CyberDORA — Mes obligations DORA

RÉGIME COMPLET

Grande entité financière

Banque, assurance, entreprise d'investissement ou autre entité de l'article 2 dépassant les seuils de proportionnalité.

Vos obligations

1. **Gouvernance des risques TIC approuvée et supervisée par l'organe de direction (Art. 5-6).**

   Le conseil d'administration ou la direction générale doit valider la stratégie de résilience numérique, en assurer le suivi régulier et en répondre directement vis-à-vis du superviseur.

2. **Registre des actifs informationnels et TIC tenu à jour (Art. 8).**

   Concrètement : cartographier tous les systèmes, applications et flux de données critiques, et identifier les interdépendances entre eux.

3. **Détection, classification et notification des incidents majeurs dans les délais réglementaires (Art. 17-19).**

   Un incident jugé majeur déclenche une notification initiale rapide à l'autorité compétente, suivie d'un ou plusieurs rapports intermédiaires puis d'un rapport final.

4. **Tests de résilience numérique annuels, avec TLPT tous les 3 ans si désignée significative (Art. 24-26).**

   Les entités les plus importantes doivent en outre simuler des attaques réelles via des tests de pénétration basés sur la menace (TLPT), sur leurs systèmes en production.

5. **Registre d'information sur l'ensemble des contrats avec des prestataires TIC (Art. 28).**

   Ce registre, transmis aux autorités, liste chaque prestataire, le service rendu, son niveau de criticité et ses éventuels sous-traitants.

6. **Plan de continuité d'activité et de reprise après sinistre (Art. 11-12).**

   Il doit fixer des objectifs de temps de reprise (RTO) et de perte de données maximale tolérée (RPO), et être testé périodiquement.