ZOOM

LA MISE EN CONFORMITÉ DORA

WEALTH & ASSET MANAGEMENT

ACCÉLÉREZ VOTRE MISE EN CONFORMITÉ À LA RÉSILIENCE OPÉRATIONNELLE NUMÉRIQUE

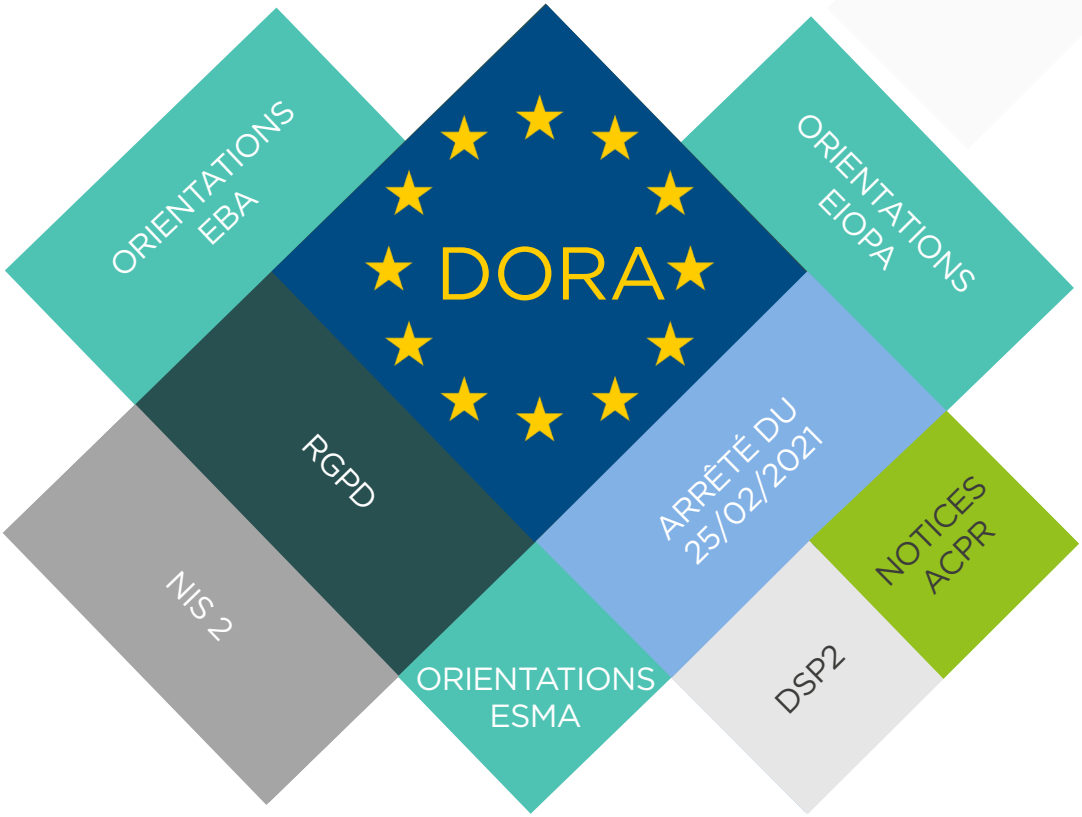
LE RÈGLEMENT DORA SE FONDE SUR DES RÉGLEMENTATIONS PRÉCÉDEMMENT PUBLIÉES

L'objectif du règlement DORA (Digital Operational Resilience Act) est d'harmoniser et d'homogénéiser la lutte contre le risque cyber systémique qui pèse aujourd'hui sur le secteur financier, à l'échelle de l'Union Européenne.

Avant son entrée en vigueur, il existait déjà divers règlements, dont il s'inspire à des degrés divers, qui visaient à réduire les risques IT et cyber des entités financières au sein de l'UE.

- Sans doute votre établissement est-il déjà en partie conforme à DORA du fait des textes existants qui vous sont directement applicables.
- Il est toutefois probable qu'un écart existe entre les exigences spécifiques de DORA et votre niveau de conformité actuel.

