Se préparer à l'implémentation du règlement DORA (Digital Operational Resilience Act)

Référence : **SECDORA02** Durée : **1 jour (7 heures)** Certification : **Aucune**

Connaissances préalables

- Connaissances de base en cybersécurité et sécurité des systèmes d'information

Profil des stagiaires

- RSSI/CISO
- Responsables conformité
- DSI des organismes concernés par DORA

Objectifs

- Comprendre le cadre du règlement DORA, ses principes et ses exigences
- Acquérir une base solide de connaissances en matière de gestion des risques pour la cybersécurité, de réponse aux incidents, d'obligations de conformité et de bonnes pratiques
- Evaluer et à atténuer les risques cyber
- Communiquer et transmettre les concepts et les stratégies de cybersécurité aux intervenants à tous les niveaux d'une organisation
- Faire un état des lieux de la situation de son entreprise versus les obligations DORA
- Analyser les écarts et élaborer un plan d'actions de mise en conformité à DORA

Certification préparée

- Aucune

Méthodes pédagogiques

- Mise à disposition d'un poste de travail par stagiaire
- Plateforme Internet pour le suivi, les quiz, l'évaluation et le dépôt des supports
- Remise d'une documentation pédagogique papier ou numérique pendant le stage
- Alternance d'apports conceptuels et d'exercices pratiques : chaque séquence combine des éléments réglementaires (obligations, cadre européen, gouvernance) et des mises en situation (auto-diagnostic de maturité DORA, analyse d'écart, construction d'un plan d'action)
- Études de cas réelles : scénarios issus d'établissements financiers, fintech et prestataires TIC permettent d'ancrer les apprentissages dans des contextes proches de la réalité des entreprises
- Ateliers collaboratifs : en sous-groupes, les stagiaires élaborent une feuille de route DORA adaptée à leur structure et débattent des priorités d'implémentation

Formateur

- Consultant-formateur expert DORA, disposant d'une expérience opérationnelle dans la conformité et la cybersécurité des services financiers

Méthodes d'évaluation des acquis

- Évaluation continue : quiz interactifs, exercices de réflexion en groupe et QCM final garantissent l'assimilation progressive des connaissances
- 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

Matinée : Comprendre le cadre et les exigences du règlement DORA (3h30)

Contexte et objectifs du règlement

• Origine du texte (règlement UE 2022/2554) et calendrier d'application
• Positionnement dans le paquet "Finance Numérique" et lien avec NIS2
• Enjeux de la résilience opérationnelle numérique pour le secteur financier

Champ d'application et acteurs concernés

• Entités financières : banques, assurances, fintech, prestataires TIC
• Sous-traitants critiques et chaîne de dépendances

Piliers du règlement DORA

• Gouvernance et pilotage de la résilience opérationnelle
• Gestion des risques TIC
• Gestion des incidents et communication aux autorités
• Tests de résilience opérationnelle
• Gestion des tiers fournisseurs TIC
• Échange d'informations (threat intelligence, coopération sectorielle)

Cartographie réglementaire

• Articulation avec les référentiels existants : RGPD, NIS2, ISO 27001, EBA Guidelines
• Rôles des autorités compétentes (ESAs, ACPR, AMF, BCE)
• 🛠 Exercice pratique : repérage des impacts DORA sur l'organisation du participant (cartographie acteurs, dépendances TIC, responsabilités)

Après-midi : Se préparer à la mise en œuvre opérationnelle (3h30)

Mettre en place une gouvernance DORA

• Rôles et responsabilités : direction générale, conformité, RSSI, IT, risk management
• Intégration dans la stratégie d'entreprise et la gestion des risques globaux

Diagnostic et plan de mise en conformité

• Évaluation du niveau de maturité
• Identification des écarts et plan d'action priorisé
• Indicateurs de pilotage et reporting

Mesures techniques et organisationnelles clés

• Gestion des incidents TIC et plan de continuité
• Contrôle des prestataires TIC critiques
• Procédures de tests de résilience et simulations de crise

Outils et ressources pour piloter la conformité

• Modèles de registres, tableaux de bord, plans d'action
• Bonnes pratiques issues de l'EBA et de l'ENISA
• 🛠️ Atelier collaboratif : élaboration d'une feuille de route DORA simplifiée adaptée à la taille et au secteur de chaque entreprise

Évaluation des acquis : quiz interactif / QCM final

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.