Aborder la conformité DORA : guide complet en 7 étapes

La loi sur la résilience opérationnelle numérique (DORA, pour Digital Operational Resilience Act) est un règlement crucial établi par l'Union européenne (UE) pour renforcer la sécurité des entités financières en matière de technologies de l'information et de la communication (TIC). Ce règlement est conçu pour traiter systématiquement la gestion des risques liés aux TIC et compte harmoniser les réglementations appliquées par les différents États membres de l'UE dans ce domaine. DORA vise ainsi à éliminer les failles, les chevauchements et les conflits possibles entre ces réglementations variées selon les pays de l'UE.

Un large éventail d'institutions de l'UE sont concernées par DORA, notamment les banques, les sociétés d'investissement et les institutions de crédit. Le règlement s'applique aussi à des entités moins traditionnelles, comme les prestataires de services d'actifs en cryptomonnaie ou les plateformes de financement participatif. Plus particulièrement, DORA couvre les prestataires de services proposant des systèmes et des services liés aux TIC aux entreprises financières. Cela comprend notamment les fournisseurs de data centers et de services sur le cloud, ainsi que les services d'informations sensibles comme les scores de crédit ou les analyses de données.

DORA décrit les normes techniques que devront mettre en œuvre les entités financières et leurs prestataires de services technologiques tiers essentiels. Ces normes devront être implémentées dans leurs systèmes de TIC avant le 17 janvier 2025. Elles englobent les principes et les exigences pour la gestion des risques liés aux TIC, de ceux liés aux tiers spécialisés en TIC, des tests de résilience opérationnelle numérique, des incidents liés aux TIC, et pour la supervision des prestataires tiers essentiels.

En harmonisant les règles de gestion des risques dans l'UE, DORA compte améliorer la cyberrésilience de tout l'écosystème financier de l'UE et garantir que toutes les institutions respectent la même norme. Ce guide vous accompagnera dans les sept étapes cruciales pour la conformité DORA et vous expliquera comment AvePoint peut aider votre organisation le long de ce parcours.

Ce qu'il faut savoir : nouvelles exigences et obligations avec DORA

Le règlement DORA apporte d'importantes modifications au cadre de sécurité des TIC pour les entités financières de toute l'UE. Pour que votre entreprise construise sa propre résilience contre les menaces liées aux TIC, comprendre les évolutions de la conformité est essentiel.

01 Gouvernance et gestion des risques liés aux TIC

Objet : le règlement DORA met l'accent sur la responsabilité de la direction des entreprises, qui doit garantir la résilience opérationnelle numérique de l'entité. Ce terme désigne la capacité de l'institution financière à construire, assurer et réviser sa fiabilité et son intégrité opérationnelles, en s'armant de toutes les capacités liées aux TIC nécessaires pour protéger son réseau et son système d'information. La direction est chargée de maintenir des défenses appropriées contre les cyberattaques et autres interruptions. Pour ce faire, elle doit mettre en place un cadre complet de gestion des risques liés aux TIC afin d'en permettre l'identification, l'évaluation, la gestion et la surveillance.

Raison : la cybersécurité doit être considérée comme un besoin essentiel des entreprises. L'objectif est de limiter les risques liés aux TIC grâce à une gestion proactive des incidents, une meilleure sécurité de la chaîne d'approvisionnement et des réseaux, une régulation plus stricte des accès et le chiffrement des données. Cette approche systématique d'analyse des risques contribue à la résilience globale face aux menaces liées aux TIC à long terme.

02 Tests de résilience

Objet : le règlement DORA impose de mettre en place un programme de tests de résilience opérationnelle numérique, fondé sur les risques et proportionnel. Ce programme doit comprendre différents tests, dont des analyses open-source, des évaluations de vulnérabilité, des analyses des failles et des évaluations de sécurité des réseaux. Les tests de base doivent être réalisés chaque année, mais les entités financières cruciales doivent se soumettre tous les trois ans à des tests de pénétration fondés sur la menace (ou TLPT pour threat-led penetration testing).

Raison : la sécurité et la stabilité des systèmes de TIC doivent être mises à l'épreuve régulièrement pour que les entreprises financières puissent opérer sans heurts. Les organisations peuvent ainsi évaluer la robustesse de leurs mesures défensives. Une approche de tests axée sur les risques permet aux sociétés de détecter et de traiter efficacement les potentielles interruptions liées aux TIC.

03 Réaction aux incidents et signalement

Objet : les entités financières doivent établir des systèmes pour surveiller, gérer, enregistrer, classer et signaler les incidents liés aux TIC. Ces rapports doivent être envoyés aux autorités de régulation ainsi qu'aux clients et partenaires affectés, en fonction de la gravité de l'incident. DORA exige que les organisations soumettent leurs rapports initiaux dans les quatre heures suivant leur conscience de l'incident, et qu'elles remettent un rapport détaillé dans la semaine.

Raison : la rapidité de signalement permet d'accélérer les mesures de réaction et de restauration, limitant ainsi les effets de l'incident. Cela permet aussi aux autorités de surveiller attentivement le paysage global des TIC et d'agir rapidement pour minimiser les dégâts potentiels.

