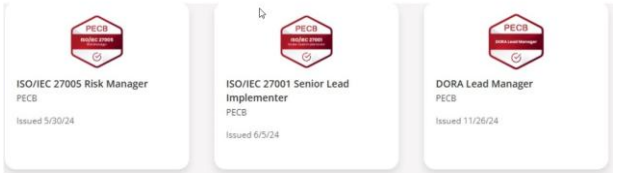
Digital **O**perational **R**esilience **A**ct



Introduction à DORA

- **Qu'est-ce que DORA ?**
  - Réglementation européenne (2022/2554)
  - Objectif : Renforcer la résilience opérationnelle numérique du secteur financier
  - Applicable à toutes les entités financières de l'UE et à leurs prestataires ICT
  - Date limite de conformité : 17 janvier 2025

Chapitre II : Gestion du risque lié aux TIC
Chapitre III : Gestion des incidents liés aux TIC
Chapitre IV : Tests de résilience opérationnelle numérique
Chapitre V : Gestion du risque lié aux tiers prestataires de services TIC

Gestion du risque TIC sous DORA

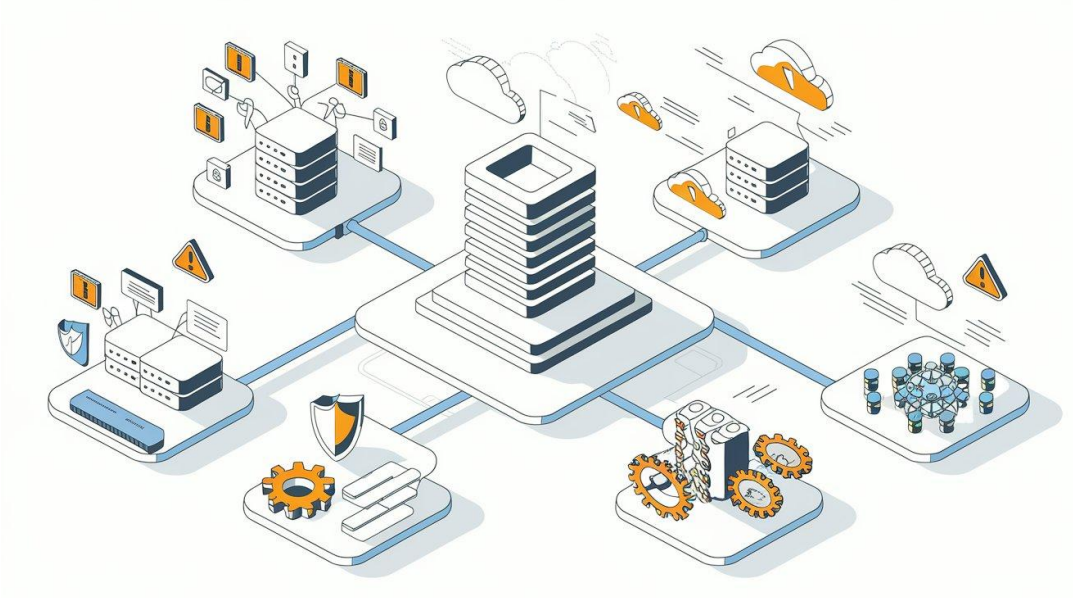
Cadre de gestion des risques TIC

- Gouvernance et organisation
- Identification et classification des actifs TIC
- Protection et prévention des incidents
- Détection et gestion des incidents TIC
- Continuité d’activité et reprise après incident

Gestion des risques liés aux tiers TIC

Évaluation et suivi des risques tiers.

- Sélection des prestataires TIC (due diligence)
- Gestion des risques tout au long du contrat
- Stratégies de sortie et plans de continuité spécifiques
- Documentation et suivi régulier



TIC (Technologies de l'information et de la communication)

Les TIC couvrent tout ce qui est relatif aux technologies numériques utilisées pour :

- **Traiter** (analyser, calculer, organiser),
- **Stocker** (conserver, sauvegarder),
- **Transmettre** (envoyer, communiquer),
- **Recevoir** (accueillir, récupérer) des données sous forme électronique.

Signalement des incidents et des menaces cyber

- **Notification des incidents majeurs**
  - Délais stricts de notification
    - 4h initial, 72h rapport médian, 1 mois rapport final
  - Contenu et format harmonisés
  - Coopération avec les autorités compétentes
  - Notification volontaire des menaces cyber significatives

Tests de résilience opérationnelle

TLPT (Threat-Led Penetration Testing)

- Identification des entités financières soumises à TLPT
- Tests basés sur les menaces réelles (TIBER-EU)
- Phases de préparation, tests, clôture et remédiation
- Collaboration entre testeurs internes/externes et autorités compétentes

- **Phase de préparation : environ 4 à 6 semaines**
- **Phase active (test proprement dit) :** minimum 12 semaines
- **Phase d'analyse, clôture et remédiation :** environ 4 semaines

Durée totale typique : entre **16 et 20 semaines (environ 4 à 5 mois)** en général

Coopération et échange d'informations

- Supervision paneuropéenne

- Coordination entre autorités compétentes nationales et européennes
- Échange d'informations pour suivi des risques ICT
- Cadre unifié d'échange d'informations
- Éviter doublons et redondances

étapes clés pour démarrer la conformité DORA

Former une équipe de pilotage DORA : Désigner des responsables, notamment un CISO ou un DPO, pour gérer le projet.
Réaliser un état des lieux (Gap Analysis) : Évaluer la maturité actuelle en cybersécurité et résilience opérationnelle numérique.
Créer le cadre de gestion des risques TIC : Mettre en place une politique interne sur la gestion et l'atténuation des risques liés aux TIC.
Élaborer un registre des services TIC externes : Lister tous les prestataires tiers fournissant des services numériques critiques.
Développer un plan de continuité d'activité TIC : Prévoir des procédures claires en cas d'incident majeur.
Préparer les tests de résilience opérationnelle : Planifier des scénarios de test (y compris TLPT) pour vérifier la robustesse des systèmes.
Concevoir un processus de gestion des incidents TIC : Prévoir notification, gestion et documentation des incidents.
Former et sensibiliser le personnel : Assurer une formation continue sur les exigences de cybersécurité.

Pourquoi choisir LL Advisory ?

Une approche pragmatique et sur-mesure

- Une expertise certifiée en gouvernance et cybersécurité
- Une capacité à piloter des projets complexes et internationaux
- Une optimisation des coûts et des processus IT
- Un engagement fort pour la sécurité et la conformité réglementaire
- Des certifications mondialement reconnues

Linkedin
Laurent LEPIEZ consultant en cybersécurité, 30 ans d'expertise en informatique
Certifié ISO 27001, LI 27005, DORA Lead manager