Tous établissements · En vigueur

DORA, résilience opérationnelle numérique

Le règlement DORA s'applique depuis le 17 janvier 2025. Il encadre la gestion du risque informatique, la déclaration des incidents, les tests de résilience et le recours aux prestataires. La BCE en fait un axe de ses contrôles pour 2027-2029.

DATE D'APPLICATION	QUI LE DEMANDE	À QUI VOUS RÉPONDEZ	NATURE DE LA DEMANDE
17 janv. 2025	Législateur européen (règlement DORA)	BCE, ACPR, AMF	Supervision prudentielle

ÉTABLISSEMENTS CONCERNÉS

- Grand groupe bancaire
- Banque de taille moyenne
- Financements spécialisés
- Banque privée
- Société de gestion
- Assureur
- Mutuelle et prévoyance
- Institution financière publique

Fond plein : concerné. Pointillé : selon le statut ou l'activité.

REPÈRES

Le calendrier du texte.

27 déc. 2022 — Publication du règlement (UE) 2022/2554

16 janv. 2023 — Entrée en vigueur

17 janv. 2025 — Application

19 nov. 2026 — Priorités de supervision 2027-2029 de la BCE

LE DÉTAIL

Ce qui change.

Quatre volets

EN APPLICATION DEPUIS LE 17 JANVIER 2025

RISQUE INFORMATIQUE
- Cadre de gestion du risque lié aux technologies

INCIDENTS
- Déclaration des incidents au superviseur

TESTS
- Tests de résilience
- Tests d'intrusion fondés sur la menace

PRESTATAIRES
- Gestion du risque de tiers
- Dépendances au cloud

Programme de la BCE pour 2027-2029 : deux campagnes d'inspections, sur la cybersécurité et sur le risque de tiers.

Le règlement (UE) 2022/2554 sur la résilience opérationnelle numérique du secteur financier est applicable depuis le 17 janvier 2025. Il couvre quatre volets : la gestion du risque informatique, la déclaration des incidents, les tests de résilience et la gestion du risque porté par les prestataires de services informatiques.

Les priorités de supervision 2027-2029 de la BCE, publiées le 19 novembre 2026, prévoient deux campagnes d'inspections, sur la cybersécurité et sur le risque de tiers, des tests d'intrusion fondés sur la

menace menés selon DORA et une revue des dépendances au cloud.

NOTRE LECTURE

Depuis l'entrée en application, le sujet n'est plus de se mettre en conformité sur le papier, mais de prouver que le dispositif fonctionne : registre des prestataires à jour, incidents déclarés dans les délais, tests suivis d'actions. Les changements de système, comme une migration de core banking ou un passage au cloud, sont les moments où ce dispositif est le plus exposé.

CE QUE NOUS FAISONS

Prise en compte des exigences DORA dans les projets de migration et de transformation des systèmes, tenue des données du registre des prestataires, documentation des contrôles.

DORA | Risque de tiers | Cloud

CORE BANKING→

POUR ALLER PLUS LOIN

Sources officielles.

BCE, priorités de supervision 2027-2029	https://www.bankingsupervision.europa.eu/framework/supervisory-policy/html/ssm.supervisory_priorities202611.en.html
ACPR, dossier DORA	https://acpr.banque-france.fr/fr/reglementation/focus-sur-la-reglementation/transverse/digital-operational-resilience-act-dora
AMF, dossier DORA	https://www.amf-france.org/fr/actualites-publications/dossiers-thematiques/dora
EIOPA, dossier DORA	https://www.eiopa.europa.eu/digital-operational-resilience-act-dora_en

Liens vérifiés le 23 novembre 2026.