MARIE-AGNÈS NICOLET,

Présidente de REGULATION PARTNERS, Présidente du comité magazine et membre du conseil d'administration du centre des professions financières

Cybersécurité : comment assurer la résilience du secteur financier ?

Le **règlement européen « DORA »** sur la résilience opérationnelle numérique du secteur financier vise à harmoniser et renforcer les exigences encadrant les risques opérationnels numériques des entités financières au sein de l'Union européenne. Il s'applique à partir du 17 janvier 2025.

Ce nouveau cadre de gouvernance s'appuie sur six piliers :

Une gouvernance renforcée : L'organe de direction est au cœur de la gestion des risques liés aux Technologies de l'information et de la communication (TIC). Il définit, approuve, supervise et est responsable de la mise en œuvre de toutes les dispositions relatives à la gestion des systèmes d'information.

Un dispositif de gestion des risques informatiques solide, complet et bien documenté intégré au système global de gestion des risques. Il détermine notamment le niveau de tolérance au risque informatique de l'entité financière en fonction de son appétit pour le risque et sa tolérance à l'incidence des perturbations informatiques.

Un processus de **gestion des incidents** permettant de détecter, gérer et notifier les incidents liés aux TIC.

Des **tests de résilience opérationnelle numérique** faisant partie intégrante du cadre de gestion des risques informatiques. Les entités financières soumettent tous les systèmes et applications informatiques essentiels à des tests au moins une fois par an.

Une **gestion des risques liés aux prestataires de services en matière de technologie de l'information et de la communication (TIC)**, encadrée par une stratégie soulignant les dépendances existantes à l'égard des prestataires. Une distinction est opérée entre ceux qui couvrent des services

TIC soutenant des fonctions critiques et ceux qui ne le font pas. Les Autorités européennes de supervision (ESMA, EBA, EIOPA) devront désigner les prestataires des services TIC critiques pour les entités financières, sur la base de critères définis par le règlement et ces prestataires seront directement supervisés par une autorité européenne de supervision.

Le **partage d'information** des entités financières entre elles dans l'objectif d'améliorer la résilience opérationnelle numérique.

Ce cadre est totalement nouveau car si les établissements de crédit, paiement, monnaie électronique et sociétés de financement, entre autres, devaient déjà suivre les orientations de l'Autorité bancaire européenne, ce texte sera à appliquer à l'ensemble des institutions financières européennes de la banque, assurances et asset management (avec des exemptions très réduites)

Et ceci se justifie évidemment par le caractère systémique des cybermenaces

Le centre des professions financières a donc souhaité approfondir le sujet en faisant s'exprimer dans ses colonnes des universitaires et d'autres nombreux experts de ce sujet, pour nous faire mieux comprendre ces nouvelles menaces et les anticiper.

Ce magazine complète donc les réflexions de la conférence organisée en juin 2022, qui avait pour vocation de mettre en exergue les réponses concrètes face aux nouvelles menaces et annonce la nouvelle conférence sur ce thème qui approfondira en 2023 certains aspects de la cyber prévention et résilience.

Nous vous souhaitons une excellente lecture.