

DORA

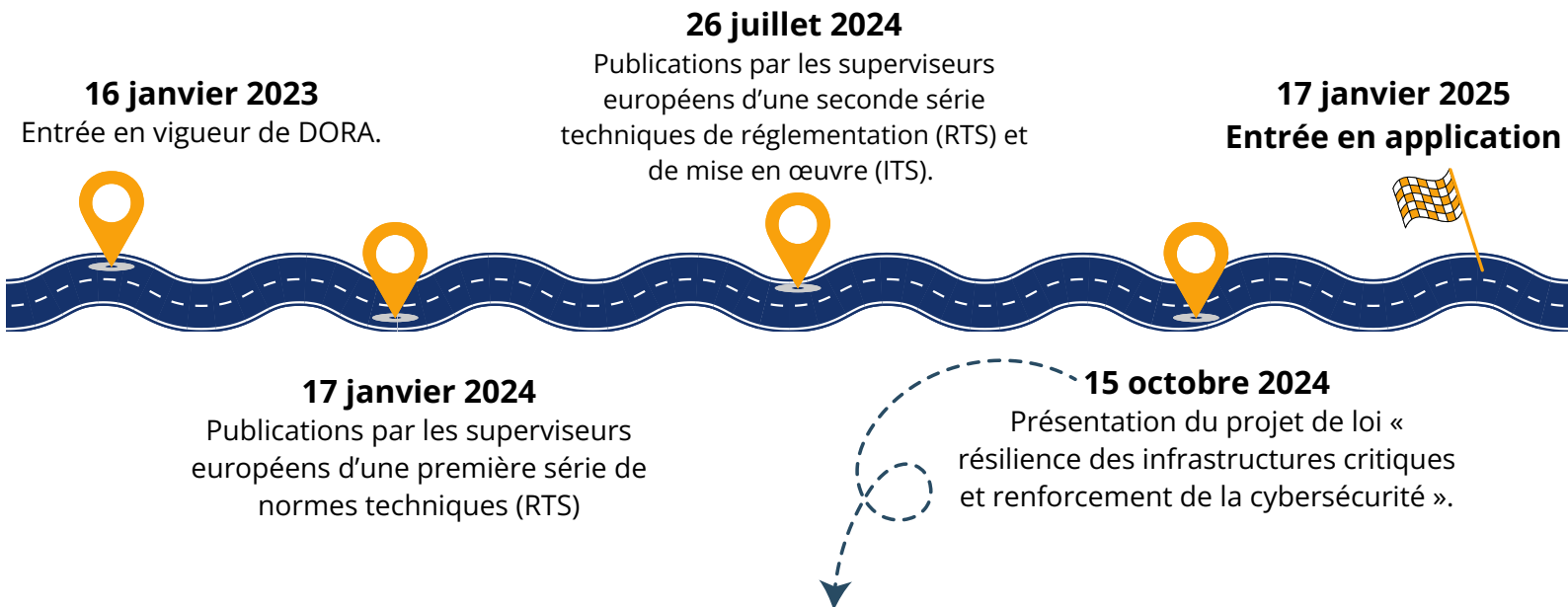
Dernière ligne droite

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 réglementation 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**.

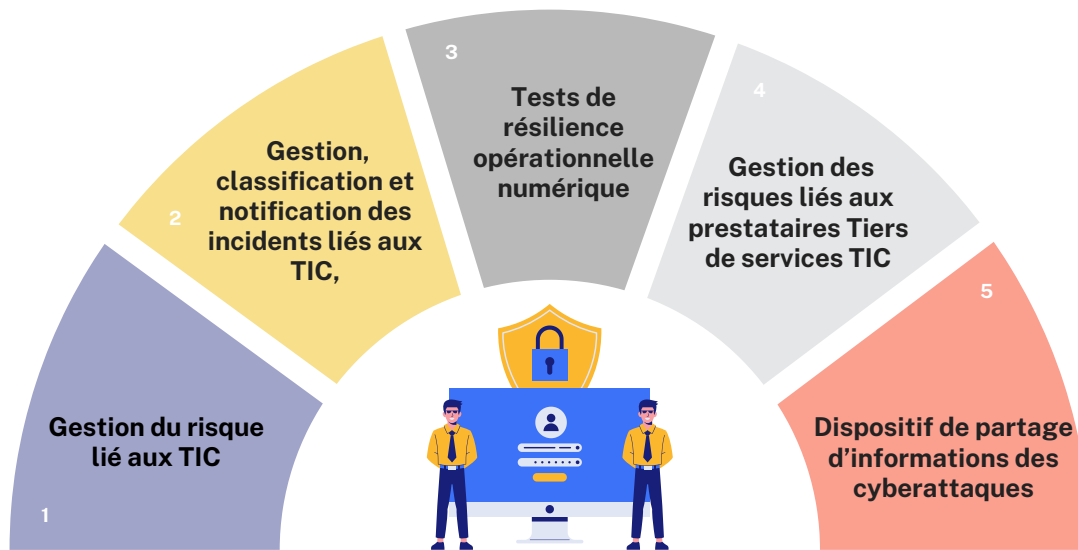
Calendrier



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 de ces réglementations, 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, accélérant ainsi l'examen du projet.

