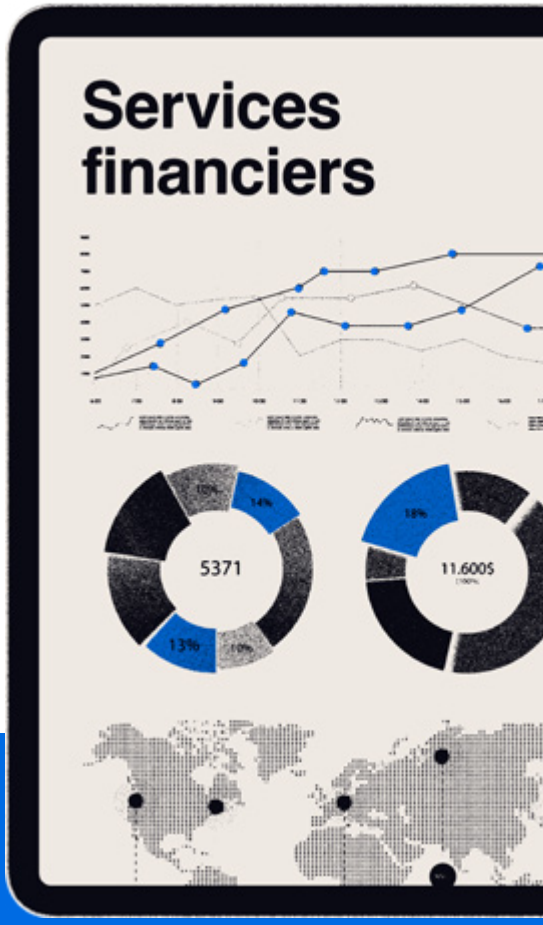
RUBRIK ET LE RÈGLEMENT DORA

Comment Rubrik aide les acteurs des services financiers à se conformer au tout dernier règlement sur la résilience numérique de l'Union Européenne.

Le règlement européen sur la résilience opérationnelle numérique (DORA) a été élaboré pour accélérer la mise en place de capacités de cyber-résilience au sein des sociétés de services financiers. Les États-membres de l'UE sont tenus de transposer le règlement dans leur droit national au 17 janvier 2025. C'est donc maintenant que les établissements de services financiers doivent améliorer leur réponse face aux perturbations opérationnelles, à commencer par les cyberattaques. Mais ils vont pour cela devoir se projeter au-delà de l'approche détecter/protéger pour s'inscrire dans une démarche de résilience/restauration.

Banques, compagnies d'assurance, fonds d'investissement, plateformes d'échange de cryptomonnaies, plateformes de trading… tous les prestataires de services financiers seront dans l'obligation de se conformer au règlement DORA, sans quoi ils seront passibles d'une amende pouvant atteindre 2 % de leur chiffre d'affaires mondial annuel[1].Le montant de l'amende dépendra de la gravité de l'infraction et du degré de coopération de l'entité financière avec les autorités.



Renforcez votre résilience opérationnelle pour vous conformer au règlement DORA

Pour pouvoir renforcer leur résilience opérationnelle et se mettre en conformité avec le règlement DORA, les sociétés de services financiers doivent avant tout répondre à un certain nombre de questions :

1. Quel est leur degré de confiance dans la résilience opérationnelle de leur organisation ?
2. Sachant que les incidents sont inévitables, quel est concrètement le plan de réponse et de restauration de leur organisation ?
3. Avec quelle rapidité peuvent-elles restaurer leurs fonctions critiques ou importantes à l'issue d'une panne de grande ampleur ?
4. À quelle fréquence effectuent-elles un audit de risque et entreprennent-elles des actions d'amélioration continue sur leurs fonctions critiques ou importantes ?
5. Sont-elles en mesure de signaler les incidents majeurs à l'autorité compétente ?

COMMENT RUBRIK PEUT VOUS AIDER À VOUS CONFORMER AU RÈGLEMENT DORA

Les 5 piliers du règlement DORA

Technologies de l'information et de la communication (TIC), gestion des risques, signalement des incidents liés aux TIC, résilience opérationnelle et tests, gestion des risques liés aux tiers, partage de renseignements. Rubrik peut aider les organisations à se conformer aux piliers clés suivants du règlement DORA :

1

Gestion des risques liés aux TIC

Les organisations concernées doivent mettre en place un cadre de gouvernance et de contrôle en interne pour assurer une gestion efficace des risques liés aux technologies de l'information et de la communication. Cette gestion concerne aussi bien l'identification des actifs critiques que la réponse aux cyber-risques et la restauration.

Comment Rubrik peut les aider : la plateforme Rubrik a été conçue à la manière d'un système unifié, qui fournit un seul point de contrôle pour gérer et protéger les données, quel que soit leur emplacement de stockage.

2

Signalement des incidents liés aux TIC

Les organisations concernées doivent définir des systèmes capables de prendre en charge la détection, la gestion et le signalement des incidents liés aux TIC.

Comment Rubrik peut les aider : avec sa visibilité globale et son système de gestion de règles, son approche axée sur les API et ses vastes fonctionnalités d'intégration/journalisation, Rubrik peut aider les organisations à classifier et signaler les incidents liés aux technologies de l'information et de la communication.