04 Gestion des risques liés aux tiers

Objet : le règlement DORA prévoit certaines exigences contractuelles concernant les fournisseurs de TIC tiers, qui doivent être implémentées dans la gestion des contrats des institutions financières. Les entités financières sont tenues par DORA de vérifier avec toute la diligence requise que leurs prestataires de services tiers appliquent des pratiques de gestion des risques appropriées. La surveillance et la supervision en continu sont également nécessaires pour s'assurer que les tiers respectent leurs obligations contractuelles et les pratiques de gestion des risques.

Raison : surveiller efficacement ces risques est d'autant plus crucial que les sociétés financières s'appuient fortement sur leurs fournisseurs. Cette mesure vise donc à réduire les risques opérationnels liés aux prestataires tiers pour renforcer les cyberdéfenses et protéger tous les aspects de l'écosystème du secteur financier.

05 Partage d'informations

Objet : le règlement DORA encourage, sans imposer, le partage d'informations entre les institutions financières. Échanger des informations et renseignements sur les cybermenaces au sein de communautés de confiance permet d'améliorer la résilience opérationnelle numérique, à condition que ces échanges respectent la législation applicable en matière de confidentialité des données et de sécurité.

Raison : le partage d'information sensibilise les utilisateurs aux cybermenaces, ce qui limite leur diffusion et augmente les capacités défensives, la détection des menaces, les stratégies d'atténuation et les efforts de réaction et de restauration.

Tracer la voie pour la cyberrésilience

Les nouvelles exigences et obligations de DORA sont conçues pour renforcer la cyberrésilience de l'Europe. En adhérant à ces normes, les entreprises évitent les pénalités pour non-conformité, mais peuvent aussi et surtout améliorer leur approche de gestion des risques liés aux TIC. Elles honorent ainsi la confiance de leurs clients et de leurs parties prenantes. De plus, comprendre et appliquer ces modifications est essentiel pour atteindre et conserver la conformité DORA, ce qui protège à terme l'intégrité et la stabilité du secteur financier tout entier.

Votre liste de contrôle en 7 étapes pour la conformité DORA

Se conformer au règlement DORA implique une approche structurée de la gestion des risques liés aux TIC, ainsi que de garantir la résilience des opérations numériques de votre entreprise. Cette liste de contrôle décrit les étapes essentielles pour satisfaire ces exigences et montre comment AvePoint peut soutenir votre démarche de conformité. .

01 Implémentez des stratégies de gestion des risques et de sécurité des TIC

Ce que vous devez faire : les organisations doivent développer des procédures et des stratégies de sécurité des TIC complètes pour traiter efficacement les risques. Cela implique d'identifier, d'évaluer, de gérer et de surveiller les risques liés aux TIC pour assurer une solide protection contre les interruptions et les cyberattaques.

Comment AvePoint vous aide : AvePoint Policies automatise l'application de vos stratégies de sécurité pour Microsoft 365 et garantit que votre organisation les implémente de manière cohérente. Cette automatisation contribue à la conformité grâce à des vérifications continues du bon respect des politiques de l'entreprise. Elle surveille les dérives et y remédie en implémentant les changements nécessaires. AvePoint Insights s'intègre parfaitement avec AvePoint Policies en vous offrant une vue complète de votre environnement Microsoft 365. Vous pouvez ainsi identifier les vulnérabilités des infrastructures informatiques de votre organisation et évaluer les menaces potentielles en déterminant qui peut accéder aux espaces de travail spécifiques et aux données sensibles.

02 Mettez en place un système de signalement et de gestion des incidents

Ce que vous devez faire : les entités du secteur financier sont tenues d'implémenter des procédés pour enregistrer et signaler rapidement les incidentés de sécurité des TIC. Elles doivent classer et signaler les incidents aux autorités de régulation et aux parties concernées en fonction de la gravité de l'incident.

Comment AvePoint vous aide : AvePoint Cloud Backup peut détecter les ransomware à l'aide de l'IA et les signaler pour que les administrateurs déterminent l'impact de la brèche. La fonctionnalité avancée de gestion des incidents de AvePoint Cloud Backup comprend l'enregistrement et l'alerte automatiques des incidents de sécurité, vous assurant de les détecter et de les signaler.sensibles.

03 Réalisez des tests de résilience opérationnelle numérique

Ce que vous devez faire : le règlement DORA exige que les organisations mènent régulièrement des tests de résilience de leurs systèmes de TIC, y compris des évaluations de vulnérabilité, des analyses de failles et des tests scénarisés. Les entités financières cruciales doivent effectuer des TLPT tous les trois ans.

Comment AvePoint vous aide : l'outil d'évaluation des risques d'AvePoint Insights vous aide à évaluer la résilience des systèmes, à identifier les marges d'améliorations, et à garantir la conformité aux exigences de DORA sur les tests. Il vous apporte également des informations utiles pour prendre des décisions et des recommandations pour renforcer votre infrastructure informatique.

