

Le 17 janvier 2025, les autorités de surveillance des services financiers compétentes attendront des entreprises assujetties qu'elles soient pleinement conformes à toutes les nouvelles exigences de DORA (Digital Operational Resilience Act).

Faut-il le rappeler, ce nouveau texte ambitionne de renforcer la résilience opérationnelle numérique de l'ensemble des acteurs du secteur financier afin de minimiser l'impact d'éventuels incidents sur leur clientèle et sur leur écosystème.

Chacun devra donc se conformer aux cinq piliers du règlement que sont : la gestion des risques liés aux TIC, la gestion des incidents, la mise en œuvre de tests de résilience, la gestion des prestataires de services TIC, la coopération en matière de partage d'information cyber.

Cependant DORA n'a pas vocation à apporter un degré de complexité supplémentaire mais au contraire, permettre d'établir un cadre réglementaire robuste et pragmatique visant à préserver la résilience des organisations des services financiers.

Les établissements de paiement sont évidemment assujettis à DORA mais sans que des exigences spécifiques ne soient formulées.

Pour autant, les enjeux liés à la résilience et aux exigences en termes de performances (disponibilité, sécurité/intégrité des données...) sont déjà au cœur des préoccupations des acteurs de l'écosystème des paiements. Bien évidemment, les services de paiement sont au cœur de l'économie, vitaux pour les entreprises, petites ou grandes, les associations... et certains acteurs ont déjà dû faire face à des incidents ou des attaques d'ampleurs variées (vol de données, DDOS, fraude). Certains dispositifs ont donc été mis en place et des tests de résilience sont même organisés ponctuellement par les instances de place sur un champ plus ou moins étendu.

Cependant, les défis pour les acteurs concernés par DORA sont nombreux et le premier chantier déterminant doit être l'identification des fonctions critiques ou importantes et les actifs qui soutiennent ces fonctions. Cette liste d'actifs critiques est nécessaire par la suite pour répondre aux exigences en termes de traitement des incidents majeurs ou de testing.

Une vigilance particulière devra également être portée sur la conformité aux exigences relatives à la gestion des tiers dans un écosystème dans lequel on peut observer une tendance à l'externalisation et aux partenariats. Un enrichissement des analyses de risques, la mise en place d'un nouveau registre ou encore une revue des clauses contractuelles sont donc à prévoir.

Alors que les établissements les plus matures, comme les banques, s'attarderont à adapter des processus existants afin de se conformer aux exigences communes, d'autres devront fournir des efforts bien plus significatifs.

<https://finegan.fr/reglementation-dora-applications-et-impacts/>