LES FICHES RÉGLEMENTAIRES CLOUD TEMPLE

DORA, en clair

LES FAITS

Le Digital Operational Resilience Act est un règlement européen qui vise à renforcer la résilience opérationnelle numérique du secteur financier au sein de l'Union Européenne, en établissant un cadre uniforme pour la gestion des risques liés aux Technologies de l'Information et de la Communication (TIC).

Il sera directement applicable dans tous les États membres de l'UE à partir du 17 janvier 2025, sans nécessiter de transposition nationale.

LE CONTEXTE

Face aux dangers croissants liés à la digitalisation du secteur financier, la Commission européenne a lancé l'initiative DORA en septembre 2020. Cela s'inscrit dans une stratégie globale de renforcement de la finance numérique en Europe, répondant à la vulnérabilité grandissante des systèmes numériques.

DORA est une « lex specialis » qui précise, complète et prime sur NIS 2 pour le secteur financier pour la gestion des risques liés aux technologies de l'information. Elle doit entrer en vigueur en janvier 2025.

LES PILIERS	QUELS IMPACTS POUR LES ACTEURS CONCERNÉS?
Gestion des risques liés aux TIC	DORA impose aux entités d'établir un cadre robuste de gestion des risques TIC, englobant l'identification des actifs, la protection contre les menaces, la détection des incidents et les processus de réponse. Les entreprises doivent prouver leur maîtrise des risques numériques et disposer de stratégies de gestion efficaces.
Tests de résilience opérationnelle numérique	DORA rend obligatoire la réalisation de tests réguliers de résilience opérationnelle numérique, comprenant des analyses de vulnérabilité, des tests de pénétration, des simulations de crise et des tests de reprise. Ces évaluations visent à confirmer la capacité des entités à poursuivre leurs activités critiques lors de perturbations majeures.
Gestion des incidents et reporting	DORA exige une gestion améliorée des incidents avec des procédures de détection et de classification selon leur gravité. Les entités doivent signaler rapidement les incidents majeurs aux autorités et partager les informations sur les menaces avec les autres acteurs, favorisant ainsi une meilleure réactivité sectorielle.
Gestion des risques liés aux tiers et fournisseurs de services TIC	Face à la dépendance aux prestataires TIC et services cloud, DORA établit une gestion stricte des risques liés aux tiers. Cela englobe l'évaluation préalable des risques, des contrats détaillés sur la sécurité, une surveillance continue des performances et des stratégies de sortie pour les fournisseurs critiques.

L'ANALYSE

Giuliano Ippoliti,
directeur de la Conformité de Cloud Temple

« Inspiré des principes de gestion de la norme ISO 27001 et en complément de la directive NIS 2, le règlement DORA met l'accent sur la résilience opérationnelle de l'ensemble du secteur financier face aux perturbations numériques, notamment en cas de crise cyber. Il insiste sur l'importance pour les organisations de développer une capacité proactive d'anticipation, de réponse et d'adaptation, afin d'assurer la continuité de leurs activités. »

QUI DOIT SE CONFORMER À DORA?

DORA s'applique à 21 types d'entités financières comme les établissements de crédit, entreprises d'investissement, assureurs, gestionnaires de fonds, et services de crypto-actifs.

La réglementation s'étend aussi aux fournisseurs tiers critiques de services TIC de ces entités, comme les fournisseurs de services cloud et de cybersécurité, les plateformes d'analyse de données ou encore les prestataires d'infrastructures et de réseaux critiques.

CLOUD TEMPLE
Innovative by design