Textes à considérer pour la mise en conformité à DORA



TNP

FOCUS SUR LES ACTEURS DU WEALTH / ASSET MANAGEMENT

Le risque cyber est identifié dans le TOP 3 des menaces pour 2/3 des SGP

Un RSSI est nommé pour seulement 68% des SGP, tendance stable depuis 2020 mais en nette augmentation depuis 2018 (+50%)

Les budgets dédiés à la sécurité augmentent pour 97% des SGP (+10% en 1 an)

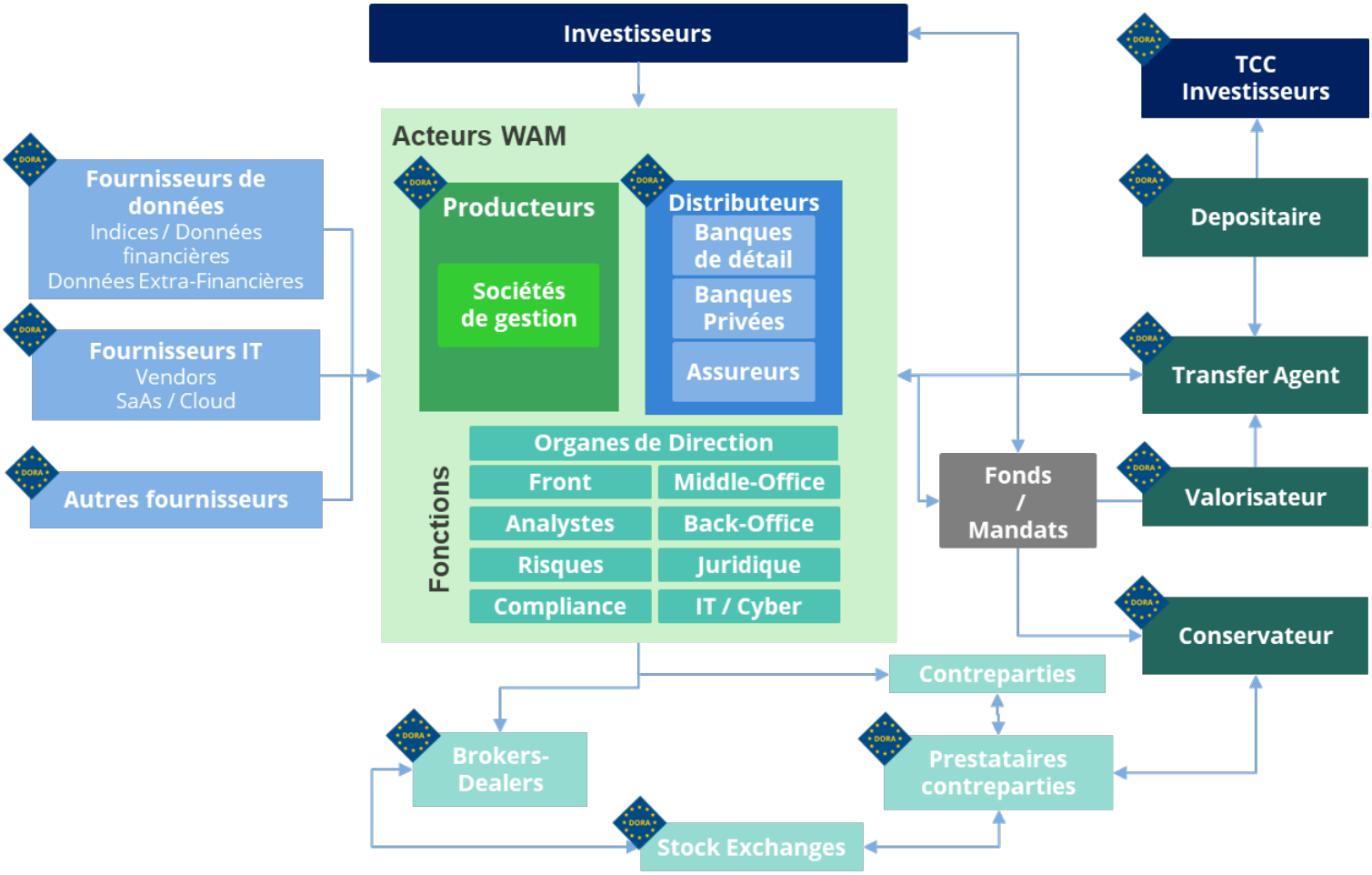
53% des SGP disposent de tableaux de bord de reporting et 81% d'entre elles ont mis en place des comités semestriels dédiés à la cybersécurité

Livre Blanc AFG Innovations Technologiques
Quelles stratégies pour les SGP ? – Février 2023

Les acteurs de la chaîne de valeur de la gestion d'actifs impactés par DORA

DORA nécessite une revue du cadre de gouvernance et de contrôle interne liée à la gestion des risques cyber ainsi que celui de la gestion du risque de tiers avec notamment la supervision directe des prestataires de services critiques.

Une revue contractuelle avec les prestataires de services TIC sera également à prévoir.



QUELLES NOUVEAUTÉS DANS DORA ?