Les 5 piliers de la réglementation 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,

DORA exige une **identification précise des risques liés aux TIC**, y compris les cybermenaces, les défaillances des infrastructures et les risques associés aux prestataires de services. Les entreprises devront **intégrer ces risques dans leur stratégie globale**, en **développant des plans de continuité et de reprise d'activités**.

3. Tests de résilience opérationnelle numérique

Ce pilier met l'accent sur l'importance de **tester régulièrement la robustesse des systèmes critiques** face aux cybermenaces. 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 réalisés par des experts tiers pour assurer leur objectivité. DORA vise ainsi à identifier et corriger les vulnérabilités, renforçant la sécurité des systèmes et la résilience face aux cyberattaques.

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. En cas de défaillance ou d'incident, des mécanismes de gestion des crises et des plans de continuité des activités doivent être prévus afin de minimiser les perturbations des services critiques.

5. Dispositif de partage d'informations des cyberattaques

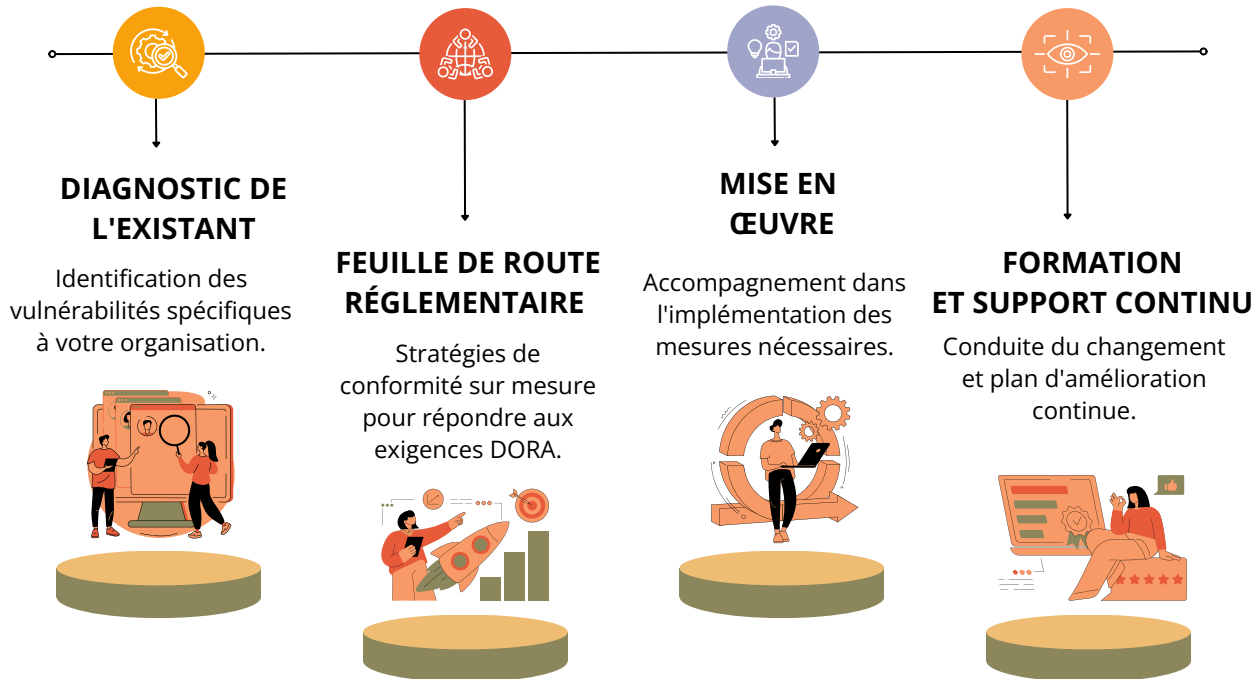
Le pilier dispositif de partage d'informations des cyberattaques de DORA vise à **renforcer la résilience numérique des institutions financières** par un **partage rapide et sécurisé des informations relatives aux cyberincidents**. Les entités doivent **mettre en place des mécanismes pour signaler les cyberattaques majeures aux régulateurs dans un délai de 24 heures** et, le cas échéant, **partager ces informations avec d'autres acteurs du secteur**. 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**.

Dans un **contexte de cybersécurité de plus en plus complexe**, marqué par des **attaques de plus en plus fréquentes et sophistiquées**, la **mise en conformité** avec le Digital Operational Resilience Act (DORA) **devient non seulement une obligation légale** mais aussi une **nécessité 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 la 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 :



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

CONFORMITE REGLEMENTAIRE - DATA MANAGEMENT - GESTION DE PROJET - FORMATION & SENSIBILISATION



Cabinet de conseil en Organisation et Systèmes d'Information

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

Ensemble.

