HADRIAN

Le Guide Pour se Préparer à la Réglementation sur la Résilience Opérationnelle Numérique (DORA)

Qu'est-ce que la Réglementation sur la Résilience Opérationnelle Numérique ?

Marquant un moment charnière dans la cybersécurité et la norme financière, la Réglementation sur la Résilience Opérationnelle Numérique (DORA) est officiellement entré en vigueur le 16 janvier 2023. Avec une attention pointue, DORA mène la mission d'élever et d'unifier les protocoles de risque à travers le spectre des technologies de l'information et de la communication (TIC) au sein du domaine financier de l'Union européenne. L'objectif principal est d'unifier et de renforcer le cadre de résilience opérationnelle numérique.

DORA établit des critères cohérents pour sécuriser les réseaux et les systèmes d'information des entreprises et entités du secteur financier, ainsi que des prestataires tiers essentiels offrant des services liés aux TIC tels que les plateformes cloud ou les services d'analyse de données. Il construit une structure réglementaire axée sur la résilience opérationnelle numérique, exigeant que toutes les entreprises garantissent leur capacité à supporter, répondre et se remettre de diverses perturbations et menaces liées aux TIC. Ces exigences sont standardisées dans tous les États membres de l'Union européenne, avec pour objectif principal la prévention et la réduction des cybermenaces.

La réponse rapide

Comment les responsables de la sécurité et de la gestion des risques (SRM) peuvent-ils se préparer à la Réglementation sur la Résilience Opérationnelle Numérique de l'UE:

- Déterminez si votre organisation doit répondre aux exigences de DORA
- Concentrez-vous d'abord sur la gestion des risques TIC, les risques liés aux tiers, le partage d'informations, la déclaration d'incidents et les tests de résilience opérationnelle
- Développez un plan complet pour combler les lacunes en matière de conformité

Élever les pratiques de sécurité

L'applicabilité large de DORA suscite des questions de la part d'entités tant à l'intérieur qu'à l'extérieur de l'UE. La résilience exigée par DORA s'étend à divers départements et rôles managériaux, y compris le Chief Information Security Officer (CISO), le Chief Information Officer (CIO) et les équipes de gestion des risques d'entreprise. Des facteurs tels que les objectifs de point de reprise (RPO) et les objectifs de temps de reprise (RTO) pour les accords de niveau de service (SLA) sont mis en lumière.

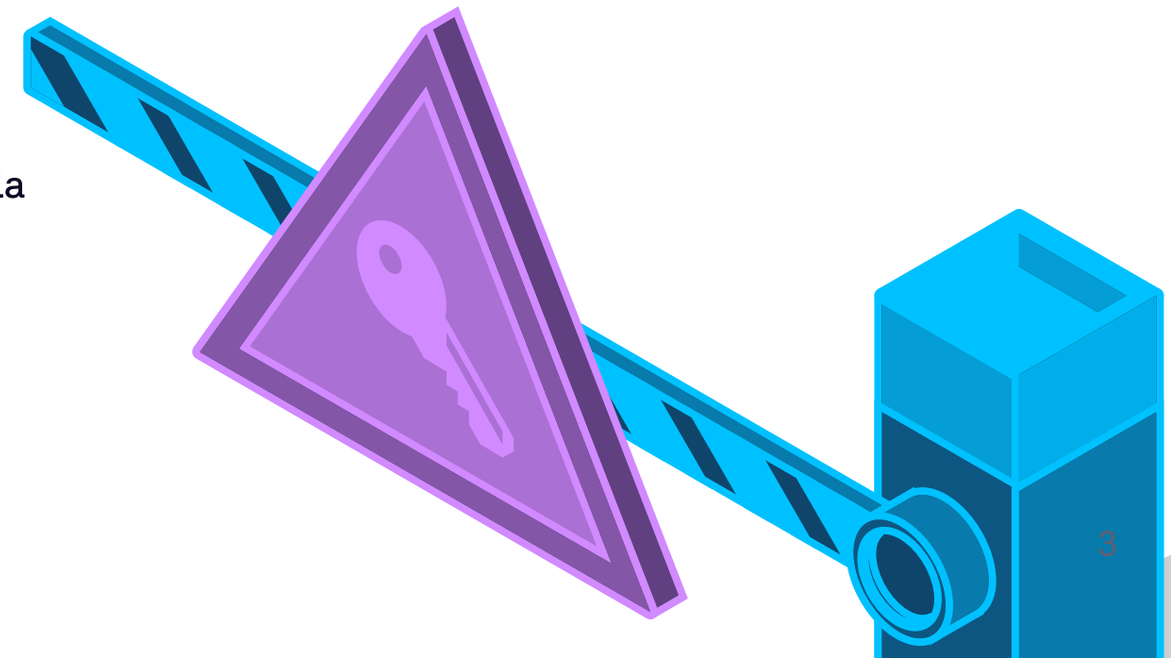
Au cours de la dernière décennie, les Autorités Européennes de Surveillance (AES) ont fourni des orientations sur la gestion des risques TIC, influençant des régulateurs comme la Banque centrale européenne (BCE) et De Nederlandsche Bank (DNB). Maintenant, avec l'entrée en vigueur de DORA, il est temps d'évaluer vos pratiques de gestion des risques TIC. Examinez votre posture actuelle, identifiez les lacunes et alignez-vous sur DORA. Ce n'est pas une simple case à cocher bureaucratique ; c'est une occasion de renforcer les contrôles. Standardisez et automatisez pour une gestion des risques TIC rentable. Préparez-vous aux audits et inspections initiés par DORA.

