

**Se préparer à l'implémentation du règlement DORA**  
Digital Operational Resilience Act – Réf. 2502

Durée	7 heures
Inter entreprise	990 euros H.T.
Intra entreprise	Nous consulter
Taux de satisfaction	N/A

Le règlement DORA entré en vigueur le 16 janvier 2023 ou comment renforcer sa résilience opérationnelle, à pour objectif de pouvoir répondre et se rétablir face à toute perturbation opérationnelle grave liée aux technologies de l'information et de communication (TIC).

Cette formation a pour objectif de former aux impacts et modalités opérationnelles de mise en œuvre cette directive européenne.

Pré-requis	<ul style="list-style-type: none"> <li>Aucun</li> </ul>
Public concerné	<ul style="list-style-type: none"> <li>RSSI/CISO,</li> <li>Responsables conformité,</li> <li>DSI des établissements de crédit, établissements de paiement, prestataires de services de cryptoactifs, entreprises d'assurance et de réassurance, gestionnaires d'actifs et tiers fournisseurs de services TIC</li> </ul>
Nombre de stagiaires	<ul style="list-style-type: none"> <li>Minimum 4 à 12 personnes</li> </ul>
Délai d'accès au public	<ul style="list-style-type: none"> <li>2 semaines à compter de la demande de formation</li> <li>Pour les formations 'sur-mesure', deux entretiens préliminaires sont proposés pour définir ensemble la session de formation souhaitée.</li> </ul>
Compétences visées	<ul style="list-style-type: none"> <li>Etre à même de faire un état de lieux de la situation de son entreprise vs. DORA</li> <li>Pouvoir analyser les écarts et élaborer un plan d'actions pour la mise en conformité à DORA</li> <li>Contribuer à améliorer la résilience opérationnelle numérique de votre entreprise</li> </ul>
Méthode d'évaluation	<ul style="list-style-type: none"> <li>Evaluation sous la forme d'un questionnaire. Ce questionnaire permettra de confirmer les acquis des participants sur les thèmes des modules vus durant la formation.</li> </ul>
Certificat de stage	<ul style="list-style-type: none"> <li>Attestation de fin de stage</li> </ul>
Références bibliographiques & sitographiques utilisés pour ce module de formation	<ul style="list-style-type: none"> <li><a href="https://www.ssi.gouv.fr/">https://www.ssi.gouv.fr/</a></li> <li><a href="https://www.cybermalveillance.gouv.fr/">https://www.cybermalveillance.gouv.fr/</a></li> </ul>
Méthodes pédagogiques	<ul style="list-style-type: none"> <li>En français ou en anglais</li> </ul>

	<ul style="list-style-type: none"> <li>• Remise d'une documentation pédagogique numérique pendant le stage</li> <li>• La formation est constituée d'apports théoriques, d'exercices pratiques, de réflexions et de retours d'expérience</li> <li>• Les échanges seront encouragés autour de retours d'expériences, témoignages des participants.</li> </ul>
Débouché et suite du parcours	<ul style="list-style-type: none"> <li>• Compétence permettant la mise en place et la gestion du projet de mise en conformité NIS2</li> <li>• Gérer la conformité de son organisation</li> </ul>
Lieu	<ul style="list-style-type: none"> <li>• Paris Centre, en région, sur site ou à distance</li> </ul>
Nom de l'intervenant	<ul style="list-style-type: none"> <li>• Consultant-Formateur expert cyberSécurité</li> </ul>
Éléments de biographie de l'intervenant	<ul style="list-style-type: none"> <li>• A préciser</li> </ul>
Modalités d'accès	<ul style="list-style-type: none"> <li>• Pour vous inscrire vous pouvez nous contacter à l'adresse suivante : <a href="mailto:contact@adhel.fr">contact@adhel.fr</a></li> <li>• Ou remplir le questionnaire ci-joint - <a href="https://adhel.fr/contact">https://adhel.fr/contact</a></li> <li>• Nous nous engageons à vous répondre dans les 48H</li> </ul>
Accessibilité	<ul style="list-style-type: none"> <li>• Nous vous invitons à préciser, dans le formulaire d'inscription, tout besoin spécifique d'accompagnement.</li> <li>• Notre équipe se tient également à votre disposition par email à l'adresse <a href="mailto:contact@adhel.fr">contact@adhel.fr</a> afin de recueillir vos éventuels besoins d'aménagements et de vous garantir les meilleures conditions d'accueil, notamment pour les personnes en situation de handicap.</li> </ul>

#### Contenu de la formation

- Pourquoi ce règlement DORA ?
- Gestion du risque lié aux TIC
- Gestion, classification et notification des incidents liés aux TIC
- Tests de résilience opérationnelle numérique
- Gestion des risques liés aux prestataires tiers de services
- Dispositifs de partage d'informations et de renseignements
  - Quel est le lien entre le règlement DORA et la directive NIS2 ?
  - Délai d'application des exigences du règlement DORA
  - Comment assurer sa conformité au règlement DORA
  - 10 étapes pour se mettre en conformité
- Récapitulatif des points clés

#### FIN DU DOCUMENT

**CONTACT :**

✉ [contact@adhel.fr](mailto:contact@adhel.fr)

☎ + 33 (0)9 80 80 22 89

🌐 <https://adhel.fr>

ADHEL – 63 rue Nationale - 92100 Boulogne Billancourt  
Siret : 88274050900014 – NDA : 11922660392

Organisme de formation Qualiopi au titre des actions de formation continue

