5 exigences clés du règlement DORA

et comment l'identité simplifie la conformité

La rapide transition vers le numérique a stimulé l'innovation dans le secteur des services financiers en Europe, mais a également exposé les entreprises aux cybermenaces.
En réaction, l'Union européenne a introduit le règlement sur la résilience opérationnelle numérique (DORA, Digital Operational Resilience Act) qui fournit une feuille de route claire pour renforcer la cybersécurité dans l'ensemble du secteur.

Une approche stratégique en matière d'identité numérique est essentielle à la conformité.

1. Un framework pour gérer les risques liés à l'informatique

Le règlement DORA impose aux entreprises de recenser leurs systèmes informatiques, d'identifier et de surveiller en permanence les fonctions et ressources informatiques, et d'implémenter des mécanismes robustes pour détecter les anomalies et prévenir toute défaillance système. À cela viennent s'ajouter une politique de sauvegarde et une stratégie de reprise destinées à limiter autant que possible les interruptions en cas d'incident.

Rôle clé de l'identité

Une solution d'identité moderne incluant à la fois les collaborateurs et les clients est un composant essentiel du framework de gestion des risques liés à l'informatique.
Elle constitue un outil complet de surveillance et de contrôle de l'accès au niveau de votre entreprise, mais aussi des parties externes qui interagissent avec vos services.

Siège Social
27 rue de la Télématique
42000 Saint-Etienne

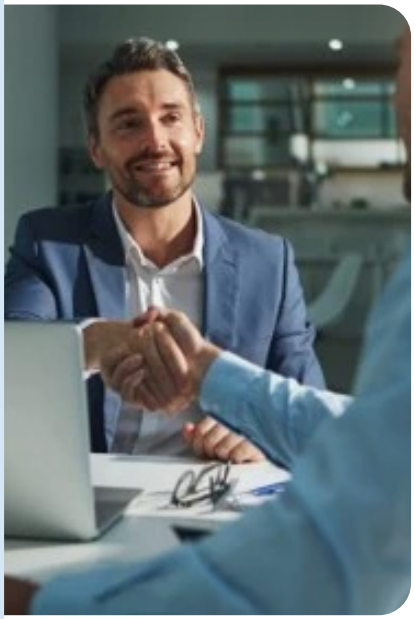
Nos implantations en France : Ile de France, Auvergne Rhône-Alpes, Occitanie

Trouvez votre agence sur
https://www.value-info.fr/

DEVIS & INFORMATIONS
09 70 24 01 80
contact@value-info.fr

2. Notification des incidents liés à l'informatique

La journalisation et la notification rapides des incidents de sécurité liés à l'informatique constituent une exigence clé du règlement DORA. Celles-ci doivent s'inscrire dans le cadre d'une procédure complète de gestion des incidents, capable de détecter, de gérer et de notifier les incidents liés à l'informatique, mais aussi d'identifier et d'éliminer les causes profondes afin d'éviter toute récurrence.



Rôle clé de l'identité

Il est essentiel de disposer d'une visibilité complète sur les activités système, avec des informations sur l'utilisateur à l'origine de l'action, ainsi que l'emplacement et le moment de cette dernière.
Une plateforme d'identité procure les fonctions de surveillance et d'analyse numérique indispensables à la notification précise et dans les délais prévus aux autorités réglementaires.

3. Test de la résilience opérationnelle numérique

Les entités doivent tester régulièrement leurs systèmes informatiques pour évaluer leur préparation aux incidents, mettre en évidence toute vulnérabilité ou lacune, et appliquer rapidement des mesures correctives. Ces tests du programme, à exécuter sur base annuelle, doivent être confiés à une entité indépendante pour les systèmes et applications informatiques critiques.

Rôle clé de l'identité

Une plateforme d'identité telle que celle d'Okta possède un double rôle : elle permet de détecter les problèmes liés aux comptes à privilèges excessifs, tout en se soumettant elle-même aux tests requis. Vous pouvez ainsi valider diverses procédures, le provisioning de l'accès et les autorisations pour vérifier si vos processus et contrôles fonctionnent de manière optimale.

17 janvier 2025

Entrée en application du règlement DORA

Siège Social
27 rue de la Télématique
42000 Saint-Etienne

Nos implantations en France : Ile de France, Auvergne Rhône-Alpes, Occitanie

Trouvez votre agence sur https://www.value-info.fr/

DEVIS & INFORMATIONS
09 70 24 01 80
contact@value-info.fr

4. Risques liés aux tiers prestataires de services informatiques

DORA ne concerne pas uniquement les entités financières, mais aussi leurs prestataires de services informatiques. Son respect impose donc une approche active de gestion des risques posés par les tiers, l'entreprise assumant l'entière responsabilité de la conformité à toutes les obligations réglementaires et des services financiers. De même, il est conseillé d'éviter de concentrer toutes les fonctions auprès d'un même prestataire.

Rôle clé de l'identité

Dans un monde où les chaînes logistiques exposent souvent les entreprises aux risques et autres vulnérabilités, l'identité joue un rôle crucial dans la définition des droits d'accès et dans l'extension de la visibilité au-delà de l'entreprise, ce qui permet à celle-ci de rester attentive aux défis de sécurité potentiels posés par leurs prestataires.

2% du chiffre d'affaire annuel

Amende en cas de non-conformité au règlement DORA

×2

Les cyberattaques visant les prestataires de services financiers en Europe ont plus que doublé entre le 2e trimestre 2022 et le 2e trimestre 2023.

Source : Akamai, State of the Internet

5. Partage d'informations

Pour réaliser l'objectif de résilience opérationnelle à l'échelle de tout le secteur, les institutions financières sont encouragées à partager des informations sur les cybermenaces, par exemple des données sur les indicateurs de compromission ou les tactiques et techniques des cybercriminels. Toute information partagée doit être sécurisée dans le respect des directives en matière de confidentialité, de protection des données à caractère personnel et de politique de concurrence.

Rôle clé de l'identité

En surveillant continuellement les données, les identités et les autorisations, une plateforme d'identité fournit de précieuses informations sur les menaces émergentes. Des alertes automatiques sur les comportements anormaux et des processus d'identité efficaces renforcent la protection et le partage responsable des informations critiques, ce qui contribue à une meilleure collaboration et à une sécurité renforcée de tout l'écosystème financier.

Pour en savoir plus sur DORA et sur nos services, contactez-nous au 09 70 24 01 80 ou par email contact@value-info.fr