Oo2 Formations & Consulting

Digital Operational Resilience Act

DORA

PECB AUTHORIZED TITANIUM PARTNER

DORA Digital Operational Resilience Act

Qualiopi processus certifié

RÉPUBLIQUE FRANÇAISE

La certification qualité a été délivrée au titre de la catégorie d'action suivante : ACTIONS DE FORMATION.

DORA

Transformez les risques numériques en opportunités stratégiques

La transformation numérique rapide des entreprises a accru leur dépendance aux technologies, rendant la résilience opérationnelle numérique essentielle pour assurer la continuité des activités face aux perturbations. Le Digital Operational Resilience Act (DORA), introduit par l'Union européenne, vise à renforcer cette résilience en encadrant les entreprises face aux risques numériques.

Qu'est-ce que DORA ?

Entrée en vigueur le 17 janvier 2025, la DORA (Digital Operational Resilience Act) est une législation européenne conçue pour garantir que les institutions financières et autres entreprises sensibles puissent résister, réagir et se rétablir rapidement après une perturbation numérique. Elle couvre les cyberattaques, les pannes techniques et les catastrophes naturelles, renforçant ainsi la résilience numérique des acteurs clés.

Les cinq axes principaux de DORA

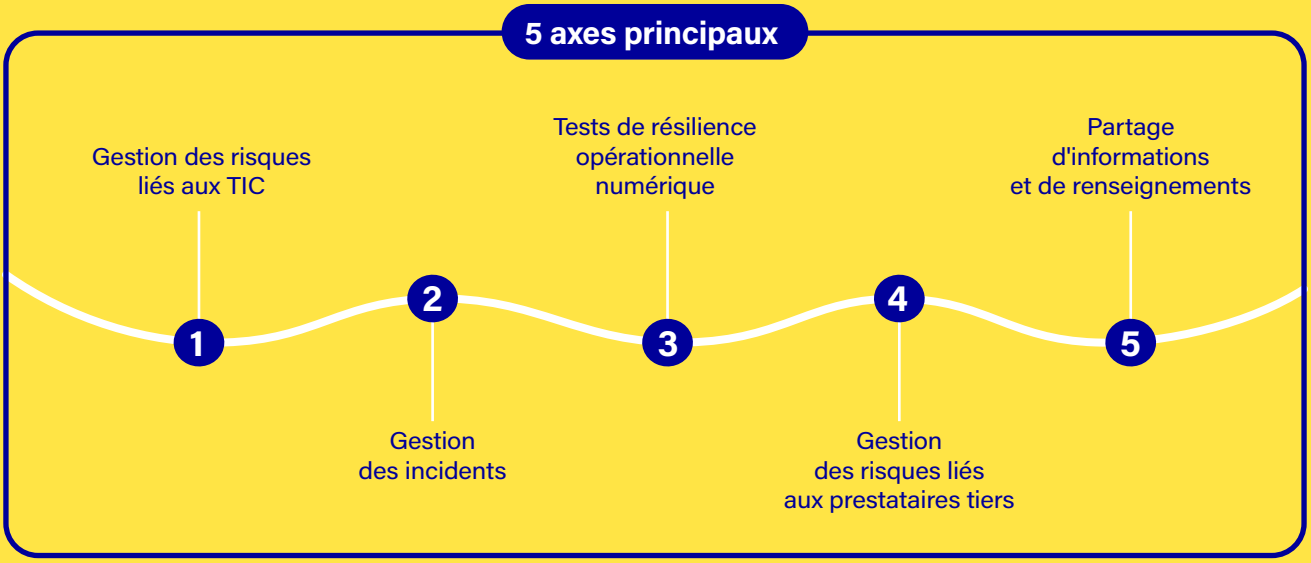
1. Gestion des risques liés aux TIC : Élaboration de stratégies pour identifier, évaluer et gérer les risques associés aux technologies de l'information et de la communication, incluant la cybersécurité et la protection des infrastructures critiques.

2. Gestion des incidents : Obligation de signaler rapidement les incidents majeurs aux régulateurs pour minimiser les impacts et garantir la transparence.

3. Tests de résilience opérationnelle numérique : Tests réguliers pour évaluer la capacité des infrastructures à résister aux menaces numériques.

4. Gestion des risques liés aux prestataires tiers : Surveillance accrue des prestataires critiques comme les fournisseurs de cloud computing.

5. Partage d'informations et de renseignements: Encouragement au partage de renseignements sur les cybermenaces pour renforcer les défenses collectives.



Pourquoi obtenir la certification DORA ?

- Démontrez une compréhension approfondie des exigences de DORA.
- Concevez et mettez en œuvre des stratégies de résilience numérique.
- Devenez un acteur clé dans l'alignement des processus organisationnels.

Avantages pour votre organisation

- Sécurisation des données et systèmes critiques : Réduction des impacts des cyberattaques.
- Conformité avec les régulations européennes : Évitez les sanctions et démontrez votre engagement.
- Confiance accrue des parties prenantes : Renforcez votre réputation et gagnez un avantage concurrentiel.
- Continuité des opérations : Tests réguliers pour minimiser les interruptions de service.
- Gestion des prestataires externes sécurisée : Assurez une continuité des services critiques en toutes circonstances.

