

DORA — résilience opérationnelle numérique du secteur financier

Mise à jour le 29/10/2026

1. Statut juridique et entrée en application

DORA est le règlement (UE) 2022/2554 du 14 décembre 2022. Il est applicable depuis le 17 janvier 2025. Il ne faut pas confondre ce règlement directement applicable avec la directive (UE) 2022/2556 qui procède à des ajustements sectoriels et nécessite une transposition nationale.

DORA harmonise la gestion des risques liés aux technologies de l'information et de la communication (TIC) dans les entités financières visées et le suivi de certains prestataires tiers de services TIC.

2. Entités concernées et principe de proportionnalité

Le périmètre comprend notamment établissements de crédit, entreprises d'investissement, assureurs, entités de paiement et autres acteurs financiers définis par le règlement. L'intensité des exigences dépend du type et des caractéristiques de l'entité.

Les entreprises TIC non financières ne deviennent pas automatiquement des entités financières soumises à toutes les obligations de DORA. En revanche, les prestataires TIC critiques désignés sont soumis à un cadre européen spécifique de surveillance.

3. Cinq grands blocs d'obligations

- Gouvernance et cadre de gestion des risques TIC : responsabilité de l'organe de direction, politiques, cartographie des actifs, continuité et reprise.
- Gestion et notification des incidents majeurs TIC selon les classifications, contenus et délais des normes techniques applicables.
- Tests de résilience opérationnelle numérique, avec tests avancés fondés sur la menace (TLPT) pour les entités visées.
- Gestion du risque lié aux prestataires TIC : contrats, concentration, auditabilité, stratégie de sortie, registre des contrats.
- Partage volontaire d'informations sur les cybermenaces dans les conditions du règlement.

4. Application pratique

Pour un établissement financier : dresser l'inventaire des services TIC et de leurs dépendances, définir les seuils d'incident majeur, vérifier le dispositif de notification et le registre des contrats de prestataires.

Distinguer la continuité d'activité, la sauvegarde, la reprise après sinistre et les obligations de notification. Un contrat cloud n'est pas « conforme DORA » sans analyse de son périmètre, de ses droits d'audit et des modalités de sortie.

5. Vigilance réglementaire

Les délais de notification et modèles de déclaration sont fixés par les textes délégués et d'exécution ; ne pas inventer un délai unique pour tous les incidents. Les sanctions et autorités compétentes doivent être appréciées selon la situation et les règles de mise en œuvre.

Le règlement 2022/2554 s'applique depuis 2025 même si toutes les mesures de transposition de la directive d'accompagnement ne sont pas finalisées dans un État membre.

Sources institutionnelles

<https://eur-lex.europa.eu/eli/reg/2022/2554/oj>

https://finance.ec.europa.eu/regulation-and-supervision/financial-services-legislation/implementing-and-delegated-acts/digital-operational-resilience-regulation_en

https://finance.ec.europa.eu/news/digital-finance-2024-12-19_en