DES EXIGENCES
RENFORCÉES
ET INÉDITES

- Certaines exigences existantes, comme l'obligation de réduire le risque de concentration des fournisseurs, feront l'objet d'une surveillance accrue de la part des autorités compétentes.
- D'autres seront appliquées à l'ensemble des fournisseurs TIC, notamment les stratégies de sortie.

Sont introduites de nouvelles exigences :

- Organisationnelles, telles que l'implémentation d'une stratégie multi-fournisseurs de services TIC ou la mise en place de dispositifs de partage d'informations sur les cybermenaces entre entités financières ;
- Techniques, tels que les tests de pénétration fondés sur la menace et l'élaboration de scénarios de cyberattaques.

VOTRE MISE EN CONFORMITÉ EN 4 ÉTAPES

Analyse d'écart

Sur la base de l'évaluation effectuée, la liste des écarts de conformité est établie selon les degrés de difficulté et les priorités.

Accompagnement opérationnel

Nous vous assistons dans la réalisation de vos travaux grâce à nos consultants experts en cybersécurité : audit de sous-traitants, red teaming, politiques de sauvegardes, incidents...

Évaluation indépendante

Nous vous aidons à mesurer votre résilience opérationnelle numérique selon les 5 piliers de DORA, grâce à la mobilisation de nos équipes cybersécurité, réglementations et métiers.

Feuille de route

Les actions sont quantifiées, priorisées, et leurs conditions de suivi sont définies.
DORA prévoit la validation de ce plan d'actions par l'organe de direction, dont l'implication est attendue dans la gestion du risque lié aux TIC.

UN ACCOMPAGNEMENT MÉTIER ET TRANSVERSE

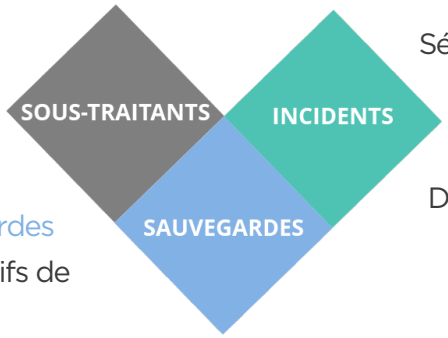
Au-delà de l'accompagnement à la mise en conformité DORA, nos consultants sont mobilisés pour vous assister sur les activités suivantes :

Évaluation des prestataires

Analyse contractuelle

Politiques de sauvegardes

Evaluation de dispositifs de sauvegardes



Sécurité offensive : Red teaming

Investigations numériques

Détection et réponse à incidents (CSIRT)

Gestion de crise et résilience

Nos activités d'audit cybersécurité sont qualifiées PASSI en France sur toutes les portées

DES NORMES TECHNIQUES RÉGLEMENTAIRES À SUIVRE DE PRÈS

La période de mise en conformité est courte (24 mois) considérant l'ampleur du chantier relatif notamment aux prestataires ainsi qu'aux normes techniques réglementaires (Regulatory Technical Standards – RTS).

16 janvier 2023 — Entrée en vigueur du texte

17 janvier 2024 — Date limite des RTS #1
Les Autorités de Surveillance Européenne doivent soumettre les RTS concernant les articles 15,16,18 et 28 du règlement (1)

17 juillet 2024 — Date limite des RTS #2
Adoption par la Commission d'un acte délégué précisant les critères de désignation des prestataires « critiques », les détails de l'article 43 (2) et ceux concernant les articles 20, 26, 30 et 41 (2)

17 janvier 2025 — Application de DORA
Rapport sur la mise en place d'un centre européen de déclaration des incidents

(1)
Art.15 : Outils, méthodes, processus, politiques de gestion du risque lié aux TIC
Art.16 : Cadre simplifié
Art 18 : Classification des incidents et des cybermenaces
Art 28 : Stratégie de risques liés aux prestataires TIC / Modèles types aux fins du registre d'informations

(2)
Art 20 : Contenu et modèles des rapports de notification
Art 26 : Tests avancés
Art 30 : Sous-traitance de services TIC
Art 41 : Supervision des prestataires de services TIC critiques
Art 43 : Redevances de supervision

CONTACTS

Pascal ANTONINI
Partner Cybersécurité
+33 (0)6 08 74 64 54
pascal.antonini@tnpconsultants.com

Nadège REYNAUD
Directrice Associée Cybersécurité
+33 (0)6 82 16 73 82
nadege.reynaud@tnpconsultants.com

Boyan YANKOV
Partner Wealth/Asset Mgt
+33 (0)6 46 86 40 55
boyan.yankov@tnpconsultants.com

Christophe COTTE
Directeur Associé Wealth/Asset Mgt
+33 (0)6 63 21 79 62
christophe.cotte@tnpconsultants.com