COMETH CONSULTING

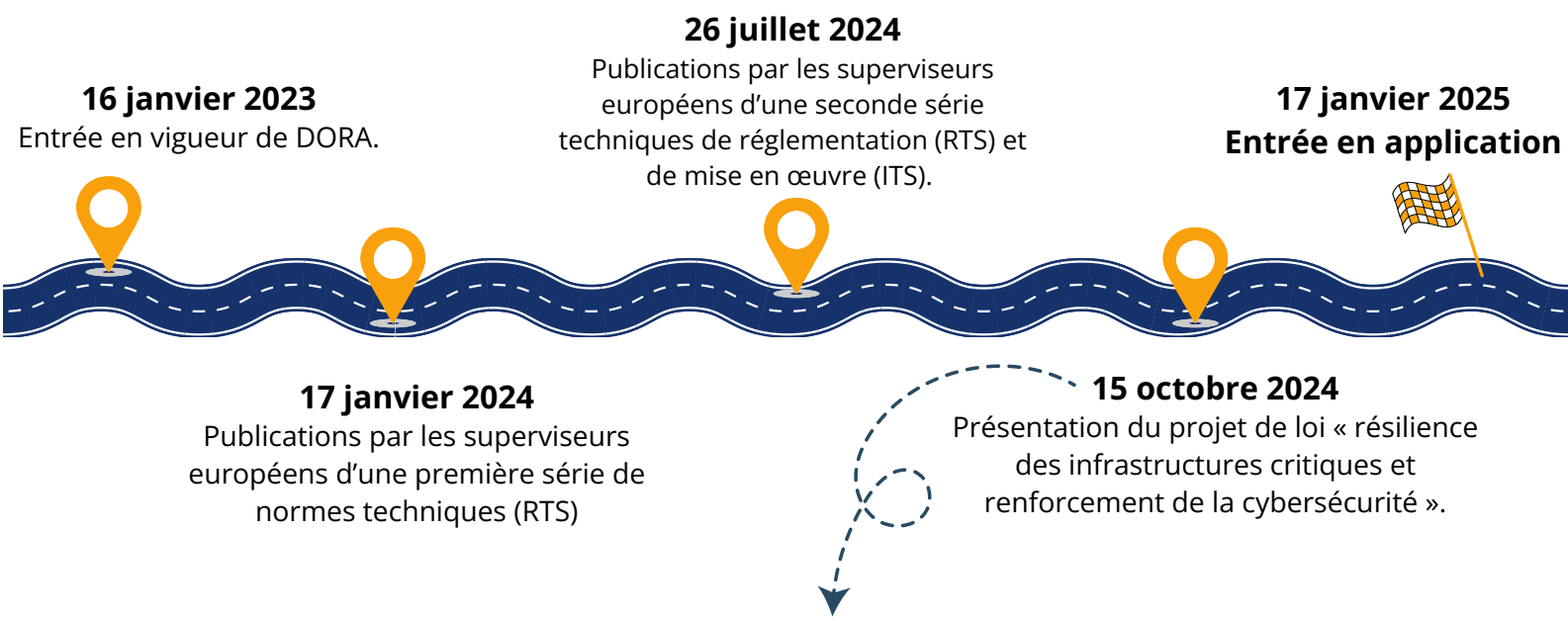
DORA

Dernière ligne droite ECL #140

Le Digital Operational Resilience Act (DORA) vient redéfinir en profondeur la gestion des risques liés aux technologies de l'information et de la communication (TIC) dans le secteur financier européen.

À partir du 17 janvier 2025, cette nouvelle règlementation s'appliquera à toutes les institutions financières de l'UE, avec pour objectif **de renforcer leur résilience numérique et de protéger les infrastructures critiques contre les cybermenaces.**

Calendrier



Le gouvernement a déposé un projet de loi visant à transposer le règlement DORA en droit français. Ce texte, présenté lors du conseil des ministres du 15 octobre 2024, s'inscrit dans une démarche plus large **de renforcement de la cybersécurité et de la résilience des infrastructures critiques**. Le projet inclut également la **transposition de deux autres directives européennes :** la directive sur la résilience des entités critiques **(REC)** et la directive **NIS2.**

Afin de respecter le délai fixé au 17 janvier 2025 pour la transposition, le gouvernement a opté pour une procédure accélérée. Celle-ci permet de limiter le processus parlementaire à une seule lecture par le Sénat et l'Assemblée nationale.

