DORA

Durée : 1 jour (7 heures)

CONNAISSANCES PREALABLES

- Connaissances générales des systèmes d'information.
- Notions de cybersécurité et de gestion des risques.
- Une connaissance de l'environnement réglementaire du secteur financier constitue un plus, sans être indispensable.

PROFIL DES STAGIAIRES

- RSSI et responsables cybersécurité
- DSI et responsables informatiques
- Responsables conformité et gestion des risques
- Auditeurs internes
- Responsables PCA/PRA
- DPO
- Responsables des fournisseurs et de la sous-traitance
- Toute personne impliquée dans la mise en conformité réglementaire du secteur financier.

OBJECTIFS

À l'issue de la formation, les participants seront capables de :

- Comprendre les objectifs et le périmètre du règlement DORA.
- Identifier les obligations applicables aux entités financières concernées.
- Comprendre les exigences en matière de gestion des risques TIC.
- Structurer un dispositif de résilience opérationnelle numérique.
- Organiser la gestion des incidents TIC conformément à DORA.
- Maîtriser les exigences relatives aux prestataires TIC tiers.
- Préparer leur organisation à une démarche de conformité DORA.
- Construire une feuille de route de mise en conformité.

CERTIFICATION PREPAREE

Aucune

METHODES PEDAGOGIQUES

- Alternance d'apports théoriques et d'illustrations pratiques.
- Analyse des exigences réglementaires et de leurs impacts opérationnels.
- Études de cas inspirées d'organisations financières.
- Ateliers collaboratifs de cartographie des écarts.
- Exercices de réflexion autour de scénarios de conformité.
- Échanges d'expériences et retours terrain.

FORMATEUR

- Consultant expert en cybersécurité, gestion des risques et conformité réglementaire disposant d'une expérience significative dans l'accompagnement d'organisations soumises aux réglementations européennes en matière de résilience numérique, de cybersécurité et de gouvernance des risques.

METHODE D'EVALUATION DES ACQUIS

- Questionnaire de positionnement en début de formation.
- Évaluation continue au travers des ateliers et études de cas.
- Quiz de validation des connaissances.
- Cas pratique de synthèse en fin de formation.
- Questionnaire d'évaluation des acquis.

CONTENU DU COURS

Module 1 : Comprendre DORA et ses enjeux pour les organisations financières (1h30)

Objectifs

- Comprendre l'origine et les objectifs du règlement DORA.
- Identifier les organisations concernées et les impacts attendus.

Contenu

- Contexte réglementaire européen.
- Présentation du règlement DORA.
- Objectifs de résilience opérationnelle numérique.
- Périmètre d'application.
- Organismes concernés.
- Calendrier de mise en conformité.
- Articulation avec NIS2, RGPD et les autres réglementations sectorielles.

Mise en pratique

Brainstorming collectif :

- Identification des impacts potentiels de DORA sur l'organisation des participants.

Module 2 : Gestion des risques TIC et gouvernance de la résilience numérique (1h30)

Objectifs

- Comprendre les exigences de DORA en matière de gestion des risques TIC.
- Identifier les éléments constitutifs d'une gouvernance conforme.

Contenu

- Cadre de gestion des risques TIC.
- Gouvernance et responsabilités.
- Identification et évaluation des risques.
- Mesures de protection et de prévention.
- Détection et surveillance des incidents.
- Résilience et continuité des activités.

Mise en pratique

Atelier :

- Cartographie simplifiée des risques TIC d'une organisation financière.

Module 3 : Gestion des incidents TIC et obligations de notification (1h30)

Objectifs

- Organiser la gestion des incidents conformément aux exigences DORA.
- Comprendre les obligations de déclaration.

Contenu

- Classification des incidents TIC.
- Critères de gravité.
- Détection et qualification.
- Processus d'escalade.
- Notification aux autorités compétentes.
- Documentation et retour d'expérience.

Mise en pratique

Étude de cas :

- Qualification d'un incident TIC et détermination des obligations de notification.

Module 4 : Gestion des prestataires TIC tiers et contrôles de conformité (1h30)

Objectifs

- Maîtriser les exigences applicables aux fournisseurs TIC.
- Renforcer la gestion des risques liés à la sous-traitance.

Contenu

- Risques liés aux prestataires critiques.
- Obligations contractuelles.
- Surveillance des prestataires TIC.
- Externalisation et Cloud.
- Audits et contrôles.
- Gestion de la concentration des risques.

Mise en pratique

Atelier :

- Analyse d'un scénario d'externalisation Cloud au regard des exigences DORA.

Module 5 : Construire sa feuille de route de mise en conformité DORA (1h)

Objectifs

- Identifier les écarts de conformité.
- Définir un plan d'action réaliste.

Contenu

- Méthodologie d'analyse des écarts.
- Priorisation des actions.
- Gouvernance du projet DORA.
- Pilotage de la conformité.
- Amélioration continue.

Mise en pratique

Cas pratique de synthèse :

À partir d'une organisation fictive :

- Identification des exigences applicables.
- Analyse des écarts.
- Priorisation des actions.
- Élaboration d'une feuille de route de mise en conformité.
- Présentation des recommandations.

Notre référent handicap se tient à votre disposition au 01.71.19.70.30 ou par mail à mailto:referent.handicap@edugroupe.com pour recueillir vos éventuels besoins d'aménagements, afin de vous offrir la meilleure expérience possible.