

RÈGLEMENT DORA : APPROFONDISSEMENT

Découvrez les 17 exigences du Règlement DORA et les possibilités de mise en œuvre

Code : ADORA

Le Règlement DORA (n°2022/2554), ou Digital Operational Resilience Act(*), est un texte législatif majeur de l'Union Européenne sur la cybersécurité des entités financières, comme les banques ou les établissements de crédit.

Cette formation permet d'étudier de façon détaillée et complète les 17 exigences de DORA sur la résilience opérationnelle numérique pour les entités financières. Chaque stagiaire pourra identifier les possibilités de mise en œuvre du Règlement avec des mesures techniques, organisationnelles et physiques.

(*) En français : DORA = Règlement sur la résilience opérationnelle du numérique.

PROGRAMME

Méthodes mobilisées : cette formation est construite avec une alternance de cours théoriques et de cas pratiques afin de favoriser l'acquisition des savoirs du programme (cf. Ressources).

Modalités d'évaluation : les objectifs sont régulièrement évalués tout au long de la formation (30% d'exercices pratiques + étude d'un cas pratiques) et formalisés sous forme de grille d'évaluation des compétences complétée en fin de module par le formateur.

JOUR 1

Chapitre 1

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

JOUR 2

Chapitre 2

- Les institutions et organisations concernées par DORA
- Les exigences fixées par DORA

JOUR 3

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

JOUR 4

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

JOUR 5

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

Étude & correction d'un cas pratique

PROCHAINES DATES

24 juin 2024
2 décembre 2024



OBJECTIFS

- Découvrir le Règlement DORA au travers de ses 17 exigences
- Repartir avec des pistes concrètes de mise en œuvre afin de répondre aux exigences du Règlement



INFORMATIONS GÉNÉRALES

Code : ADORA

Durée : 5 jours

Prix : 4 150 € HT

Horaires : 9h30 - 17h30

Lieu : Levallois (92)



PUBLIC VISÉ

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



PRÉ-REQUIS

- 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)



RESSOURCES

- Support de cours
- 30% d'exercices pratiques + étude d'un cas pratique
- 1 PC par personne