

Redéfinir la sécurité financière :

Guide de la conformité DORA et de la résilience des données avec Veeam



Introduction : maintenir le cap dans une ère de cyber-résilience

Des cyberattaques aux pannes système, en passant par les ransomwares, les institutions financières sont confrontées à des menaces numériques incessantes qui peuvent perturber leur exploitation, ternir leur réputation et entraîner d'importantes pertes financières. En réponse, l'Union européenne a adopté le [Règlement DORA](#) (Digital Operational Resilience Act), entré en vigueur le 17 janvier 2025. DORA établit des normes strictes pour les banques, les compagnies d'assurance, les sociétés d'investissement et leurs partenaires technologiques afin de résister aux perturbations numériques et de s'en remettre efficacement.

Pour les dirigeants, DORA est synonyme de nouvelles responsabilités et d'une responsabilisation accrue, mais représente aussi une excellente occasion de positionner leur organisation en tête des structures fiables et résilientes dans un paysage financier de plus en plus numérique.

Les ransomwares restent une menace permanente. Selon le [rapport sur les risques pour la résilience en 2025](#), **69 %** des entreprises ont subi au moins une attaque par ransomware l'année dernière. Dans les faits, **89 %** des entreprises victimes d'une attaque par ransomware ont vu leurs bases de sauvegarde ciblées, ce qui met en danger les données sensibles et les capacités de restauration. Le besoin d'infrastructures cyber-résilientes n'a jamais été aussi évident.

Pourquoi le règlement DORA est-il important ?

DORA s'applique à un large éventail d'entités financières ainsi qu'à leurs fournisseurs de technologies critiques, en harmonisant les exigences en matière de résilience numérique dans toute l'Union européenne. Le secteur financier est chargé de faire preuve d'une vigilance sans faille — en garantissant la résilience opérationnelle à grande échelle face à des perturbations graves liées aux menaces.

La non-conformité expose à des amendes substantielles, à une atteinte à la réputation, à des perturbations opérationnelles, et engage la responsabilité personnelle de la direction. La conformité protège non seulement votre entreprise et vos clients, mais renforce également la confiance et l'avantage concurrentiel.

Le règlement DORA en bref : les cinq piliers

Les exigences de DORA reposent sur cinq piliers clés, adaptés à la taille et à la complexité de votre organisation :



1. Gérer les risques numériques :

Mettez en place des infrastructures robustes pour identifier, évaluer et limiter les risques liés aux TIC, afin de garantir la sécurité et la résilience de vos données et systèmes.



2. Signaler les incidents rapidement :

Notifiez rapidement les régulateurs des cyberincidents importants, tels que les violations de données ou les pannes, afin de permettre une réponse coordonnée et transparente.



3. Tester régulièrement votre résilience :

Effectuez en permanence des tests de résilience, notamment des simulations de crise et des tests d'intrusion, afin de valider votre capacité à résister aux perturbations et à vous en remettre.



4. Superviser les fournisseurs tiers :

Assurez-vous que tous les fournisseurs tiers de TIC, en particulier les fournisseurs critiques tels que les plateformes cloud, répondent aux normes strictes de sécurité et de résilience de DORA.



5. Partager les renseignements sur les menaces :

Collaborez avec vos pairs du secteur en partageant des informations sur les cybermenaces, afin de favoriser une défense collective dans l'ensemble du secteur financier.

Équipes de direction : les attentes vous concernant

En tant que dirigeant, vous êtes responsable de la conformité DORA. Cela signifie que vous devez :

- **Mettre en avant la conformité** : faites de DORA une priorité de leadership et communiquez son importance à l'ensemble de l'organisation.
- **Financer les principales initiatives** : allouez des ressources pour l'analyse des écarts, les mises à niveau du système, la formation du personnel et la supervision des fournisseurs.
- **Favoriser la collaboration** : constituez des équipes interfonctionnelles pour coordonner les efforts de conformité, et impliquer les services informatiques, juridiques, commerciaux ainsi que de gestion des risques.
- **Agir vite** : avec l'entrée en vigueur de l'exigence de conformité, vous devez lancer une analyse des écarts, élaborer une feuille de route de conformité et vous tenir informé des mises à jour réglementaires.