Formation DORA Lead Manager :

mettre en œuvre des stratégies de résilience numérique avec certification

Durée : 4,5 jours *Code : DLMFR*

Objectifs

- Connaître les 5 principes fondamentaux de la réglementation DORA (Digital Operational Resilience Act).
- Mettre en œuvre des stratégies et des solutions pour améliorer la résilience opérationnelle et atténuer les risques liés aux TIC dans les institutions financières, selon les exigences de la réglementation DORA et les bonnes pratiques du secteur.
- Identifier, analyser, évaluer et gérer les risques informatiques pour les organismes financiers.
- Élaborer et maintenir des systèmes fiables de gestion des risques liés aux TIC, des plans de réponse aux incidents, des plans de continuité des activités et des plans de reprise après sinistre.
- Faciliter des échanges avec les principales parties prenantes afin d'assurer le succès et la conformité continue avec la loi DORA.
- Utiliser des outils et des méthodes spécifiques pour surveiller, évaluer, gérer les risques et les vulnérabilités liés aux TIC, afin d'améliorer le niveau de sécurité global des établissements financiers.
- Réussir l'examen PECB Certified DORA Lead Manager et obtenir l'une des 4 certifications associées.

Programme

Jour 1 : introduction à la réglementation DORA

- Le contexte et les enjeux du règlement DORA.
- Le périmètre d'application et les parties prenantes.
- Les principes fondamentaux et les objectifs de DORA.
- Analyse détaillée des 5 piliers DORA :
  - La gestion des risques liés aux TIC ;
  - La gestion des incidents liés aux TIC ;
  - Les tests de résilience opérationnelle numérique ;
  - La gestion des risques liés aux prestataires tiers de services TIC ;
  - Le partage d'informations et de renseignements.

Jour 2 : gestion des risques et des incidents liés aux TIC

- Le cadre de gestion des risques liés aux TIC : identification, analyse, évaluation et traitement des risques.
- Les méthodes d'évaluation des risques liés aux TIC : analyse de l'impact sur les activités, scénarios de défaillance, etc.
- La mise en œuvre de mesures de contrôle et de plans de remédiation adaptés.
- Les processus de gestion des incidents liés aux TIC : détection, classification, enquête, réponse et récupération.
- Les plans de continuité des activités et de reprise après sinistre pour les systèmes d'information critiques.

Jour 3 : gestion des risques liés aux tiers et partage d'informations

- L'identification et l'évaluation des risques associés aux fournisseurs de services tiers.
- La mise en place de procédures rigoureuses de contrôle et de contractualisation.
- La surveillance continue des prestataires de services et les mesures de contrôle adaptées.
- L'importance des échanges d'informations et de renseignements entre les acteurs financiers.
- Les méthodes de communication et de coopération en cas d'incident ou de crise.
- Le rôle des autorités de surveillance et des organisations des marchés financiers.

Jour 4 : réévaluation et amélioration continue

- L'importance de la réévaluation et de l'amélioration continue du cadre de gestion de la
- résilience opérationnelle.
- La mise en place de processus de suivi et d'indicateurs de performance.
- Les audits internes et externes pour garantir la conformité à DORA.
- Les bonnes pratiques en matière de résilience opérationnelle.
- L'évolution future de la réglementation et les questions émergentes.
- Les attentes et les défis liés à la mise en place de DORA.

Jour 5 : préparation à l'examen PECB DORA Lead Manager

- Présentation de la structure et du format de l'examen.
- Conseils et astuces pour réussir l'examen.

Examen de certification DORA

- Format : 80 questions à choix multiple (QCM)
- Durée : 3 heures
- Note de passage : Minimum 70 % de bonnes réponses

Prérequis

- Connaître les concepts de base de la sécurité de l'information et de la cybersécurité.
- Connaître les principes de la gestion des risques liés aux technologies de l'information et de la communication (TIC).
- Savoir lire et comprendre l'anglais pour accéder au support de cours et passer l'examen.

Public

- Analyste cybersécurité ;
- Directeur des Systèmes d'Information (DSI) ;
- Directeur financier ;
- Manager ;
- Responsable des risques, compliance manager ;
- Décideur dans les institutions financières et toute organisation impactée par DORA.

en savoir +

Oo2 Formations & Consulting

France

- **Agence Paris**
  128, rue de la Boétie
  75008 Paris
- **Agence Bordeaux**
  162 cours du Maréchal Gallieni
  33400 Talence

+33 (0)188 24 70 33
+33 (0)188 24 70 34

contact@oo2.fr

Belgique

- **Agence Bruxelles**
  Rue de la Colonne 1A
  1080 Bruxelles

+32 28.08.51.75

contact@oo2.be

www.oo2.fr

Pourquoi choisir Oo2 ?

- Des formateurs experts et certifiés dans les domaines de la résilience numérique.
- Une approche pédagogique alliant théorie et pratique pour une meilleure assimilation.
- Une certification reconnue et valorisée à l'échelle internationale.
- Un accompagnement personnalisé pour votre conformité avec DORA.