



ABISERVIZI
ABI
FORMAZIONE

DORA È ORA: RESILIENZA OPERATIVA DIGITALE IN AZIONE

*Cosa cambia nel 2025 per il settore finanziario:
dall'autovalutazione richiesta dalla Banca d'Italia alla messa
a terra delle azioni necessarie al conseguimento della piena conformità*

Ciclo di approfondimenti formativi e confronto

dal 12 febbraio 2025



IL CONTESTO NORMATIVO

Il 2025 inizia con la piena applicabilità, dal 17 gennaio, del Regolamento Dora – Digital Operational Resilience Act, che rappresenta una disciplina normativa complessa e articolata e impegna il settore bancario e finanziario in un processo di adeguamento che procede con ritmo incalzante.

Tra i provvedimenti di recente pubblicazione, oltre la dichiarazione delle ESAs del 4 dicembre sul Registro degli accordi contrattuali con i fornitori ICT, **Banca d'Italia ha richiamato l'attenzione degli operatori al rispetto degli obblighi in materia di sicurezza ICT conseguenti all'applicazione del Regolamento DORA**, emanando comunicazioni il 23 e il 30 dicembre 2024.

In tali comunicazioni **ha richiesto agli operatori vigilati di eseguire un'autovalutazione dell'ICT Risk management framework, ed una valutazione di conformità dei propri processi interni ai requisiti DORA, fornendone evidenza entro il 30 aprile 2025, ha esteso i presidi di sicurezza anche al tema degli accessi e ha chiarito alcuni aspetti importanti.**

L'autovalutazione dovrà essere effettuata con il supporto delle Funzioni di Controllo con particolare attenzione a:

- i presidi e le policy interne di adeguamento al Dora;
- strategie dell'intermediario sui rischi di terza parte,
- attività e programma dei test di resilienza operativa digitale;
- sistema di gestione dei rischi ICT;
- modalità per prevenire, o rilevare tempestivamente, violazioni alla riservatezza dei dati e/o dei servizi;
- valutazione circa la conformità al Dora del quadro di ICT change management dell'intermediario.

Inoltre, con atto del governo sottoposto a parere parlamentare n. 242 del 7 gennaio 2025 è stato reso noto uno "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" in applicazione degli articoli 1 e 16 della legge 21 febbraio 2024, n. 15.

Il decreto avrà l'obiettivo di dettare disposizioni necessarie all'adeguamento del quadro normativo nazionale al Regolamento Dora e nonché a garantire il coordinamento con le vigenti disposizioni di settore.

Dallo schema emergono tre ambiti di rilievo:

- il ruolo delle autorità di vigilanza (Banca d'Italia, IVASS, COVIP, CONOSB) per il rispetto degli obblighi posti dal Regolamento a carico dei soggetti vigilati dalle medesime autorità, secondo le rispettive attribuzioni di vigilanza;
- applicazione del Regolamento agli intermediari finanziari e a Bancoposta;
- impianto sanzionatorio che prevede impatti significativi (fino al 10% del fatturato) e applicabili anche a coloro che svolgono ruoli di amministrazione, direzione e controllo.



LA NUOVA OFFERTA FORMATIVA

Per accompagnare operativamente le aziende nei primi mesi di messa in opera delle azioni di adeguamento, ABIFormazione ha progettato una nuova formula di approfondimento e confronto formativo, articolata in due cicli:

Il primo ciclo si declina in tre giornate formative “La gestione operativa delle prime scadenze nel processo di adeguamento al Regolamento DORA”. In modo particolare le giornate analizzeranno il complessivo quadro regolamentare e faranno il punto sull'autovalutazione del ICT Risk management framework, sulle Comunicazioni Banca d'Italia e sulle ultime novità regolamentari per accompagnare le banche nella gestione operativa delle prime scadenze del processo di adeguamento.

IL CALENDARIO

Giornate formative	DORA è ora: la gestione operativa delle scadenze nel processo di adeguamento 12 febbraio, Aula virtuale
	18 e 19 febbraio, Aula virtuale
	— Autovalutazione del rischio ICT: modalità operative di esecuzione - 18 febbraio — L'implementazione del registro delle informazioni degli accordi contrattuali per l'utilizzo di servizi ICT prestati da fornitori terzi - 19 febbraio

Infine, da marzo, il ciclo di incontri “DORA è ora: resilienza operativa digitale in azione”, sarà focalizzato sulla messa a terra delle azioni necessarie al conseguimento della piena conformità al DORA.