Pour certains, DORA marque le début d'un parcours de maturité accéléré ; pour d'autres, c'est une occasion d'améliorer les capacités. Dans un monde valorisant la résilience numérique, DORA vous guide. Il ne s'agit pas seulement de conformité, mais de créer un écosystème financier résilient.

Pourquoi la loi sur la résilience opérationnelle numérique change-t-elle la donne ?

2 minutes de lecture

Lire l'article



Qui est concerné et qui ne l'est pas : champ d'application de DORA

Plongez dans l'Article 2 de DORA pour comprendre sa portée

Dans le champ d'application :

- Établissement de crédit
- Établissement de paiement
- Fournisseur de services d'information sur les comptes
- Entreprise d'investissement
- Fournisseur de services d'actifs cryptographiques
- Entreprises d'assurance et de réassurance

...et bien d'autres, totalisant 21 types d'entités. (Voir l'Article 2 pour la liste complète.)

Hors du champ d'application :

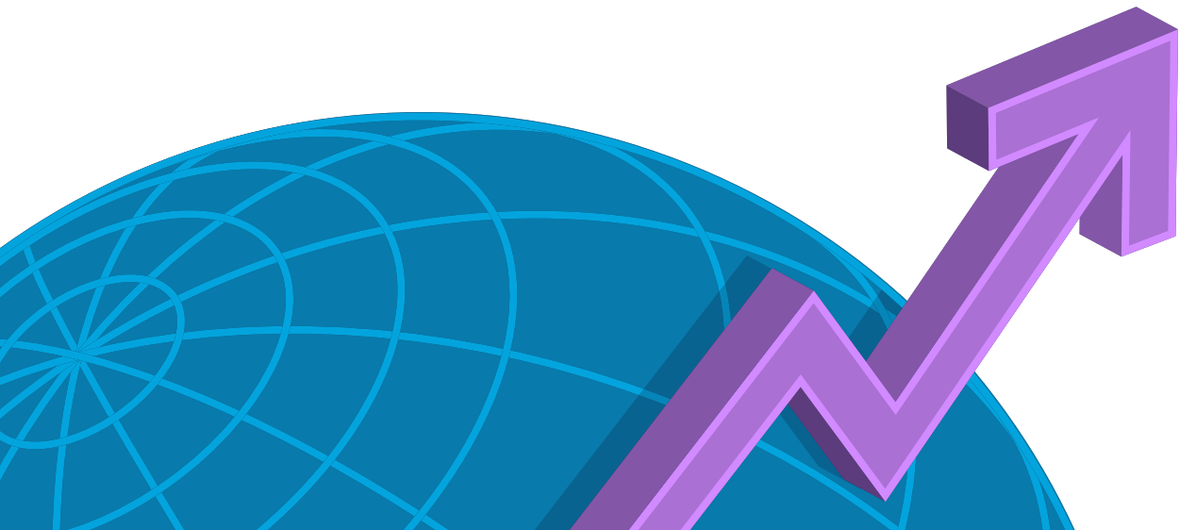
- Gestionnaires de certains fonds d'investissement alternatifs
- Certaines entreprises d'assurance et de réassurance
- Régime de pension de petite taille
- Microentreprises ou petites et moyennes entreprises d'intermédiation d'assurance
- Institutions de chèques postaux

> **Note**
> Les États membres peuvent avoir des exclusions spécifiques. Référez-vous toujours aux directives originales pour des détails précis.

