EURO CYBER GROUP

RÉSILIENCE

CYBERSÉCURITÉ

CONFORMITÉ

FINANCE

DORA : Réglementation européenne sur la résilience numérique des entités financières, en application dès janvier 2025.

# GAP ANALYSIS DORA

## Description de DORA

La réglementation DORA (Digital Operational Resilience Act) est une législation européenne adoptée par tous les États membres de l'Union européenne en décembre 2022. Elle vise à renforcer la résilience opérationnelle numérique des entités financières. DORA impose des exigences strictes en matière de gestion des risques liés aux technologies de l'information, de rapport d'incidents TIC, de tests de résilience et de gestion des tiers fournisseurs, afin de mieux protéger le secteur financier contre les cybermenaces et les perturbations technologiques. La réglementation DORA entre en application début janvier 2025.

## Composition des piliers DORA

### Pilier 1 Gestion des risques liés aux TIC

Ce piliers impose aux entités financières de mettre en place des politiques et des processus solides pour identifier, évaluer et gérer les risques liés aux technologies de l'information. Cela inclut la protection des systèmes critiques, la continuité des activités, et une surveillance proactive des menaces.

### Pilier 2 Rapport d'incidents TIC

Les entités doivent établir des procédures claires pour signaler les incidents liés aux technologies de l'information. Cela inclut la documentation des incidents, leur analyse, et leur communication rapide aux autorités compétentes et aux parties prenantes internes.

### Pilier 3 Test de résilience opérationnelle numérique

Ce pilier exige que les entités effectuent régulièrement des tests de résilience sur leur systèmes critiques. Ce tests, incluant des scénarios réalistes de cyberattaques, permettent d'évaluer et d'améliorer la capacité des entités à répondre aux perturbations et à renforcer leur résilience.

### Pilier 4 Gestion des risques liés aux TIC par des tiers

Les entités doivent évaluer et surveiller les risques TIC posés par leurs fournisseurs tiers. Cela implique des évaluations régulières, des audits, et l'intégration des fournisseurs dans les tests de résilience pour assumer leur conformité aux exigences de sécurité.

### Pilier 5 Partage d'informations et de renseignements

Le dernier pilier encourage la coopération et le partage d'informations sur les menaces et les incidents TIC entre les entités financières et les autorités compétentes. Des mécanismes sécurisés doivent être mis en place pour échanger des renseignements tout en assurant la confidentialité des données partagées.

## Entités concernées par DORA

- Les sociétés de gestion
- Les institutions bancaires
- Les prestataires de services de communication de données
- Les entreprises d'assurance et de réassurance,
- Les intermédiaires d'assurance, de réassurance et d'assurance à titre accessoires
- Les institutions de retraite professionnelle
- Les agences de notation de crédit
- Les contrôleurs des comptes et les cabinets d'audit
- Les administrateurs d'indices de référence d'importance critiques
- Les prestataires de service de financement participatif
- Les référentiels des titrisations,
- Les tiers prestataires de services informatiques.

# EXPERTISE SUR DEMANDE EN CONFORMITÉ DORA
# GESTION DES RISQUES, TECHNOLOGIES ET RÉSILIENCE OPÉRATIONNELLE

## DES EXPERTS À VOTRE SERVICE POUR VOUS ACCOMPAGNER SUR LA RÉGLEMENTATION DORA

Optimisez votre conformité DORA avec nos experts en gouvernance et conformité. Nous offrons une flexibilité totale en mettant à votre disposition des spécialistes qualifiés pour répondre à vos besoins en gestion des risques TIC, de résilience opérationnelle et de gouvernance.

## La méthodologie de notre Gap Analysis

### Identification des rôles clés et des responsabilités

Identification des rôles clés et des responsabilités des personnes impliquées dans la gestion des risque TIC conformément à la réglementation DORA.

### Décomposition de DORA par fonction concernée :

Analyse des exigences DORA en fonction des parties prenantes de l'organisation.

### Création de questionnaires par fonction :

Élaboration de questions ciblées pour chaque fonction afin d'effectuer l'évaluation de la conformité.

### Collecte et analyse des données :

Recueil des réponses via entretiens et identification des écarts de conformité

### Résultats et plan d'action :

Développement d'un plan d'action pour remédier aux écarts identifiés lors de l'analyse des réponses.

## Rapport du Gap Analysis DORA

À l'issue de la prestation, le client reçoit un rapport détaillé comprenant une synthèse managériale des constats clés et recommandations. Le rapport rappelle brièvement les exigences de la réglementation DORA, avec une synthèse des piliers et des articles. La méthodologie du gap analysis est expliquée, suivie d'une liste des fonctions et interlocuteurs évalués.
Enfin, une restitution détaillée des écarts identifiés est fournie, organisée à la fois par piliers et par fonctions, accompagnée d'un plan d'action précis pour combler chaque écart et assurer la conformité complète à la réglementation DORA.

## Pourquoi nous choisir ?

Une expertise éprouvée dans la conformité DORA, avec une équipe dédiée qui maîtrise à la fois les aspects techniques et réglementaires.

Une méthodologie personnalisée, adaptée aux besoins spécifiques de chaque entreprise pour identifier précisément les écarts de conformité.

## Pourquoi faire un Gap Analysis ?

Anticiper les exigences réglementaires avant l'entrée en vigueur en janvier 2025 pour éviter les sanctions potentielles.

Identifier et corriger les vulnérabilités dans la gestion des risques TIC et la résilience opérationnelle.

Planifier et évaluer les coûts ainsi que la charge de travail nécessaires à la mise en conformité.

Renforcer la confiance des parties prenantes (clients, autorités, partenaires) grâce à une conformité démontrée.

Membre de la Fédération Française de la Cybersécurité.

EXPERT CYBER

UGAP

CRiP

## CONTACTEZ NOUS

contact@eurocybergroup.fr - 01 46 94 62 00
Euro Cyber Group - 75 rue de Lourmel - 75015 Paris

**www.eurocybergroup.fr**