Les 5 piliers de la règlementation DORA

1. Gestion des risques TIC

DORA impose la mise en place **d'une gouvernance solide** pour gérer les risques technologiques, en mettant l'accent sur la responsabilisation des dirigeants, notamment du conseil d'administration**.** Ce cadre repose sur des politiques internes et des processus de gestion des risques visant à adopter une posture proactive en matière de sécurité. L'objectif est de renforcer la responsabilité des décideurs face aux risques, en assurant **une gestion plus réactive et anticipative des vulnérabilités technologiques**

2. Gestion, classification et notification des incidents liés aux TIC,

Les institutions financières se doivent désormais de détecter rapidement les incidents, limiter les perturbations, et informer les autorités compétentes en cas d'incident majeur. Une documentation complète est requise pour chaque incident, incluant une évaluation de l'impact opérationnel et financier. La communication avec les parties prenantes internes et externes est essentielle pour la transparence. Enfin, les processus de gestion des incidents doivent être régulièrement revus pour s'adapter aux nouvelles menaces et renforcer la résilience.

3. Tests de résilience opérationnelle numérique

Ce pilier met l'accent sur l'importance de tester régulièrement la robustesse des systèmes critiques. Deux types de tests sont requis : les **tests de résilience opérationnelle annuels pour les systèmes critiques,** et les **tests de pénétration dirigés par les menaces (TLPT)** tous les trois ans pour les institutions jugées essentielles. Ces tests doivent être supervisés par des autorités compétentes et intégrés des experts tiers pourassurer leur objectivité.

4. Gestion des risques liés aux prestataires Tiers de services TIC

Le pilier de gestion des risques liés aux prestataires tiers de services TIC dans DORA exige la mise en place de mesures permettant d'identifier et évaluer les risques associés aux fournisseurs externes, notamment en termes de sécurité et de continuité des services. Pour cela, les contrats avec les fournisseurs doivent spécifier clairement les exigences en matière de résilience et de sécurité. Une surveillance continue des prestataires est indispensable pour garantir qu'ils respectent les engagements pris.

5. Dispositif de partage d'informations des cyberattaques

Le pilier dispositif de partage d'informations des cyberattaques de DORA vise à renforcer la résilience numérique des institutions financières par un partage rapide et sécurisé des informations relatives aux cyber-incidents. Ce système de partage facilite la détection précoce des menaces et la gestion des risques, permettant ainsi une réponse coordonnée pour limiter l'impact des attaques. L'objectif est de renforcer la sécurité collective en encourageant la collaboration entre les autorités, les institutions financières et leurs partenaires.

La mise en conformité avec le Digital Operational Resilience Act (DORA) est une obligation légale mais également une opportunité stratégique pour les institutions financières. En effet, DORA impose des exigences rigoureuses en matière de gestion des risques numériques, de résilience face aux incidents et de protection des infrastructures critiques, dans le but de garantir une continuité des services et de renforcer la confiance des parties prenantes.

Notre approche pour vous accompagner :

En tant qu'**expert des organismes d'assurances et de la conformité réglementaire,** notre **approche pragmatique et complète,** nous permet de vous proposer un accompagnement personnalisé et adapté à votre structure :

DIAGNOSTIC DE L'EXISTANT

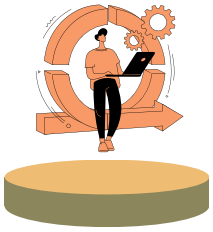
Identification des vulnérabilités spécifiques à votre organisation.

FEUILLE DE ROUTE RÉGLEMENTAIRE

Stratégies de conformité sur mesure pour répondre aux exigences DORA.

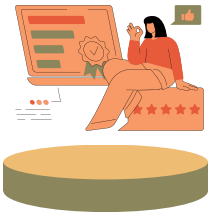
MISE EN ŒUVRE

Accompagnement dans l'implémentation des mesures nécessaires.



FORMATION ET SUPPORT CONTINU

Conduite du changement et plan d'amélioration continue.



RENDEZ-VOUS PROCHAINEMENT POUR UN NOUVEL ÉCLAIRAGE...
N'HÉSITEZ PAS À NOUS CONTACTER POUR VOS BESOINS D'ACCOMPAGNEMENT.

Cabinet de conseil en Organisation et Systèmes d'Information

Créer de la valeur et s'engager sur la réussite.
Ensemble.

COMETH Consulting - Tour Trinity, 1bis Place de la Défense, 92400 - Courbevoie
www.cometh-consulting.com / contact@cometh-consulting.com / Tél : 01 40 54 83 81