Le rôle des AES dans la résilience du marché

En plongeant dans les 64 articles de DORA, le rôle accru que joueront les Autorités Européennes de Surveillance (AES) dans la supervision des mises en application locales devient essentiel. Les entreprises doivent s'attendre à une supervision renforcée et à des contrôles robustes, y compris des obligations telles que :

- Élaborer un cadre de gestion des risques TIC solide, complet et bien documenté (article 6(1)) qui doit inclure au minimum les stratégies, politiques, procédures, protocoles TIC et outils nécessaires pour protéger toutes les informations et actifs TIC
- Partager des rapports obligatoires sur les incidents majeurs liés aux TIC
- Développer des plans de continuité des activités (PCA) et des plans de reprise après sinistre (PRS) résilients
- Tester les plans de continuité des activités TIC et les plans de réponse et de reprise des TIC au moins une fois par an



Qu'est-ce que les AES ?

Les Autorités Européennes de Surveillance (AES) sont des composants essentiels du Système Européen de Surveillance Financière (SESF) établi en 2011.

Composées d'entités telles que l'Autorité Bancaire Européenne (ABE) à Paris, l'Autorité Européenne des Marchés Financiers (AEMF) à Paris, et l'Autorité Européenne des Assurances et des Pensions Professionnelles (AEAPP) à Francfort, les AES jouent un rôle crucial dans la surveillance microprudentielle au niveau de l'Union Européenne.

Elles ont été proposées par la Commission Européenne en 2009 en réponse à la crise financière de 2007-2008.

Sanctions et implications

Les institutions financières qui ne respectent pas la réglementation peuvent faire face à plusieurs conséquences, notamment :

Amendes administratives

Les infractions graves peuvent entraîner des amendes allant jusqu'à 10 millions d'euros ou 5 % du chiffre d'affaires annuel total, selon le montant le plus élevé.

Mesures correctives

Les autorités de surveillance peuvent obliger les institutions à prendre des mesures correctives pour remédier aux faiblesses de la résilience opérationnelle.

Réprimandes publiques

Les organismes de surveillance peuvent dénoncer publiquement les institutions financières qui ne répondent pas aux exigences de la réglementation.

Retrait d'autorisation

Les manquements répétés à la conformité peuvent entraîner le retrait de l'autorisation de l'institution.

Indemnisation des dommages

Les institutions peuvent être tenues d'indemniser les clients ou les tiers pour les dommages résultant de la non-conformité.

Identifier les obstacles à l'horizon de DORA

La loi approuvée accorde aux entreprises jusqu'en 2025 pour la mise en œuvre de DORA. Pendant les deux années de préparation (2023 et 2024), alignez la gouvernance avec les piliers de DORA. Effectuez une évaluation des écarts pour une stratégie de résilience numérique. À partir de 2025, des rapports obligatoires, des tests et des évaluations annuelles seront requis. Les tests d'intrusion et la certification par les AES deviendront obligatoires d'ici fin 2025.

24 septembre 2020 : Publication de la proposition de DORA par la Commission Européenne

23 juillet 2022 : Accord provisoire sur DORA atteint

10 novembre 2022 : Ratification de la réglementation DORA par le Parlement européen

Q4 2022 (Nov/Dec) : Publication de DORA au Journal officiel de l'UE

17 janvier 2023 : Jour d'adoption
DORA entre en vigueur

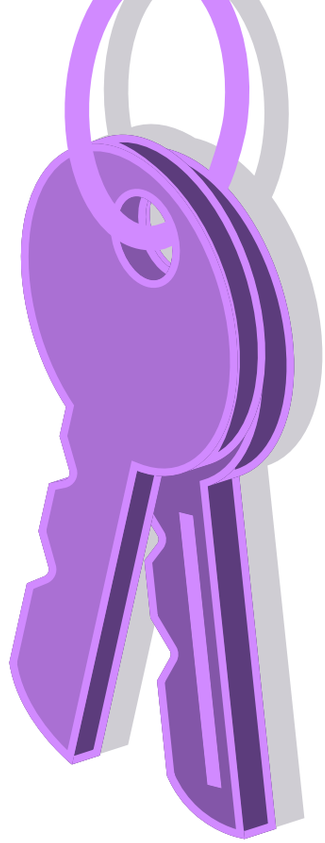
Q3 2023 - Q4 2024: Soumission des normes techniques par les AES

17 janvier 2025 : Applicabilité de DORA
Conformité complète avec DORA et ses normes techniques requise

Attention !

