DORA

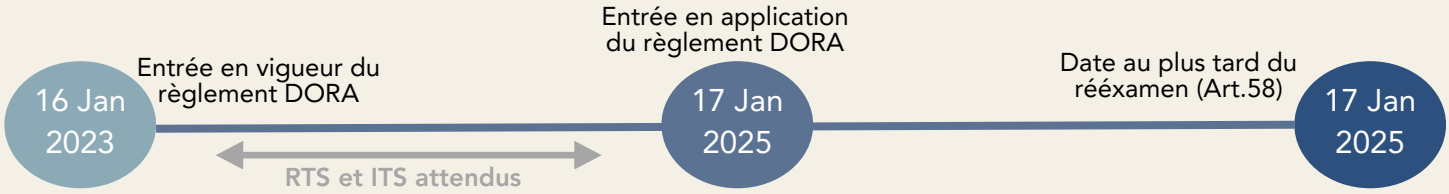
L'Europe adresse par DORA le risque systémique de la cyber-criminalité financière
Coup d' œil sur le RÈGLEMENT (UE) 2022/2554 DU PARLEMENT EUROPÉEN ET DU CONSEIL du 14 décembre 2022

Instance réglementaire

Parlement européen & le conseil de l'union européenne
Avec le support de Comité européen du risque systémique (CERS)

Scope

Toutes les entités financières à l'exception des fonds alternatifs, assurance/réassurance/courtier, institutions de retraite, offices des chèques postaux, et la CDC si l'état français en fait le choix.



Contexte

L'interconnexion des systèmes des 22 000 entités financières de l'Union européenne rend l'ensemble du système financier vulnérable à la cyber-criminalité, et confère une potentialité systémique à ce type d'attaque.

Objectif

Le règlement vise consolider et à mettre à niveau les exigences en matière de risque lié aux technologies de l'information dans le cadre des exigences en matière de risque opérationnel (considérant 12), pour atteindre un niveau élevé de résilience opérationnelle numérique (article premier)

Description

Le règlement définit des exigences en matière i) de gestion des risques liés aux TIC*, ii) de communication avec les autorités, iii) de tests de résilience, iv) de gestion opérationnelle et contractuelle des prestataires (extrait de l'article premier).

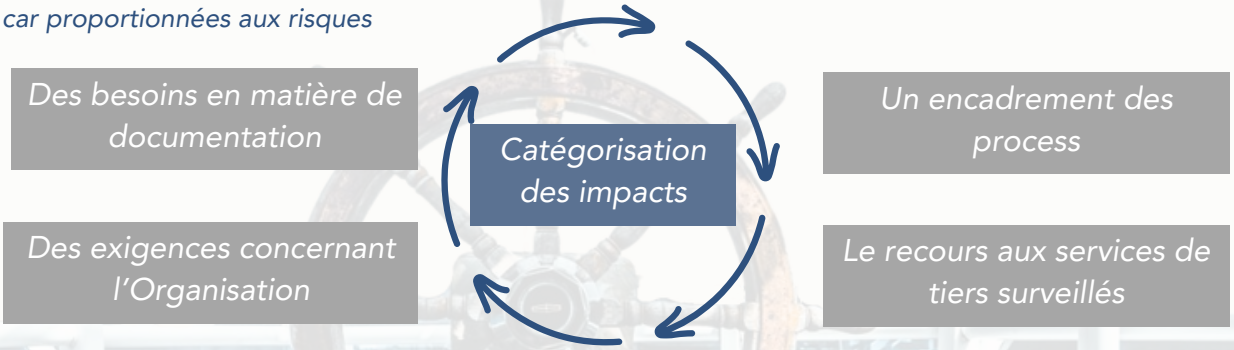
Quels impacts pour les établissements ?

Comment regarder le texte ?

Le secteur financier est celui auquel le grand public accorde le plus de confiance en matière de sécurité informatique. Cela résulte d'un investissement important des établissements dans leurs systèmes et infrastructures.

Notre conviction : partir de l'existant pour vérifier l'adéquation des pratiques en place avec les exigences de Dora, et les améliorer/renforcer le cas échéant.

Attention toutefois aux prestataires tiers critiques de services TIC (article 31) qui endosseront des exigences plus importantes car proportionnées aux risques



TIC* : Technologie de l'Information et de la Communication (pour tout le reste du document)

SOLENT CONSULTING

DORA

Formalisme exigé par DORA

Liste non exhaustive de documents dont doit disposer un groupe dans son ensemble, et qui est explicitement mentionnée dans le texte. Au titre de l'article 38, ces documents sont exigibles du superviseur général dans le cadre d'une inspection.

Stratégie

Groupe

Entreprise

Départements

Opérationnel

Stratégie de gestion des risques

Stratégie de résilience opérationnelle (article 6) : justification du cadre de gestion, niveau de tolérance, indicateurs (perf, risque), architecture des TIC, mécanisme de détection et mitigation, analyse as-is, tests, stratégie de com'

Stratégie en matière de risque liés aux tiers, et stratégie de sortie de contrat (article 28)

Politique de gestion des risques

Politique de continuité des activités de TIC, intégrable à la politique de continuité des activités (article 11)

Plan de communication, en situation de crise (article 14)

Politiques d'utilisation des TIC fournis par le prestataire (article 28)

Politiques et procédures de sauvegarde, définissant données et fréquence (article 12)

Politique relative aux modalités d'utilisation des services TIC (article 5)

Procédures de gestion des risques

Procédure de capture et suivi des incidents (article 17)

Plan de réponse et de rétablissement des TIC, audité par l'Audit interne (article 11)

Procédure et méthode de restauration (article 12)

Procédure de hiérarchisation et résolution des incidents (article 24)

L'articulation entre les documents faitiers de plus haut niveau (Groupe ou entreprise) et les procédures opérationnelles reste à l'appréciation de l'entreprise.