Résilience des données : les bases de la conformité

La véritable résilience des données ne se limite pas à protéger ces dernières. Elle englobe la sauvegarde, la restauration rapide, la sécurité des données, la facilité de la portabilité et la veille. Elle permet aux entreprises de résister, de se relever et de s'adapter

à toute perturbation numérique. Une stratégie de données résilientes constitue la pierre angulaire de la conformité réglementaire, de la continuité d'activité et de la confiance des clients.

Prise en charge de la conformité DORA par Veeam

Les solutions de Veeam sont spécifiquement conçues pour aider les établissements financiers à respecter et même dépasser les exigences de DORA en matière de résilience numérique :



Protection robuste des données : sauvegarde et restauration fiables et sécurisées des données et systèmes stratégiques pour prendre en charge les tests de continuité d'activité, de reprise après incident et de résilience.



Sauvegardes inaltérables : protégez-vous contre les ransomwares grâce aux sauvegardes inaltérables, pour garantir l'intégrité des données et la préparation à la restauration.



Tests automatisés et reporting : la vérification automatisée des sauvegardes et le reporting détaillé simplifient les audits de conformité et la validation de la résilience.



Supervision complète : supervision et alertes en temps réel pour une évaluation continue des risques et une détection rapide des incidents.



Atténuation des risques liés aux tiers : gérez et protégez vos données, avec fluidité, dans l'ensemble des environnements hybrides, multicloud et locaux.



Collaboration et partage sécurisé de l'information : facilitez le partage sécurisé des données pour répondre aux exigences de DORA en matière de réponse coordonnée aux incidents et de renseignements sur les menaces à l'échelle du secteur.



Le leadership de Veeam est reconnu dans le secteur entier. Des milliers d'entreprises lui font confiance et pour la cinquième fois consécutive, Gartner a honoré Veeam en plaçant la société en tête de son classement pour sa capacité d'exécution et en la désignant leader, pour la huitième année, des solutions logicielles de sauvegarde et de restauration des données d'entreprise. Veeam offre l'expertise et les connaissances nécessaires pour démontrer votre conformité à la norme DORA.

Garder une longueur d'avance : DORA est en pleine évolution

Les normes techniques de DORA vont continuer à évoluer. Déléguez à votre équipe de conformité la responsabilité de surveiller les mises à jour réglementaires et d'adapter votre feuille de route

si nécessaire. Une approche proactive permet d'assurer un alignement permanent et de minimiser les risques de conformité.

Mettez l'accent sur la résilience des données — agissez maintenant

DORA est plus qu'une exigence réglementaire ; c'est l'occasion pour vous de renforcer votre résilience numérique et d'être en tête, en toute confiance, dans un contexte volatile. Avec Veeam comme partenaire,

vous pouvez protéger votre entreprise, faire preuve de leadership et établir une relation de confiance durable avec vos clients et les autres parties prenantes.

À propos de Veeam Software

Veeam®, le n°1 mondial de la résilience des données, estime que chaque entreprise doit pouvoir se relever après un incident en conservant la confiance et le contrôle de toutes ses données, au moment et à l'endroit voulus. C'est ce que Veeam appelle la résilience totale. Nous mettons tout en œuvre pour développer des solutions innovantes grâce auxquelles nos clients pourront atteindre cet objectif. Les solutions proposées par Veeam sont conçues pour assurer la résilience des données grâce à des fonctions de sauvegarde, de restauration, de portabilité, de sécurité et d'intelligence des données. Avec Veeam, les responsables informatiques et de la sécurité ont l'assurance que leurs applications et leurs données sont protégées et disponibles sans interruption dans leurs environnements cloud, virtuels, physiques, SaaS et Kubernetes. Basé à Seattle et possédant des bureaux dans plus de 30 pays, Veeam protège plus de 550 000 clients dans le monde, dont 67 % des entreprises du Global 2000, qui font confiance à Veeam pour le maintien de leur activité. La résilience totale commence avec Veeam. Pour en savoir plus, rendez-vous sur www.veeam.com ou suivez Veeam sur LinkedIn [@veeam-software](https://www.linkedin.com/company/veeam) et X [@veeam](https://twitter.com/veeam).

➔ Pour en savoir plus sur DORA et découvrir comment Veeam peut accélérer votre démarche de conformité DORA et préserver l'avenir de votre entreprise, rendez-vous au [Veeam.com](https://www.veeam.com)