DORA prévaut sur des textes qui se chevauchent comme la directive NIS ou les lignes directrices des AES, en faisant la référence principale pour les contrôles de conformité réglementaire afin d'éviter les lacunes lorsqu'il deviendra effectif en 2025.

Naviguer dans DORA - Composants clés



Le texte légal de DORA, défini par l'Union européenne, délimite les dispositions de la législation et cible cinq piliers fondamentaux de la cybersécurité pour amélioration.

Des exigences en matière de cybersécurité à la gestion des risques, chaque élément joue un rôle crucial dans la définition de l'avenir de la cybersécurité financière.

5 Piliers Fondamentaux

Gestion des risques

Établir des preuves de gouvernance interne et des cadres de contrôle qui assurent la gestion efficace de tous les risques TIC.

Risque TIC des tiers

Gérer efficacement le risque TIC des tiers, y compris les risques découlant de la contractualisation de prestataires de services TIC tiers.

Partage d'informations

Faciliter l'échange d'informations et d'intelligence sur les cybermenaces entre les entités financières.

Rapport d'incidents liés aux TIC

Développer la capacité de signaler les incidents majeurs aux autorités compétentes et d'informer les utilisateurs de services et les clients.

Tests de résilience opérationnelle

Mettre en œuvre, maintenir et réviser des programmes de tests de résilience opérationnelle numérique.

Exigences pour devenir conforme à DORA

L'introduction de la Réglementation sur la Résilience Opérationnelle Numérique marque un moment charnière pour le secteur financier, déplaçant les institutions de la gestion principalement des risques opérationnels par l'allocation de capital à l'adhésion à des règles pour des capacités complètes de protection, détection, confinement, récupération et réparation des incidents liés aux TIC. Cependant, ce changement réglementaire pose des défis de conformité pour les organisations ciblées :

Applicabilité étendue : La portée large de DORA couvre diverses institutions financières et les fournisseurs de services tiers critiques (CTPS), rendant la délimitation précise de son applicabilité difficile.

Exigences complexes : Les mandats complexes de DORA nécessitent une compréhension détaillée et une planification stratégique, ajoutant de la complexité à la fois à la compréhension et à l'exécution.

Pression financière : La conformité à DORA entraîne des implications financières palpables alors que les institutions investissent dans le renforcement des systèmes TIC et la restructuration des processus.

Changement culturel : La résilience opérationnelle nécessite un changement de mentalité, présentant un défi important pour passer des opérations conventionnelles à une approche axée sur la résilience.