Ciclo di incontri di approfondimento e confronto	“DORA è ora: resilienza operativa digitale in azione” - dal 4 marzo Aula virtuale
	— Il framework di gestione dei rischi ICT: i nodi critici - 4 marzo
	— Governance e assetti organizzativi: vantaggi e svantaggi delle possibili soluzioni - 18 marzo
	— Strategia di resilienza operativa digitale: le componenti - 27 marzo
	— La catena di fornitura dei servizi ICT a supporto di funzioni essenziali o importanti: il modello operativo - 8 aprile
	— La classificazione degli incidenti e delle minacce informatiche significative - 15 aprile
	— La stima dei costi annuali aggregati e delle perdite causate da incidenti TIC rilevanti - 6 maggio
	— Il piano di comunicazione e i flussi informativi - 20 maggio
	— I test di penetrazione basati sulle minacce - 29 maggio
	— Lo «human firewall» come prima linea di difesa contro il cyber crime - 10 giugno
	— Strumenti di gestione dei rischi cyber e applicazione della cyber threat intelligence - 24 giugno



PROGRAMMA

Giornata formativa

DORA è ora: la gestione operativa delle scadenze nel processo di adeguamento

12 febbraio, Aula virtuale (10.00/16.00)

10.00 ► **Apertura dei lavori e introduzione**

Barbara Filippella, Responsabile Settore Sviluppo Competenze **ABIFormazione**

OPEN SESSION

10.10 ► **Le aspettative delle Autorità sul piano di adeguamento: priorità e punti di attenzione**

- La comunicazione Banca d'Italia del 23 dicembre: gap analysis dei requisiti DORA e l'autovalutazione dell'ICT risk management framework
- La nota Banca d'Italia sulle modalità operative per la segnalazione di gravi incidenti ICT e delle minacce informatiche significative
- La Comunicazione Banca d'Italia del 30 dicembre sull'applicazione del DORA al settore finanziario: le specifiche per le diverse entità finanziarie e le linee di indirizzo

Valentina Cappa, Servizio Rapporti Istituzionali di Vigilanza **Banca d'Italia**

10.50 **Questions & Answers**

11.30 **Break**

SESSIONE 1

11.40 ► **Aggiornamento del quadro regolamentare: il punto su ITS, RTS e Regolamenti**

Maria Cristina Daga, Partner **Partner4Innovation**

12.00 ► **Dalla regolamentazione agli impatti operativi: le applicazioni**

- Le peculiarità di una vista per settori: le ricadute per le diverse entità finanziarie
- Il processo di autovalutazione dell'ICT risk management framework: i driver da prendere in considerazione
- Gli impatti dell'abrogazione delle normative
- Schema di decreto legislativo recante disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2022/2554
- Focus sull'impianto sanzionatorio: le diverse applicazioni in base ai diversi destinatari e ruoli organizzativi

Paolo Carcano, Partner **PwC**

Samantha Trama, Director **PwC**

12.45 ► **Le ricadute per il settore bancario**

Romano Stasi, Segretario Generale **ABI Lab**

13.15 **Pausa pranzo**

14.15 ► **Gap analysis e piani di adeguamento: focus sulla trasformazione ICT**

Massimo Messina, senior advisor

SESSIONE 2

14.45 ► **Focus sul Regolamento di esecuzione 2024/2956 relativo al registro delle informazioni**

- La dichiarazione congiunta ESAs del 4 dicembre
- Le evidenze emerse dal "dry run exercise" delle ESAs sul registro delle informazioni
- Modalità di comunicazione, trasmissione informazioni, template, tempistiche

Maria Cristina Daga, Partner **Partner4Innovation**

15.40 ► **I punti aperti alle soglie dell'applicazione del DORA**

Francesco Grossi, Responsabile Organizzazione e Project Management **Banca Mediolanum Spa**

16.00 **Chiusura dei lavori**



Giornate formative

18 e 19 febbraio, Aula virtuale

Prima delle due giornate, tutti i partecipanti riceveranno una minisurvey a cui rispondere, in forma anonima, per orientare il programma sugli ambiti di maggiore criticità operativa. Gli esiti della minisurvey saranno analizzati e commentati nel corso dell'incontro.

