entità finanziarie al DORA e per designare i fornitori critici di servizi TIC di terzi soggetti al regime di sorveglianza del DORA.

La gestione della catena della fornitura richiede secondo la DORA attività di compliance integrata tra aspetti tecnologici, di sicurezza e legali

- Definizione di un modello organizzativo, metodologico e operativo che permetta di attuare e la strategia di governo dei rischi associati alle terze parti definita
- Predisposizione di un set documentale a supporto del modello (es. guidelines metodologiche, policy e procedure, ruoli e responsabilità, etc.)
- Individuazione dei criteri di selezione dei fornitori, in coerenza con le linee di indirizzo strategiche definite



- Disegno e formalizzazione di un processo di selezione dei fornitori coerente con il modello organizzativo, metodologico e operativo di Third Party Risk Management
- Progettazione e implementazione di un set di strumenti a supporto del processo di valutazione del fornitore e della specifica fornitura (es. tassonomia delle forniture, checklist di assessment, strumenti automatizzati per la gestione delle interlocazioni con i fornitori)

- Programmi di audit e assessment allineati al profilo di rischio associato alla specifica fornitura
- Template contrattuali allineati agli obiettivi della strategia di Third Party Risk Management

DEFINIRE UNA GOVERNANCE DELLE FORNITURE E ADOTTARE UN APPROCCIO RISK BASED		GARANTIRE ALLINEAMENTO NORMATIVO E PRESIDIO CONTRATTUALE	
Definire processi chiari che coinvolgano tutti gli interlocutori necessari	Adottare un approccio di gestione del rischio completo , che analizzi tutti gli aspetti operativi, strategici, di conformità e reputazionali	Adottare un presidio costante rispetto alle novità che la normativa comporta	Presidiare in modo corretto i rischi di fornitura gestendo ogni fase della relazione . Ogni fase è strettamente interconnessa alle altre
Assicurarsi di coinvolgere tutti gli interlocutori necessari	Definire un approccio alla gestione degli incidenti sui fornitori con particolare attenzione nelle fasi pre-contrattuali	Attivare piani ed azioni per coprire gli indirizzi di rafforzamento ampliamento del perimetro di applicazione della normativa	Pianificare e attuare tutte le azioni necessarie a definire strumenti di tutela in corso di esecuzione del contratto (es: exit strategy)

3 Cantieri progettuali

Assessment Contrattuale (Compliance, Direzione ICT)

- Mappatura dei fornitori di servizi ICT
- Revisione dei Modelli Contrattuali e analisi e revisione dei contratti in corso di validità
- Invio delle comunicazioni ai fornitori ICT con le schede di contract assessment
- Stipulazione dei nuovi contratti con i fornitori ICT, secondo le previsioni DORA

Aggiornamento Procedure e Policy (Compliance, Organizzazione)

- Aggiornamento Regolamento di gestione dei costi operativi, per normare la funzione delle gare di appalto
- Nuova policy Gestione e Valutazione dei fornitori ICT e/o revisione della Policy Esternalizzazioni per normare il procurement ICT (con particolare riferimento alla fase precontrattuale)
- Set procedurale norme tecniche DORA (con il supporto di un fornitore in fase di scouting)

Alimentazione Registro trattamenti (Compliance, RISK, Sviluppo ICT, Sistemi,)

- Sviluppo sviluppo registro trattamenti, metriche e kpi
- Generazione Report Risk Assessment

Il progetto DORA in numeri...

6 persone GF coinvolte nell'analisi e nell'attuazione del Regolamento DORA

1 Dottorato attivato in partnership con l'Università di Verona

Oltre 70 Contratti di servizi ICT attivi analizzati, riferiti a circa 50 fornitori ICT

21 articoli di Linee Guida scritti per la revisione contrattuale

Data	Argomenti	Relatori
Giovedì 30 gennaio 2025 ore 11.00-12.30	Caso aziendale e valutazione dei contratti di servizi TIC (FEI e Critici)	<i>Relazione introduttiva a cura di:</i> CA Commercial Finance + dibattito
Giovedì 27 marzo 2025 ore 11.00-12.30	Panoramica della normativa DORA: obiettivi, ambito di applicazione e impatti sul settore finanziario	<i>Relazione introduttiva a cura di:</i> Studio Legale La Scala <i>Commento a cura di:</i> Unicredit Factoring + dibattito
Giovedì 29 maggio 2025 ore 11.00-12.30	Gestione dei rischi ICT: identificazione e valutazione dei rischi ICT, misure di mitigazione e controllo, best practices per la gestione dei rischi	<i>Relazione introduttiva a cura di:</i> Università di Verona - Facoltà di Giurisprudenza <i>Commento a cura di:</i> Generalfinance + dibattito
Giovedì 25 settembre 2025 ore 11.00-12.30	Incidenti informatici e resilienza operativa: classificazione e segnalazione degli incidenti informatici, piani di risposta e recupero, test di resilienza operativa digitale	TBD
Giovedì 27 novembre 2025 ore 11.00-12.30	Gestione dei rischi da terze parti: rischi derivanti da fornitori terzi di servizi TIC, contratti e accordi con fornitori, monitoraggio e valutazione continua dei fornitori	TBD