Renforcer
Les règles de gestion des risques TIC

Étendre
La régulation TIC à toutes les parties

Harmoniser
Le rapport et le partage d'informations

Standardiser
Les tests et la surveillance de la résilience

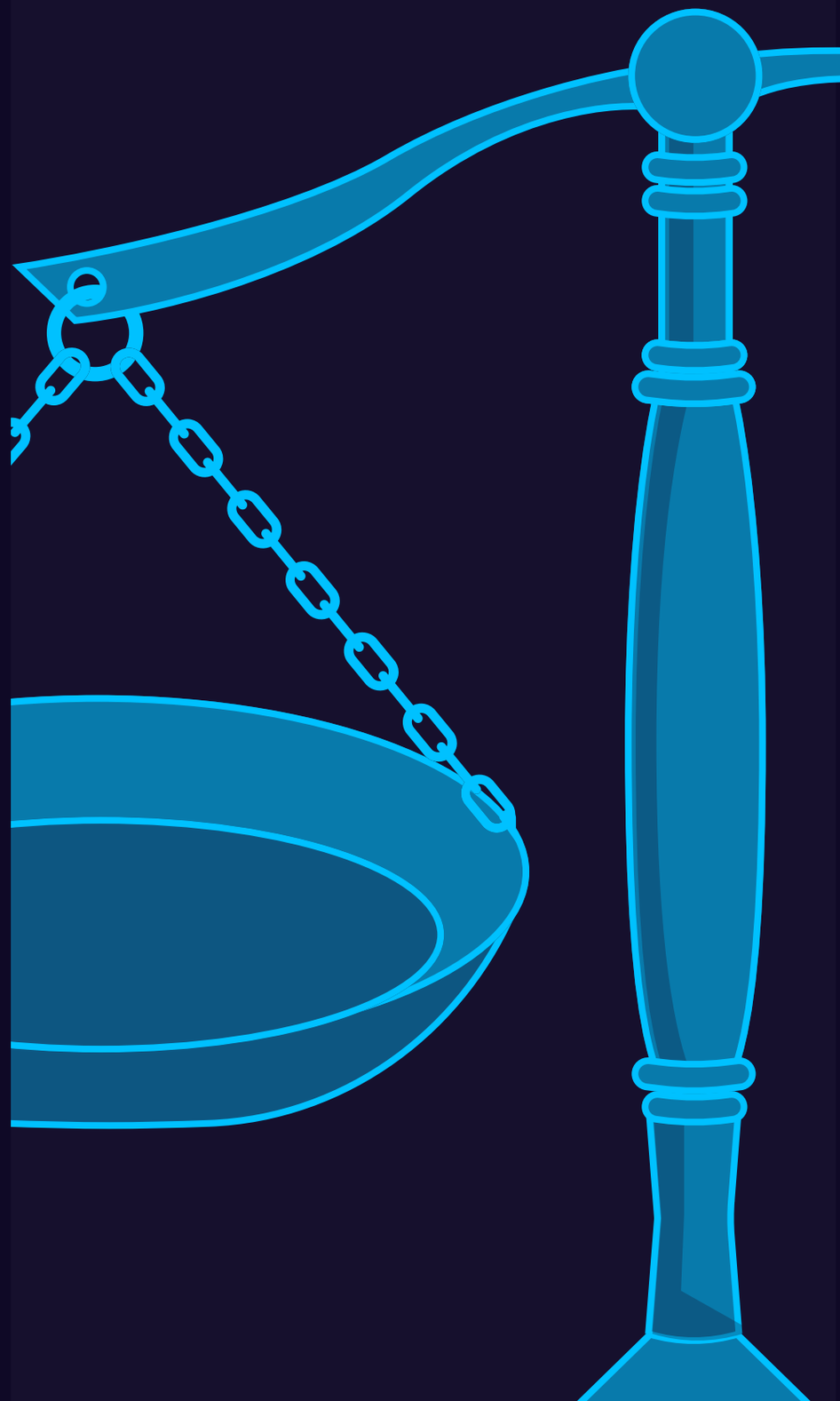
Exigences pour devenir conforme à DORA (Suite)

Limitations des ressources : Les contraintes de ressources, y compris les limitations budgétaires, les déficits de compétences et les pénuries de personnel, peuvent entraver la mise en œuvre à grande échelle de DORA, en particulier pour les petites entités.

Défis de collaboration : Les efforts de coopération, en particulier avec des tiers, sont souvent nécessaires sous DORA. Cependant, obtenir une coopération cohérente, notamment de la part des entités en dehors de la juridiction de DORA, peut être ardu.

Paysage réglementaire dynamique : Le paysage réglementaire en constante évolution dans le secteur financier pose un défi persistant pour maintenir une conformité continue avec DORA.

Malgré ces obstacles, embrasser la conformité à DORA promet de préparer le terrain pour un écosystème financier plus résilient, sécurisé et fiable dans l'UE.



Adapter à la conformité DORA

Les AES anticipent une nouvelle ère de rapports et de communication des institutions financières, fournissant des informations précieuses pour améliorer l'intelligence cybernétique de l'UE. Les AES affineront les RTS pendant cette période, nécessitant que les entreprises alignent leur gouvernance et leurs pratiques sur les piliers de résilience de DORA.

Pour concrétiser une stratégie de résilience numérique, les entreprises peuvent effectuer une évaluation initiale des écarts, en analysant leur niveau de maturité. Cela implique d'évaluer la conformité aux directives existantes (AES, NIS, CROE) et aux normes de gestion des risques informatiques (ITIL, COBIT, NIST CSF, ISO). En identifiant les écarts, une feuille de route peut prioriser les efforts pour répondre aux exigences de DORA. Pendant cette phase, les régulateurs définiront de nouveaux RTS et ITS, nécessitant une stratégie agile.

Changement majeur : Tests de résilience opérationnelle numérique. Basé sur les tests de pénétration dirigés par les menaces (proposition de l'article 23), ce changement comprend deux catégories :

Tests internes annuels obligatoires	Tests avancés (tous les trois ans)
Applicables à toutes les entités du secteur financier	Applicables aux entreprises répondant aux critères définis par les régulateurs
Nécessitent la soumission des résultats aux AES dans un format spécifié	Réalisés par une entité externe, avec les AES délivrant des certificats de conformité
	La non-conformité pourrait entraîner une éventuelle suspension des activités de l'entreprise.