04 Partagez des informations avec vos homologues en toute sécurité

Ce que vous devez faire : DORA encourage les organisations à échanger des informations sur les cybermenaces avec leurs homologues afin d'améliorer la résilience opérationnelle numérique du secteur dans son ensemble. Notez cependant que les entités sont tenues de vérifier que ces informations sont partagées au sein de communautés de confiance et en respectant la législation applicable.

Comment AvePoint vous aide : AvePoint Cloud Governance aide les organisations à gérer les permissions et l'accès aux données, aux contenus et aux espaces de travail. Le cadre de gouvernance ainsi établi permet aux équipes informatiques de garantir le respect du bon niveau de sécurité et de classification de données. Son application harmonieuse des règles à vos espaces de travail contribue à limiter l'accès aux informations sensibles et à protéger vos données.

05 Implémentez des mesures de sauvegarde et reprise après une catastrophe

Ce que vous devez faire : les entreprises doivent stocker leurs sauvegardes séparément et définir des RTO (recovery time objectives) ainsi que des RPO (recovery point objectives). Testez régulièrement vos procédures de sauvegarde et de restauration pour vérifier qu'elles répondent aux besoins de votre organisation.

Comment AvePoint vous aide : AvePoint Cloud Backup Express restaure les données de SaaS 20 fois plus vite que les sauvegardes cloud traditionnelles. Alimenté par le stockage de Microsoft 365 Backup, ce service protège les informations sensibles sur Exchange Online, OneDrive, SharePoint Online, Teams, et Microsoft 365 Groups plus rapidement et à plus grande échelle.

06 Développez et testez votre plan de continuité des opérations

Ce que vous devez faire : les organisations doivent tester leurs plans de continuité des opérations et de sauvegarde et de restauration des données à intervalles réguliers pour s'assurer qu'ils sont efficaces et à jour. Les tests réguliers contribuent à identifier les failles et à améliorer la résilience de vos opérations.

Comment AvePoint vous aide : tout plan de continuité des opérations s'appuie sur des mesures de sauvegarde et de restauration solides. AvePoint Cloud Backup vous permet d'isoler vos sauvegardes de votre environnement de production, protégeant ainsi vos identifiants administrateur pour les sauvegardes, et entrepose vos copies de sauvegarde dans des espaces de stockage immuables. AvePoint a simulé six scénarios de perte de données pour montrer comment AvePoint Cloud Backup peut vous aider à récupérer les données critiques perdues lors de compromission ou de suppression accidentelle des données.

07 Établissez un cadre d'application des stratégies et de gouvernance des données

Ce que vous devez faire : les organisations doivent mettre en place un cadre complet pour l'application des stratégies de sécurité des données et assurer une conformité constante aux exigences réglementaires de DORA. Cela implique de surveiller et d'actualiser en continu les stratégies afin de s'adapter aux menaces émergentes.

Comment AvePoint vous aide : AvePoint Policies peut assister les organisations dans leur gouvernance des données et leur application des stratégies en leur permettant d'automatiser les règles d'accès, de paramètres et d'autres configurations au sein de leur environnement Microsoft 365 pour une application proactive et automatique des stratégies. Cette automatisation les aide à garder le contrôle de leurs données et à assurer le respect des stratégies de gouvernance, ce qui augmente la sécurité des données et la conformité à long terme.

Protégez vos données grâce à AvePoint

Saisir et respecter toutes les nuances de la conformité au règlement DORA exige une approche solide de la gestion des risques liés aux TIC et de la résilience opérationnelle numérique. En suivant ce guide, les organisations peuvent établir des stratégies et des procédures complètes, mettre en œuvre des protocoles de tests rigoureux, et promouvoir des pratiques de partage d'informations sûres.

AvePoint est un partenaire de confiance dans cette démarche, et propose des solutions avancées pour automatiser l'application des stratégies, améliorer les capacités de gestion des incidents et faciliter la sauvegarde et la restauration des données en toute sécurité. Grâce à l'expertise d'AvePoint en gouvernance et en application des stratégies sur plusieurs plateformes cloud, les organisations peuvent répondre aux exigences DORA en toute confiance, renforcer leurs cadres de gouvernance des données et appliquer les meilleures normes de sécurité des données.

Leader mondial de la sécurité et de la gestion des données depuis plus de vingt ans, AvePoint continue de donner aux organisations le pouvoir de protéger leurs opérations numériques, de limiter les risques, et de se conformer aux normes dans un paysage réglementaire en constante évolution.

AvePoint s'engage à appliquer les meilleures normes de confidentialité et de sécurité des données pour ses clients. C'est pourquoi notre entreprise est certifiée ISO 27001, ISO 27701 et ISO 27017, et nous détenons également les certifications SOC2 Type II et CSA STAR de niveau 2. Vous pouvez donc nous faire confiance pour protéger vos données et garantir le respect des réglementations.

AvePoint France

Startway, Immeuble Le Crossing, 24-32 Boulevard Gallieni, 92130 Issy-les-Moulineaux

www.avepoint.com | +33 (0)1 70 61 02 17 | sales@avepoint.com

AvePoint