

LES PLUS DE
DE LA FORMATION

- Approche d'écart basée sur les travaux existants
- Outil de diagnostic
- Discussion dirigée et échanges d'expérience pour enrichir la compréhension
- Constitution d'une trajectoire pour être conforme

DORA ET CONTRÔLE INTERNE : STRATÉGIES ET PRATIQUES

La réglementation DORA (Digital Operational Resilience Act) impose aux acteurs des services financiers et largement aux prestataires de renforcer leur résilience opérationnelle face aux risques liés aux technologies de l'information et de la communication (TIC). Cette formation d'une journée est conçue pour les contrôleurs internes et les auditeurs, afin de leur permettre de comprendre et de déployer un cadre de contrôle interne conforme aux exigences de DORA. Grâce à des séquences interactives et des études de cas pratiques, les participants apprendront à identifier les besoins spécifiques de leur organisation, à mettre en œuvre des contrôles efficaces et à assurer la continuité de leurs activités face aux perturbations majeures.

PARTICIPANTS

Contrôleurs internes, DPO, Responsable des plans de continuité d'activité, équipes Cybersécurité, auditeurs internes et externes

Accessibilité - cf. page 11

MOYENS PÉDAGOGIQUES

Visuels de présentation – fiches techniques – exercices – alternance de mises en application, de retours d'expériences et d'exposés et usage d'un outil de diagnostic sur la base du référentiel DORA et des RTS.

PRÉREQUIS

Aucun

OBJECTIFS PÉDAGOGIQUES

- **Appréhender** les objectifs et les exigences de DORA.
- **Connaître** les implications pour les acteurs concernés.
- **Identifier** les risques liés aux TIC et les vulnérabilités.
- **Développer** et implémenter des mesures de Contrôle interne DORA.

MODALITÉS D'ÉVALUATION DES ACQUIS

Progression des apprentissages et évaluation des acquis des participants réalisés par le formateur tout au long de la formation (temps d'échanges, travaux pratiques, exercices d'entraînements, quiz...).

Une évaluation de la satisfaction de chaque stagiaire est réalisée en ligne. Cette évaluation est complétée par l'appréciation du formateur à l'issue de chaque session.

INTERVENANT

Formation conçue et animée par Eric CHEMAMA, expert certifié sur les Systèmes d'information (SI), les normes de continuité et de sécurité de l'information.

CONTENU

- **Objectifs principaux et portée de DORA (différences et complémentaires avec NIS 2)**
- **Identification des entités critiques et principe de proportionnalité**
- **Obligation de gestion des risques et test de résilience**
- **Standards du référentiel (RTS/ITS)**
- **Évaluation des dispositifs actuels de gestion des risques TIC**
- **Processus de notification des incidents TIC**

1 JOUR/7h

8h45 - 17h30

Présentielle

Paris intra muros

Adhérents IFACI :
805 € HT
Non adhérents :
960 € HT

Déjeuner(s) inclus

CPE 7

12 participants

ref. Performance;
Environment

4 DATES

• 18/03 • 19/09
• 27/06 • 17/11

Code formation : **25DOSP**

Inscription inter : formation@ifaci.com

Information :
01 40 08 (48 08 / 47 85)

www.ifaci.com

Déclinaison de cette formation
en INTRA selon vos spécificités :
contactez-nous au **01 40 08**
(48 05 ou 48 06) ou intra@ifaci.com