



Services DORA

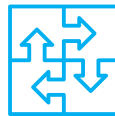
DORA s'applique-t-il à votre organisation ? Alors vous êtes tenu de vous conformer à ce règlement européen dès janvier 2025. Cela demandera des efforts. Nous pouvons vous accompagner — depuis le début de votre démarche de conformité jusqu'à la mise en conformité complète avec DORA.

Ces services DORA vous offrent :



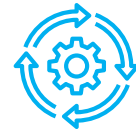
Aperçu des lacunes

Vous obtenez un aperçu de vos contrôles de sécurité actuels et des lacunes éventuelles par rapport aux exigences DORA.



Une feuille de route claire

Vous savez quelles mesures vous devez encore prendre et vous recevez une feuille de route claire pour vous améliorer.



Aide à la mise en oeuvre

Vous bénéficiez de l'aide d'experts pour mettre en oeuvre les mesures nécessaires afin d'assurer une conformité totale avec la directive DORA.

Pourquoi choisir nos services DORA ?

Pour renforcer la résilience numérique de son secteur financier, l'UE a adopté le **Digital Operational Resilience Act (DORA)**. Ce règlement s'applique à toutes les institutions financières européennes, des établissements de crédit et de paiement aux fonds de pension, sociétés d'investissement et compagnies d'assurance. Si DORA s'applique à votre organisation, vous devez répondre à cinq exigences fondamentales.

1. Mettre en place un cadre de gestion des risques et l'améliorer de manière continue
2. Réaliser régulièrement des tests et audits
3. Surveiller les prestataires de services TIC tiers
4. Déclarer les incidents graves aux autorités
5. Partager les informations pertinentes avec le secteur

Nous pouvons vous aider à vous préparer à la conformité avec ces exigences fondamentales.

Quels sont les services DORA que nous proposons ?



Formation DORA pour les conseils d'administration



La **formation DORA pour les conseils d'administration** permet à vos dirigeants de prendre des décisions éclairées concernant DORA. C'est essentiel, car DORA rend explicitement le conseil d'administration et la direction générale responsables de la conformité au règlement. Vous bénéficierez d'analyses juridiques pertinentes de notre partenaire **De Clercq Lawyers and Notary**. À l'issue de cette formation d'une journée :



Votre conseil d'administration disposera des connaissances nécessaires pour évaluer les mesures à mettre en place afin de protéger votre organisation contre les cybermenaces.



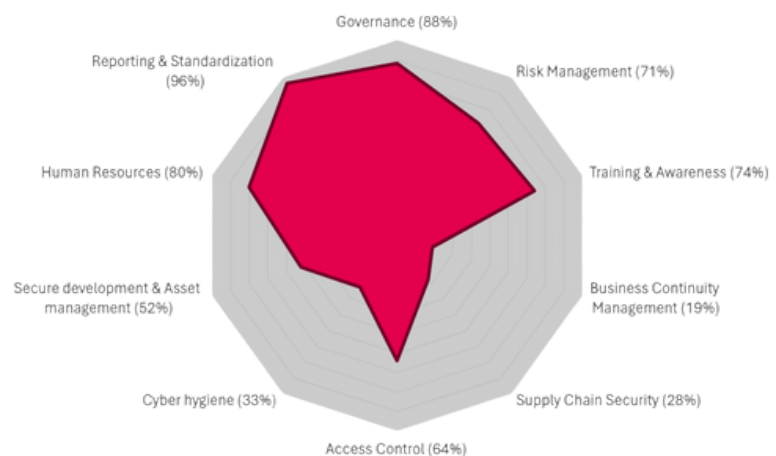
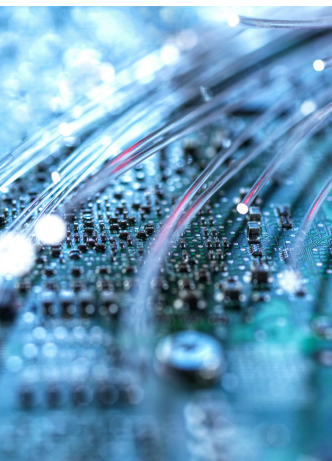
Vous répondrez ainsi aux exigences de formation des conseils d'administration prévues par DORA.



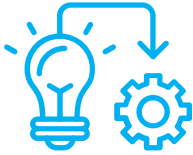
Évaluation des écarts DORA (Gap Assessment)

Vous pouvez également réaliser une **évaluation des écarts DORA (Gap Assessment)**. Quel est le niveau de maturité en cybersécurité de votre organisation ? Quels écarts subsistent en matière de conformité à DORA et quelles étapes sont nécessaires pour les combler ?

Pour cette analyse, nous utilisons une sélection de la norme ISO 27001, enrichie afin d'intégrer toutes les exigences supplémentaires de DORA qui ne sont pas couvertes par défaut. Vous obtiendrez les résultats présentés sous forme graphique, comme ci-dessous :



Les résultats de l'évaluation des écarts (Gap Assessment) vous donnent une vision précise de votre niveau de maturité ainsi que des écarts identifiés. Vous recevrez des recommandations concrètes pour les améliorer.



Accompagnement à la mise en oeuvre de DORA

En fonction des écarts révélés par l'évaluation des écarts DORA (Gap Assessment), nous proposons un accompagnement à la mise en oeuvre. Vous pouvez avoir besoin de services de cybersécurité spécifiques pour combler certains écarts. Nous pouvons vous y aider.



Peut-être souhaitez-vous investir dans la sensibilisation : nous proposons le **programme SAFE Awareness**, conçu pour provoquer un véritable changement de comportement.



Avez-vous besoin d'un plan de réponse aux incidents ? Le **service Incident Response PRO** vous aide à vous préparer à d'éventuels incidents et vous garantit un accompagnement en cas de survenue.



Le service complet de cybersécurité **CyberCare** vous aide à planifier et à mettre en oeuvre les mesures nécessaires. Nous pouvons intervenir en tant que conseiller indépendant et de confiance.



Gestion des risques

DORA exige des organisations qu'elles gèrent les risques liés à la sécurité des réseaux et des systèmes d'information. Nous pouvons vous accompagner dans cette démarche, par exemple en révisant la méthodologie de gestion des risques existante, en définissant une méthodologie adaptée à votre organisation et en réalisant des analyses de risques.



Sécurité de la chaîne d'approvisionnement

DORA exige des organisations qu'elles gèrent les risques de sécurité liés à leurs fournisseurs et prestataires de services. Vous cherchez à identifier les faiblesses potentielles dans votre chaîne d'approvisionnement ? Nous pouvons vous accompagner grâce à une Vendor Assessment.



Ce que disent nos clients

“Nous sommes heureux d'avoir commencé à temps.”

Nous pensions être prêts pour DORA puisque nous étions certifiés ISO 27001. Cependant, l'évaluation des écarts (Gap Assessment) réalisée par Bureau Veritas Cybersecurity a montré que certains de nos processus n'étaient pas couverts par notre certification ISO. Il s'est donc avéré que nous n'étions pas encore conformes à DORA.

