

# SENSIBILISATION AU RÈGLEMENT DORA

## Découvrez les 17 exigences du Règlement DORA

Code : SDORA

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 journée de sensibilisation permet une mise en lumière du Règlement via la checklist des 17 exigences de DORA.

Il sera évoqué aussi la possibilité de mise en œuvre du Règlement avec des mesures techniques, organisationnelles et physiques.

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

Cette journée de sensibilisation pourra être complétée grâce aux sessions d'approfondissement (5 jours) :

- En INTER : du 24 au 28 juin 2024 **ou** du 2 au 6 décembre 2024
- En INTRA : sur demande, avec possibilité d'ajuster le programme en fonction de vos besoins

## 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 évalués lors d'un QCM final 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

#### 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

**QCM final pour évaluer l'acquisition des savoirs du Règlement DORA**



## PROCHAINES DATES

29 janvier 2024  
25 mars 2024  
27 mai 2024  
1<sup>er</sup> juillet 2024  
9 septembre 2024



## OBJECTIFS

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



## INFORMATIONS GÉNÉRALES

**Code** : SDORA

**Durée** : 1 jour

**Prix** : 1 495 € 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
- QCM final
- 1 PC par personne

**Cette journée de sensibilisation pourra être complétée grâce aux sessions d'approfondissement (5 jours) :**

- En INTER : du 24 au 28 juin 2024 **ou** du 2 au 6 décembre 2024
- En INTRA : sur demande, avec possibilité d'ajuster le programme en fonction de vos besoins