Naviguer vers la Conformité DORA

Préparez-vous à l'entrée en vigueur complète de DORA en janvier 2025 en initiant des projets, évaluant les besoins budgétaires et mettant en œuvre des initiatives à l'échelle de l'organisation. Renforcez la résilience et atteignez la conformité DORA grâce aux étapes suivantes :

Identification des Risques par Cartographie du Réseau:

- Initiez l'identification des risques en cartographiant les dépendances des applications à travers toute l'infrastructure.
- Utilisez des solutions de sécurité comme Hadrian pour faciliter ce processus de cartographie, révélant les processus critiques et non critiques, et identifiant les dépendances vis-à-vis des tiers.
- Adressez promptement les risques précédemment inconnus dès leur découverte.

Amélioration des Capacités de Détection:

- Utilisez une meilleure compréhension de votre environnement pour renforcer les capacités de détection.

Containment Proactif des Violations

- Reconnaissez le containment des violations comme un aspect crucial de la résilience selon DORA.
- Implémentez des technologies telles que la micro-segmentation (Segmentation Zero Trust) pour séparer le réseau en zones, permettant une communication contrôlée entre les charges de travail et les appareils.
- Isoler proactivement les actifs de grande valeur ou contenir réactivement les systèmes compromis lors d'une attaque active pour arrêter la propagation d'une violation.

Comprendre le Cadre DORA

DORA va au-delà d'un simple mandat de conformité ; il représente une opportunité de préparer l'avenir de votre entreprise, d'améliorer les pratiques de cybersécurité et de préparer votre organisation aux défis et opportunités à venir dans le paysage financier numérique. Voici comment vous pouvez le faire :

Gérer les risques par une sécurité offensive proactive

Établir des preuves de gouvernance interne et de cadres de contrôle qui assurent la gestion efficace de tous les risques liés aux TIC.

Comment Hadrian peut aider

Le Continuous Automated Red Teaming (CART) de Hadrian propose des attaques simulées continues et automatisées sur votre système pour identifier les vulnérabilités et les faiblesses. Grâce à cette approche continue, nous pouvons détecter les nouvelles menaces et vulnérabilités au fur et à mesure de leur apparition.

Gérer efficacement les risques liés aux tiers

En ce qui concerne les tiers, les accords légaux appropriés pour protéger la cybersécurité sont essentiels. Mais au final, vous devrez surveiller les vulnérabilités que vos tiers apportent à votre surface d'attaque. C'est une tâche difficile, pratiquement impossible à surveiller manuellement.

Comment Hadrian peut aider

La plateforme de sécurité intelligente de Hadrian évalue l'ensemble de votre surface d'attaque, identifie les vulnérabilités provenant de sources tierces, évalue la probabilité et l'impact d'exploitation, suggère des mesures correctives et valide la sécurité après la remédiation.

Préparez-vous à un reporting d'incidents rapide et précis

DORA vise à renforcer la cybersécurité dans toute l'Union européenne grâce à un reporting d'incident rapide et efficace. Le partage d'informations contribue à accroître la sensibilisation aux menaces cybernétiques et aide à contenir les incidents liés aux TIC, selon DORA.

Comment Hadrian peut aider

Les rapports de conformité traditionnels manquent de mises à jour en temps réel, ce qui peut entraîner une prise de conscience retardée des problèmes. Hadrian fournit des rapports précis et clairs, répondant aux exigences de DORA pour les parties prenantes externes et assurant une communication confiante avec les cadres et les membres du conseil d'administration.

À propos de Hadrian

La sécurité défensive doit être validée par la sécurité offensive. Hadrian adopte le point de vue des hackers, révélant les cibles et les méthodes qui pourraient être utilisées lors d'une violation de données réelle. Les tests continus et complets de Hadrian découvrent et valident les risques de manière entièrement autonome.

La plateforme de Hadrian combine la découverte de la surface d'attaque, les tests d'intrusion automatisés et les technologies de gestion de l'exposition aux menaces dans une plateforme basée sur le cloud et sans agent. Cette technologie de pointe est constamment mise à jour et améliorée par l'équipe interne de hackers de Hadrian.