3

Résilience opérationnelle et tests

Les organisations concernées sont tenues d'entreprendre des tests de résilience opérationnelle numérique.

Comment Rubrik peut les aider : la plateforme Rubrik, intégrée dans un écosystème plus vaste, permet aux organisations d'améliorer leur résilience dans des situations de reprise après sinistre, en incorporant des fonctionnalités de pointe (sauvegarde, restauration et sécurité de base des données au repos) pour favoriser une détection active des menaces qui pèsent sur les données et prévenir les échecs d'audit. Les organisations peuvent également recourir à l'automatisation de règles pour tester et assurer la résilience opérationnelle des capacités et fonctions de leurs données de sauvegarde couvertes par le cadre de gestion des risques liés aux TIC.

4

Gestion des risques liés aux tiers

Les organisations concernées doivent gérer activement les risques associés aux tiers prestataires de services TIC dans le cadre de leur stratégie globale de gestion des risques liés aux TIC.

Comment Rubrik peut les aider : pour adopter une approche plus efficace de la gestion et de l'évaluation des risques liés aux tiers, les clients ont la possibilité d'examiner les données stockées dans la plateforme Rubrik, de manière à identifier les risques concernés par la découverte de données sensibles et par la classification/l'analyse de données. Pour élargir leur compréhension et mieux couvrir les risques liés aux TIC dans le cadre de leur stratégie globale, ils peuvent également exploiter les fonctions de recherche de menaces développées par Rubrik, qui identifient les risques associés à des indicateurs de compromission et à des ransomwares, et signalent immédiatement les éventuelles menaces détectées dans l'écosystème plus large de la plateforme de gestion des risques.

5

Partage de renseignements

Les organisations sont encouragées à adhérer à des communautés d'entités financières de confiance pour échanger des informations et des renseignements sur les cybermenaces, dans le but de renforcer la résilience opérationnelle numérique de l'ensemble du secteur.

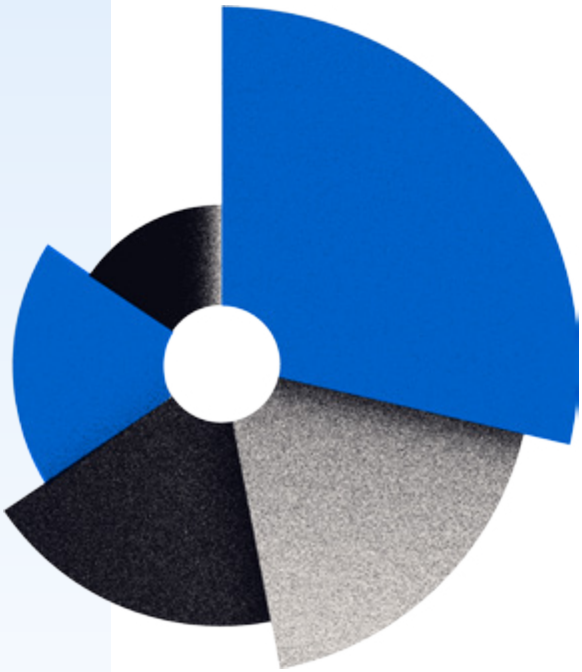
Comment Rubrik peut les aider : grâce à un cadre de visibilité unifié et à une conception largement axée sur les API, Rubrik peut aider les entreprises à honorer leur obligation de partager les informations sur les menaces qui ont été découvertes et surveillées par la plateforme avec des outils et systèmes de signalement tiers, afin de communiquer ces informations (dans la mesure où elles se rapportent à la découverte de ransomwares, à la recherche d'indicateurs de compromission et à la surveillance des menaces) à d'autres entités financières de confiance.

EN SAVOIR PLUS SUR RUBRIK

Rubrik vous aide à renforcer votre résilience opérationnelle en toute simplicité, grâce à une seule plateforme de sécurité des données qui couvre tous vos environnements : sur site, cloud et SaaS. Notre plateforme automatise la gestion des règles et l'application des mesures de sécurité pendant toute la durée du cycle de vie des données. Intégrité et disponibilité des données, surveillance des risques et des menaces, restauration en cas d'attaque… Nous agissons sur tous les fronts pour protéger et préserver vos données. Si l'ensemble de leur organisation est touchée par un sinistre, une violation ou une défaillance, les sociétés de services financiers peuvent se tourner vers Rubrik pour assurer leur résilience opérationnelle et la continuité de leur activité à grande échelle.

Les entreprises européennes qui négligent d'adopter et de respecter les derniers règlements en vigueur en matière de cybersécurité s'exposent à de lourdes conséquences. Qu'il s'agisse de la réglementation sectorielle ou de la législation européenne, les organisations doivent impérativement élaborer un plan de sécurité des données pour se préparer en amont à satisfaire à ces réglementations.

Contactez-nous pour savoir comment Rubrik peut aider les entreprises à s'aligner sur les principaux piliers du règlement DORA et soutenir les institutions financières dans leur démarche d'amélioration de la sécurité des données afin de respecter la réglementation en vigueur.



Lire notre lookbook client

Regarder les Data Security Talks en replay

Rubrik pour les services financiers