

Digital Operational Resilience Act « DORA »

Analyse d'impacts du Règlement
européen sur la résilience
opérationnelle numérique

Janvier 2023

Contexte réglementaire

Les établissements de finance et d'assurance ont subi 20% des cyber attaques en France en 2021 selon le rapport d'Anozr Way.



Un risque significatif

**01**

Pluralité de vulnérabilités :
technologiques, organisationnelles,
opérationnelles, humaines, etc.

02

Croissance de l'exposition au risque :
télétravail, open banking, accès à des
sources de données internes/externes,
entités transfrontières, etc.

03

Un contexte appelant à la vigilance :
Secteur financier parmi les plus ciblés
pendant la pandémie ;
Craintes liées à la guerre en Ukraine et
aux sanctions à l'encontre de la Russie,
etc.

Le « Digital Operational Resilience Act » traduit la forte préoccupation du législateur face au risque cyber



Risque singulier
nécessitant une
**harmonisation des
règles sectorielles à
l'échelle européenne...**



...et une meilleure
**sensibilisation des autorités
de surveillance** aux cyber-
risques et aux incidents
liés à l'informatique.



Outils dédiés issus des
règles sectorielles
existantes développées
par les AES et les
superviseurs...



...renforcées par les
mesures ciblées comme la
**surveillance des
prestataires critiques.**



6 piliers couverts par le règlement DORA



Extraits de notre étude détaillée

 Focus sur les principes généraux du règlement DORA

Présentation du périmètre d'application du règlement DORA et calendrier prévisionnel de mise en œuvre



 Analyse d'impacts des thèmes abordés

Analyse d'impacts des 6 piliers couverts par le Règlement DORA



 Roadmap indicative de mise en œuvre des travaux DORA

Focus sur l'approche proposée par Aurexia pour la mise en œuvre des travaux DORA



Nos capacités d'accompagnement

Un accompagnement sur l'ensemble des travaux de mise en conformité DORA



01

Doctrine

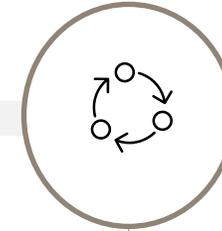
- Analyse réglementaire des textes et production de la norme DORA de l'entreprise
- Cartographie et revue des conventions de service avec des TIC pour mise à jour avec les besoins de DORA



02

Mise en œuvre opérationnelle

- Définition du processus et des procédures de gestion des incidents liés aux TIC
- Définition de la politique et des procédures de gestion des risques de tiers pour les TIC multifournisseurs



03

Conduite du changement

- Conception et déploiement des parcours de formation à destination des équipes impliqués
- Acculturation des collaborateurs sur le risque cyber et les bonnes pratiques

PILOTAGE TRANSVERSE DU PROJET

- Mise en place de la gouvernance
- Organisation des comités de suivi et comités de pilotage
- Suivi des jalons, des KPI, des risques et du budget





David VILLARD

Senior Partner

Tel : +33 (0) 6 75 53 19 47

david.villard@aurexia.com



Guillaume LEROY

Partner

Tel : +33 (0) 6 20 93 62 38

guillaume.leroy@aurexia.com

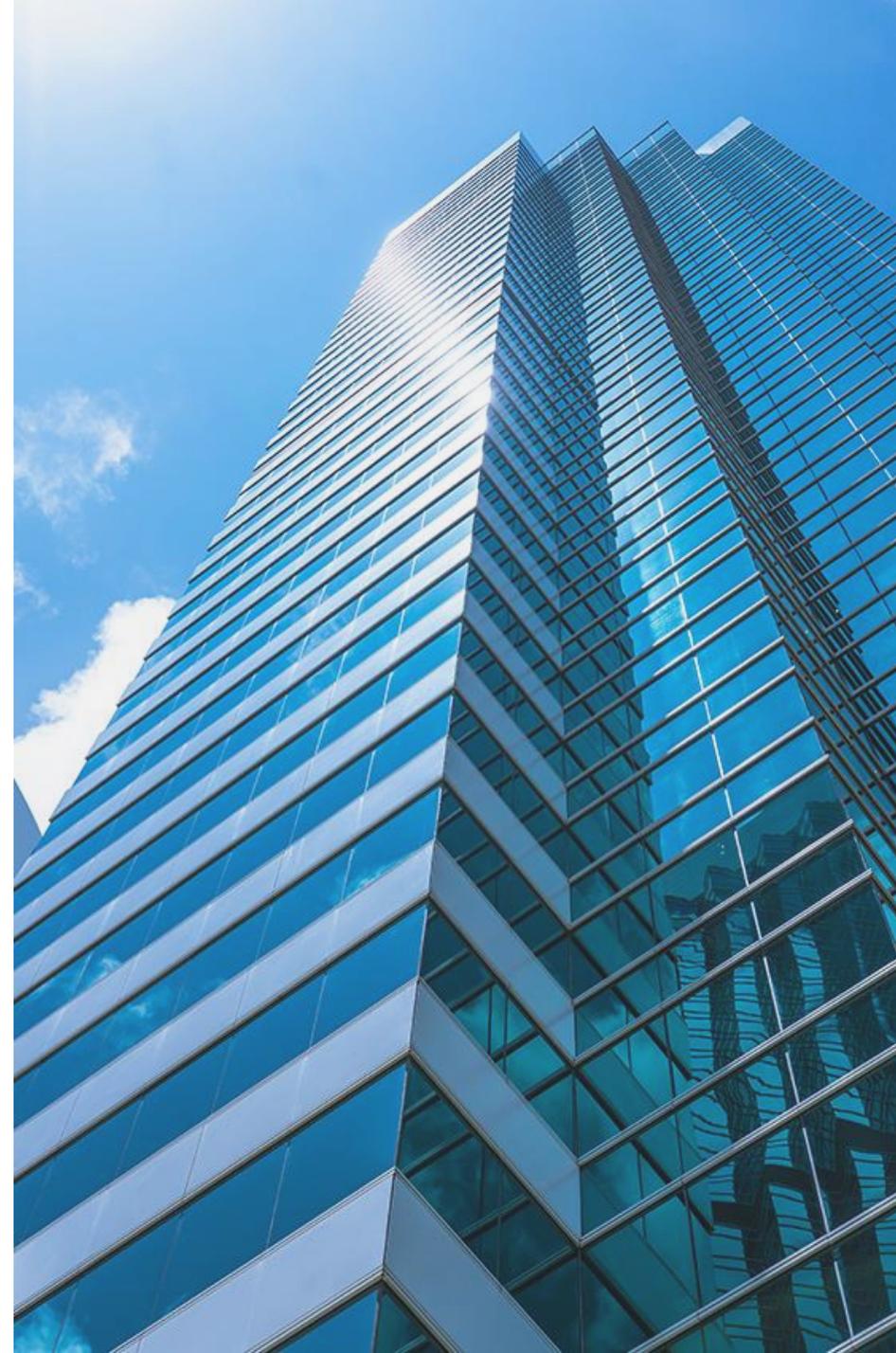


Geoffroy VUATRIN

Director

Tel : +33 (0)6 24 76 04 48

geoffroy.vuatrin@aurexia.com





Aurexia

Bringing value, together