> ‘Ce qui est passionnant dans ce que fait Hadrian, c'est qu'ils ont résolu un casse-tête apparemment impossible : trouver des failles dans un réseau complexe avec un niveau de détail proche de celui d'un humain, à grande échelle, depuis l'extérieur et de manière continue. Ce qui prend normalement à une équipe dédiée d'ingénieurs en sécurité quelques semaines pour un système, ils peuvent le faire en quelques minutes pour des milliers de systèmes.’
>
> **Tiago Teles - Responsable de la sécurité, ABN AMRO**

Approuvé par

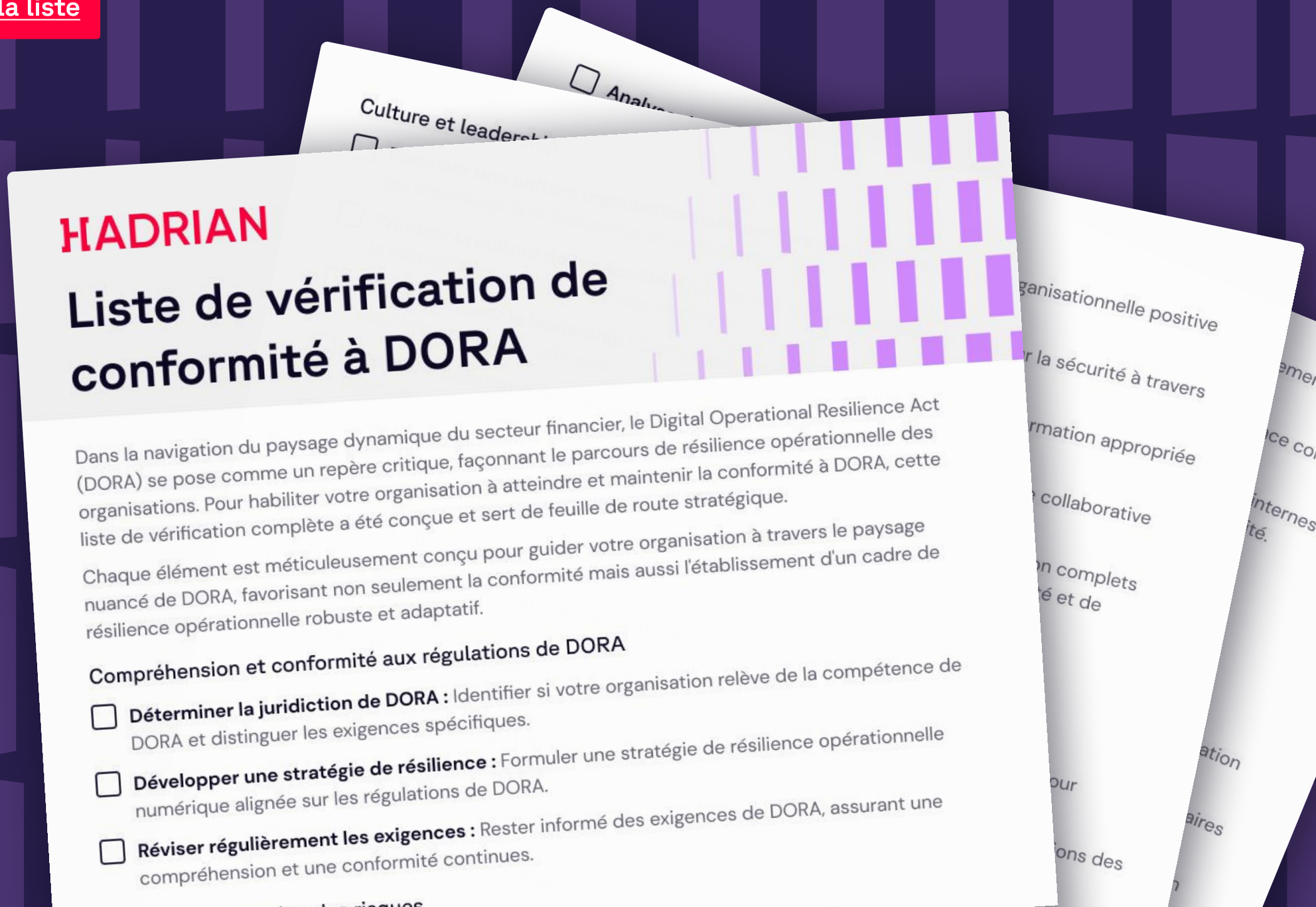
ABN·AMRO · SHV ENERGY · macmillan education · CTC GLOBAL