Les processus mentionnés au sein de DORA sont presque tous implémentés au sein de votre organisation. Néanmoins, il conviendra de vérifier les exigences ultérieures de la commission en matière de classification (critères à prendre en compte) et de reporting (format). Par ailleurs, s'il existe un processus budgétaire, les critères d'allocation du budget sont sans doute à revoir par rapport à l'existant.

Lors d'un incident (temps)

Processus d'identification

- Détection incidents (Article 10)

Processus de gestion d'incidents

- Traitement incidents (Article 17)
- Suivi incidents (Article 17)
- Remédiation (Article 17)

Processus d'analyse

- Classification incidents (Article 18)
- Classification incidents (Article 18)
- Analyses incidents (Article 17)
- Evaluation du risque (Article 13)
- Veille sectorielle (Article 22)

Reporting

- Déclaration d'incidents majeurs (article 19)
- Notification des cyber-menaces (Article19)
- Reporting clients et contrepartie (article 14)

Processus permanent

Test & controle

- Test de résilience (article 25)
- Test de pénétration tri annuel (Article 26)
- Contrôle permanent (Article 9)
- Constitution d'inventaire (Article 8)

Processus budgétaire

- Revue périodique et allocation (article 5)

Sur base quantitative principalement et donc mise en place d'indicateurs spécifiques

SOLENT CONSULTING

DORA

Organisation, des responsabilités étendues pour le management

Organe de direction (article 5)

- Responsable (ultime) de la gestion des risques
- Mise en place de la stratégie
- Définition des responsabilités et gouvernance associée
- Définition de la tolérance aux risques
- Revue périodique de la politique de continuité de service
- Revue périodique des plans d'audit & audit
- Allocation budgétaire
- Revue périodique de la politique d'utilisation des services

Confirmé à l'article 28 :
- Même en cas de délégation de service, il n'existe pas de délégation de responsabilité

Livrables exigés à l'article 8 :
- cartographie des métiers,
- cartographie des rôles
- listes des rôles et dépendance

Concernant le risque lié aux TIC

article 8 :
- sécurité et fonctionnement des TIC soumis au contrôle permanent

article 10 :
- allocation de ressources et de capacités suffisantes pour surveiller l'activité des utilisateurs

Le texte s'inscrit dans une tendance réglementaire consistant à incarner les responsabilités pour individualiser les sanctions. Ainsi, la responsabilité des dirigeants est engagée lors de la survenance de problèmes de sécurité.

Article 50 : les autorités compétentes peuvent convoquer les représentants des entités financières, et leur demander de fournir oralement ou par écrit des explications.

Lorsque des sanctions administratives (pour manquement aux obligations) sont appliquées, les autorités compétentes peuvent les appliquer aux membres de l'organe de direction

Article 52 : applications de sanctions pénales si justifiées

Ces responsabilités vont peser lors des exercices budgétaires spécifiques au sujet (qui doivent ne tenir compte que des besoins, et non des moyens….).

Utilisation des services de tiers, quelques règles à avoir en tête

Le contenu de l'accord est formalisé à l'article 30 : donne un droit illimité d'accès d'inspection et d'audit par le « client » (ce qui est conforme à l'exigence de responsabilité qui pèse sur le client)

Pour le client

Article 28 : - pas de délégation de responsabilité au prestataire -> prévoir de pouvoir auditer le tiers
- tout nouvel accord ou projet d'accord fait l'objet d'une déclaration aux autorités compétentes (nouveau process)

Article 29 : -évaluation du risque de concentration avant contractualisation (une attention particulière est portée aux services opérés depuis l'étranger)

Pour le prestataire

Article 31 : ce sont les autorités compétentes qui qualifie le caractère « critique » d'un prestataire de service TIC (« prestataire tiers critique de services TIC). Dans ce cas, ce prestataire fait alors l'objet d'une attention plus étroite par le superviseur. Cette qualification de prestataire tiers critique de services TIC peut s'appliquer aux entités financières.

Article 33 : le prestataire fait l'objet de plan de supervision chaque année

Article 35 : le superviseur émet des recommandations

--> 30 jours calendaires pour livrer le plan d'action. Au-delà, astreinte journalière (pendant 6 mois max) allant jusqu'à 1% du CA journalier de l'année précédente --> Astreinte rendue publique

Article 42 : le prestataire a 60 jours calendaires pour justifier auprès d'une autorité compétente le non suivi d'une recommandation

Article 43 : le superviseur principal perçoit, auprès des prestataires tiers critiques de services TIC, des redevances (pour couvrir ses frais de supervision)

SOLENT CONSULTING
Gardez le cap sur vos projets

Pour aller plus loin, discutons de vos priorités.

Jérôme Haniez - Associé
jhaniez@solent-consulting.com
+33 6 30 27 89 24