EduGroupe
Accompagner pour réussir

Sensibilisation au règlement DORA

Référence : **SECDORA01** Durée : **1 jour** Certification : **Aucune**

CONNAISSANCES PREALABLES

• Avoir des connaissances de l'environnement ou du contexte des entités financières, et/ou être un professionnel des Technologies de l'Information et de la Communication (TIC).

PROFIL DES STAGIAIRES

• RSSI / DSI - CTO - DPO /Juriste. • Toute personne au sein d'institutions financières souhaitant découvrir le Règlement DORA.

OBJECTIFS

• Découvrir le Règlement DORA au travers de ses 17 exigences.

CERTIFICATION PREPAREE

Aucune

METHODES PEDAGOGIQUES

- Mise à disposition d'un poste de travail par stagiaire
- Remise d'une documentation pédagogique numérique pendant le stage
- La formation est constituée d'apports théoriques, d'exercices pratiques, de réflexions et de retours d'expérience
- Le suivi de cette formation donne lieu à la signature d'une feuille d'émargement

FORMATEUR

Consultant-Formateur expert Management de la sécurité

METHODE D'EVALUATION DES ACQUIS

- Auto-évaluation des acquis par le stagiaire via un questionnaire
- Attestation des compétences acquises envoyée au stagiaire
- Attestation de fin de stage adressée avec la facture

CONTENU DU COURS

Chapitre 1
- Cadre réglementaire
- Différences et point commun entre DORA et NIS2
- Sanctions prévues par DORA

Chapitre 2
- Les institution et organisation concernés par DORA
- Les exigences fixées par DORA

Chapitre 3
- Cadre de gestion du risque lié au TIC
- Audit régulier du cadre de gestion du risque TIC

Chapitre 4
- Stratégie de résilience opérationnelle numérique
- Les mécanismes de protection et de résilience des actifs
- Les solutions de détection
- Politique de continuité des activités TIC

Chapitre 5
- Procédure de sauvegarde, restauration et de rétablissement
- Les politiques associées

Chapitre 6
- Plan de communication en situation de crise
- Processus de gestion des incidents
- Plan de réponse aux incidents

Chapitre 7
- Veille sur les cybermenaces
- Test de résilience opérationnelle numérique
- Planification des tests d'intrusion fondés sur la menace

Chapitre 8
- Vulgarisation, sensibilisation et formation à la cybersécurité

Chapitre 9

- Évaluation et gestion des prestataires de service TIC

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