HADRIAN

Liste de vérification de conformité à DORA

Dans la navigation du paysage dynamique du secteur financier, le Digital Operational Resilience Act (DORA) se pose comme un repère critique, façonnant le parcours de résilience opérationnelle des organisations. Pour habiliter votre organisation à atteindre et maintenir la conformité à DORA, cette liste de vérification complète a été conçue et sert de feuille de route stratégique.

Chaque élément est méticuleusement conçu pour guider votre organisation à travers le paysage nuancé de DORA, favorisant non seulement la conformité mais aussi l'établissement d'un cadre de résilience opérationnelle robuste et adaptatif.

Compréhension et conformité aux régulations de DORA

- [ ] **Déterminer la juridiction de DORA :** Identifier si votre organisation relève de la compétence de DORA et distinguer les exigences spécifiques.
- [ ] **Développer une stratégie de résilience :** Formuler une stratégie de résilience opérationnelle numérique alignée sur les régulations de DORA.
- [ ] **Réviser régulièrement les exigences :** Rester informé des exigences de DORA, assurant une compréhension et une conformité continues.

Évaluation et gestion des risques

- [ ] **Renforcer la sécurité de l'information :** Renforcer les mesures de sécurité de l'information, incluant les contrôles d'accès, le chiffrement, la programmation sécurisée et la protection des données.
- [ ] **Conduire une évaluation des risques :** Évaluer les risques potentiels et les vulnérabilités dans vos systèmes ICT, en abordant les menaces internes et externes.
- [ ] **Gérer le risque des tiers :** Évaluer les fournisseurs tiers pour leur résilience et leur sécurité, conformément aux exigences de DORA.
- [ ] **Identifier et sécuriser les actifs ICT :** Mettre en œuvre des mesures pour identifier et sécuriser les actifs ICT selon les régulations de DORA.
- [ ] **Utiliser des solutions automatisées :** Déployer des solutions automatisées et de détection des menaces pour une identification efficace des risques.
- [ ] **Prioriser les actions de remédiation :** Mettre l'accent sur les actions de remédiation et préparer des preuves de conformité.
- [ ] **Surveiller les risques externes :** Surveiller les sources externes pour identifier les risques potentiels et partager des renseignements pour renforcer la résilience.
- [ ] **Créer un cadre de gestion des risques ICT :** Établir un cadre de gestion des risques ICT et mener des tests de résilience opérationnelle numérique.

Culture et leadership

- [ ] **Favoriser une culture organisationnelle positive :** Assurer une culture organisationnelle positive qui encourage la collaboration et la résilience.
- [ ] **Prioriser la culture de la sécurité :** Cultiver une culture d'entreprise axée sur la sécurité à travers la formation et l'engagement des employés.
- [ ] **Responsabiliser le leadership :** Donner aux dirigeants organisationnels une formation appropriée pour une conformité efficace.
- [ ] **Approche holistique de la conformité :** Impliquer plusieurs équipes de manière collaborative pour une approche holistique de la conformité.
- [ ] **Formation et sensibilisation des employés :** Fournir des programmes de formation complets pour éduquer les employés sur les meilleures pratiques en matière de cybersécurité et de déclaration d'incidents.

Processus et automatisation

- [ ] **Mettre en œuvre CI/CD et tests automatisés :** Appliquer l'intégration continue (CI), le déploiement continu (CD) et les tests automatisés pour des processus optimisés.
- [ ] **Plan de réponse aux incidents :** Développer un plan détaillé de réponse aux incidents pour détecter, répondre et récupérer des incidents de sécurité.
- [ ] **Documentation et enregistrements :** Maintenir des enregistrements détaillés des évaluations des risques, des plans de réponse aux incidents et des mesures de conformité.
- [ ] **Tests de pénétration :** Effectuer régulièrement des tests de pénétration en utilisant des cadres comme TIBER-EU.
- [ ] **Détection automatisée des menaces :** Automatiser la détection des menaces en utilisant des outils tels que les EDR, XDR, scanners et SIEM.

Architecture, conception et gestion des tiers

- [ ] **Concevoir pour la scalabilité et la résilience :** Concevoir des systèmes pour la scalabilité, la résilience et la maintenabilité.
- [ ] **Architecture de microservices :** Mettre en œuvre une architecture de microservices et la conteneurisation pour des opérations efficaces.
- [ ] **Considérations pour les fournisseurs tiers :** Examiner les politiques sur les tiers ICT (CTPS) et tenir compte des régulations lors de l'engagement des fournisseurs de services tiers.
- [ ] **Utiliser des programmes de formation :** Utiliser des outils comme le programme de formation de CybeReady pour permettre aux développeurs de développer des applications sécurisées.