WeatherTech · LEROY MERLIN · LOTTOMATICA · CA

RITUALS... · BIOLANDES · nedap · Van Oord

Liste de vérification de conformité à DORA

Télécharger la liste



Termes essentiels de DORA à connaître

Fournisseur de services d'information sur les comptes : Un fournisseur de services d'information sur les comptes tel que défini à l'article 33(1) de la Directive (UE) 2015/2366 ;

Fournisseur de services d'actifs numériques : Un fournisseur de services d'actifs numériques tel que défini dans la disposition pertinente du Règlement sur les marchés des actifs numériques ;

Cyberattaque : Un incident malveillant lié aux TIC causé par une tentative perpétrée par tout acteur de menace visant à détruire, exposer, altérer, désactiver, voler, ou accéder de manière non autorisée à, ou faire un usage non autorisé d'un actif ;

Résilience opérationnelle numérique : La capacité d'une entité financière à construire, garantir et évaluer son intégrité opérationnelle et sa fiabilité en assurant, directement ou indirectement par l'intermédiaire de services fournis par des fournisseurs de services tiers en TIC, l'ensemble complet des capacités liées aux TIC nécessaires pour garantir la sécurité des réseaux et des systèmes d'information utilisés par une entité financière, et qui soutiennent la fourniture continue de services financiers et leur qualité, y compris en cas de perturbations ;

Autorités de supervision européennes : Les organismes de régulation établis dans le cadre du Système européen de supervision financière afin d'assurer la stabilité financière ;

Actif en TIC : Un actif logiciel ou matériel dans les réseaux et systèmes d'information utilisés par l'entité financière ;

Risque en TIC : Toute circonstance raisonnablement identifiable en relation avec l'utilisation des réseaux et systèmes d'information qui, si elle se matérialise, pourrait compromettre la sécurité des réseaux et systèmes d'information, de tout outil ou processus technologique dépendant, des opérations et processus, ou de la fourniture de services en produisant des effets néfastes dans l'environnement numérique ou physique ;

Incident lié aux TIC : Un événement isolé ou une série d'événements liés non planifiés par l'entité financière qui compromettent la sécurité des réseaux et systèmes d'information, et ont un impact négatif sur la disponibilité, l'authenticité, l'intégrité ou la confidentialité des données, ou sur les services fournis par l'entité financière ;

Entreprise d'assurance : Une entreprise d'assurance telle que définie à l'article 13, point (1), de la Directive 2009/138/CE ;

Normes techniques d'exécution (ITS) : Un acte d'exécution technique permettant l'application uniforme de certaines dispositions de l'acte législatif de base ;

Gestionnaire de fonds d'investissement alternatifs : Un gestionnaire de fonds d'investissement alternatifs tel que défini à l'article 4(1), point (b), de la Directive 2011/61/UE ;

Entreprise de taille moyenne : Une entité financière qui n'est pas une petite entreprise, emploie moins de 250 personnes et a un chiffre d'affaires annuel qui ne dépasse pas 50 millions d'euros et/ou un bilan annuel qui ne dépasse pas 43 millions d'euros ;

Termes essentiels de DORA à connaître (Suite)

Microentreprise : Une entité financière, autre qu'un marché, un contrepartie centrale, un référentiel de transactions ou un dépositaire central de titres, qui emploie moins de 10 personnes et dont le chiffre d'affaires annuel et/ou le total du bilan annuel n'excède pas 2 millions d'euros ;

Réseau et système d'information : Réseau et système d'information tel que défini dans le règlement 2022/2555 ;

Établissement de paiement : Un établissement de paiement tel que défini à l'article 4, point (4), de la Directive (UE) 2015/2366 ;

Normes techniques réglementaires (RTS) : Un acte délégué technique préparé par une Autorité de surveillance européenne ;

Entreprise de réassurance : Une entreprise de réassurance telle que définie à l'article 13, point (4), de la Directive 2009/138/CE ;

Petite entreprise : Une entité financière qui emploie 10 personnes ou plus, mais moins de 50 personnes, et dont le chiffre d'affaires annuel et/ou le total du bilan annuel dépasse 2 millions d'euros, mais n'excède pas 10 millions d'euros ;

Test d'intrusion basé sur les menaces : Un cadre qui imite les tactiques, techniques et procédures des acteurs de menace réels perçus comme représentant une véritable menace cybernétique, qui fournit un test contrôlé, personnalisé et orienté par le renseignement (équipe rouge) des systèmes de production en direct critiques de l'entité financière.