Autovalutazione del rischio ICT: modalità operative di esecuzione

18 febbraio (10.00/13.30)

► Le comunicazioni di Banca d'Italia: i punti di attenzione dell'Autorità di vigilanza

- Gli ambiti che rilevano carenze dalle segnalazioni di gravi incidenti operativi o di sicurezza: modalità operative per una gestione efficace
- Le criticità evidenziate da Banca d'Italia nel contesto della sicurezza ICT
- Le carenze nella capacità di gestire e aggregare i dati sui rischi
- Le inadeguatezze dei sistemi ICT utilizzati per supportare i processi decisionali e le attività di gestione dei rischi
- Le richieste di Banca d'Italia agli operatori:

Paolo Carcano, Partner **PwC**

Samantha Trama, Director **PwC**

► L'autovalutazione da effettuare e comunicare all'Autorità entro il 30 aprile 2025

- La valutazione del rischio ICT di terze parti
- Le indicazioni sulla segnalazione preventiva degli accordi contrattuali
- La valutazione dell'adattamento di presidi e politiche interne
- La valutazione delle attività e programma di test di resilienza operativa digitale
- L'autovalutazione dell'adeguatezza dei sistemi di gestione dei rischi ICT
- Le misure per il controllo degli accessi, compresi quelli del personale interno
- La conformità dell'ICT change management al Regolamento DORA
- Gli ulteriori profili di attenzione per l'applicazione del Regolamento DORA individuati da Banca d'Italia

Romina Vignotto, Partner **PwC**

Francesco Brunetti, Director **PwC**

► Gap analysis di scostamento dal DORA

- La complessità di mettere in evidenza gli ambiti di miglioramento



Confronto guidato: gli esiti della minisurvey e casi pratici

Samantha Trama, Director **PwC**

Testimonianze bancarie

► L'autovalutazione del rischio ICT: gli ambiti di indagine

- Strategie sul rischio di terza parte, sul rinnovo dei contratti di fornitura e sulla trasmissione all'Autorità del Registro delle Informazioni;
- Adattamento di presidi e politiche interne;
- Attività e programma di test di resilienza operativa digitale



Confronto guidato: gli esiti della minisurvey e casi pratici

Romina Vignotto, Partner **PwC**

Francesco Brunetti, Director **PwC**

Testimonianze bancarie

► Focus-on: La gestione efficace degli accessi:

- Rafforzamento del legame tra ambito DORA e controllo degli accessi: un punto nevralgico per il settore bancario e finanziario
- La relazione con i presidi GDPR
- La gestione degli accessi e la salvaguardia dell'integrità dei dati



Confronto guidato: gli esiti della minisurvey e casi pratici

Paolo Carcano, Partner **PwC**

Testimonianze bancarie



L'implementazione del registro delle informazioni degli accordi contrattuali per l'utilizzo di servizi ICT prestati da fornitori terzi

19 febbraio (10.00/13.30)

► Il quadro regolamentare relativo al registro delle informazioni degli accordi contrattuali per l'utilizzo di servizi ICT prestati da fornitori terzi

- La dichiarazione congiunta ESAs del 4 dicembre
- Il regolamento di esecuzione 2024/2956 relativo al registro delle informazioni
- Le sovrapposizioni tra le diverse normative in vigore

Gabriele Faggioli CEO **Partner4Innovation**

Maria Cristina Daga, Partner **Partner4Innovation**

► Il registro delle informazioni come strumento gestionale: le finalità e logiche

- La definizione di terze parti, fornitori ed esternalizzazioni ICT: quali aspetti rendono la classificazione ancora problematica
- Le scadenze, i template e le modalità operative di compilazione e di trasmissione



Confronto guidato: gli esiti della minisurvey e casi pratici

Maria Cristina Daga, Partner **Partner4Innovation**

Testimonianza bancaria

► L'implementazione del registro delle informazioni

- Lo stato dell'arte nel settore bancario e finanziario
- Migliori prassi e lezioni apprese
- Simulazione di casistiche



Confronto guidato: gli esiti della minisurvey e casi pratici

Maria Cristina Daga, Partner **Partner4Innovation**

Testimonianza bancaria