Suivi, mesure et amélioration continue

- [ ] **Établir des indicateurs clés de performance et un suivi en temps réel :** Établir des indicateurs clés de performance (ICP) et mettre en place un suivi en temps réel.
- [ ] **Réviser régulièrement les stratégies de résilience :** Examiner et mettre à jour périodiquement les stratégies et les politiques de résilience.

- [ ] **Analyser les incidents passés :** Analyser les incidents passés, intégrer les enseignements tirés et apporter des améliorations.
- [ ] **Surveillance et évaluation continues :** Mettre en œuvre des processus de surveillance continue afin de détecter les nouveaux risques et vulnérabilités et d'y répondre rapidement.
- [ ] **Audits et évaluations internes :** Réaliser régulièrement des audits et des évaluations internes afin d'identifier les domaines à améliorer et de combler les lacunes en matière de conformité.

Sécurité et conformité légale

- [ ] **Intégrer les pratiques de sécurité :** Intégrer les pratiques de sécurité dans le cycle de développement avec une approche DevSecOps.
- [ ] **Effectuer des audits de sécurité :** Effectuer régulièrement des audits de sécurité et des évaluations de la vulnérabilité, afin de garantir la confidentialité des données.
- [ ] **Mettre en place un SGSI :** Mettre en place un système de gestion de la sécurité de l'information (SGSI) conforme aux normes internationales telles que la norme ISO 27001.
- [ ] **Respecter les normes juridiques :** Assurer la conformité avec les normes légales, réglementaires et sectorielles, y compris le GDPR.
- [ ] **S'engager avec les régulateurs :** Restez informé des mises à jour réglementaires et engagez un dialogue ouvert avec les autorités compétentes pour comprendre la conformité.

Comment Hadrian peut aider

En continu

Le Continuous Automated Red Teaming (CART) d'Hadrian permet de simuler des attaques permanentes et automatisées sur votre système afin d'en identifier les vulnérabilités et les faiblesses.

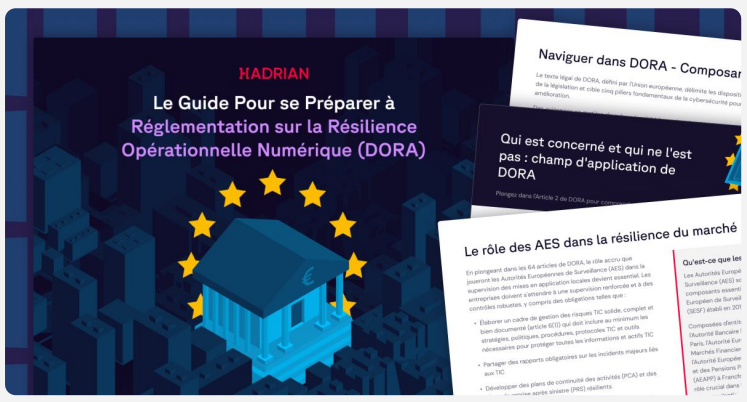
Comme il s'agit d'un processus continu, nous pouvons identifier les nouvelles menaces et vulnérabilités au fur et à mesure qu'elles apparaissent.

Autonomes

La plateforme de sécurité d'Hadrian, alimentée par une intelligence avancée, évalue l'ensemble de votre surface d'attaque, en découvrant les vulnérabilités de tiers. Elle évalue la probabilité et l'impact de l'exploitation dans l'ensemble de votre organisation, en proposant des recommandations de remédiation et en assurant une sécurité continue après la remédiation.

Complet

Les rapports de conformité traditionnels manquent de mises à jour en temps réel, laissant les entreprises dans l'ignorance des problèmes jusqu'à ce qu'il soit trop tard. Hadrian propose des rapports précis et clairs pour les parties prenantes externes, répondant aux exigences de la loi DORA. Partageables facilement, ils tiennent tout le monde informé de la conformité à la loi DORA.



Lire Le Guide Pour se Préparer à la Réglementation sur la Résilience Opérationnelle Numérique

Télécharger le Guide

Ou scannez le code QR