Dora Lead Manager, certification

Maîtriser la conformité réglementaire et la résilience opérationnelle dans le secteur financier - Certification incluse

Présentiel ou en classe à distance

5 jours (35 h)

Prix inter : 4.990,00 € HT
Forfait intra : 26.550,00 € HT

Réf.: MG871

Dans un contexte de digitalisation accrue et d'exigences réglementaires toujours plus strictes, la **certification DORA Lead Manager** s'impose comme une référence incontournable pour les professionnels de la cybersécurité et de la gestion des risques TIC. Elle permet d' **assurer la conformité aux exigences du Digital Operational Resilience Act** (DORA) et d'optimiser la sécurité des infrastructures critiques.
Les participants apprendront à **optimiser la gestion des risques TIC** , à renforcer la sécurité des systèmes d'information, à améliorer la gestion des incidents et à assurer la conformité réglementaire. L'accent est mis sur l'application concrète des principes du DORA dans des domaines clés tels que la gouvernance des risques, la cybersécurité, la surveillance des prestataires tiers et l'amélioration continue des processus opérationnels.
Cette formation prépare à la certification Certification Dora Lead Manager et inclus le voucher pour passer l'examen.

A qui s'adresse cette formation ?

Pour qui

- RSSI/CISO, responsables conformité, DSI des établissements de crédit, établissements de paiement, prestataires de services de cryptoactifs, entreprises d'assurance et de réassurance, gestionnaires d'actifs et tiers fournisseurs de services TIC

Prérequis

- Aucun.

Programme

1 - Objectifs de la formation

- Introduction
- Informations générales
- Objectifs d’apprentissage
- Approche pédagogique
- Examen et certification
- À propos de PECB

2 - Aperçu du Digital Operational Resilience Act (DORA)

- Contexte et historique
- Définition et principaux objectifs
- Champ d’application
- Principe de proportionnalité
- Exigences clés
- Sanctions en cas de non-conformité
- Normes techniques et directives sous DORA
- Relation avec d’autres réglementations de l’UE

3 - Concepts fondamentaux de la gestion des risques liés aux TIC

- Micro, petites et moyennes entreprises
- Concepts liés aux TIC
- Définition du risque
- Gestion des risques
- Résilience organisationnelle
- Résilience opérationnelle numérique

4 - Mise en oeuvre d’un projet DORA

- Éléments essentiels et exigences du cadre de gestion des risques liés aux TIC
- Stratégie de résilience opérationnelle numérique
- Analyse de l’organisation et de son contexte
- Identification et analyse des parties prenantes
- Détermination des objectifs de mise en oeuvre du projet DORA
- Réalisation d’une analyse des écarts

5 - Gouvernance et organisation

- Cadre de gouvernance interne et de contrôle
- Modèle des trois lignes
- Mise en oeuvre du cadre de gestion des risques liés aux TIC
- Responsabilités des organes de direction
- Rôle de surveillance des prestataires tiers en TIC
- Développement professionnel continu

6 - Gestion des risques liés aux TIC

- Systèmes, protocoles et outils TIC
- Politique de gestion des risques liés aux TIC
- Composantes de la politique de continuité des activités TIC
- Plans de réponse et de reprise TIC
- Plans de gestion de crise
- Processus de gestion des risques liés aux TIC

7 - Gestion et déclaration des incidents liés aux TIC

- Processus de gestion des incidents liés aux TIC
- Cycle de vie de la gestion des incidents
- Composantes essentielles d’une gestion efficace des incidents TIC
- Classification des incidents liés aux TIC
- Déclaration des incidents liés aux TIC
- Procédures de déclaration pour les entités financières
- Délais de déclaration
- Contenu des rapports

8 - Tests de résilience opérationnelle numérique

- Tests de résilience opérationnelle numérique
- Tests des outils et systèmes TIC
- Exigences pour les tests d’intrusion basés sur les menaces
- Attestation des tests d’intrusion basés sur les menaces
- Sélection des testeurs pour effectuer les tests d’intrusion basés sur les menaces

9 - Gestion des risques liés aux prestataires tiers TIC

- Principes d’une gestion saine des risques liés aux prestataires tiers TIC
- Prérequis contractuels pour les services TIC financiers
- Procédures de résiliation des contrats de services TIC
- Évaluation préliminaire du risque de concentration TIC au niveau de l’entité
- Clauses contractuelles clés

10 - Cadre de supervision et superviseur principal

- Désignation des prestataires critiques de services TIC tiers
- Structure du cadre de supervision
- Missions du superviseur principal
- Pouvoirs du superviseur principal
- Mesures d’application en cas de non-conformité
- Demandes d’informations
- Inspections
- Suivi par les autorités compétentes

11 - Informations et renseignements

- Accords de partage d’informations sur les menaces cybernétiques et les renseignements
- Types de renseignements sur les menaces
- Comment se préparer à un partage efficace des informations
- Sensibilisation au partage d’informations

12 - Formation et sensibilisation

- Élaboration d’une stratégie de formation et de sensibilisation
- Détermination des besoins en développement des compétences
- Planification des activités de développement des compétences
- Conduite des activités de formation et de sensibilisation
- Évaluation des résultats du programme de formation et de sensibilisation
- Amélioration du programme de formation et de sensibilisation

13 - Autorités compétentes

- Autorités compétentes
- Coopération avec les structures et autorités
- Exercices intersectoriels financiers, communication et coopération
- Sanctions administratives et mesures correctives
- Sanctions pénales
- Secret professionnel
- Protection des données

14 - Suivi, mesure, analyse et évaluation

- Détermination des besoins en information
- Définition des éléments à surveiller et mesurer
- Surveillance du cadre de gestion des risques liés aux TIC
- Établissement d’indicateurs de performance pour le cadre de gestion des risques TIC
- Détermination de la fréquence et de la méthode de surveillance et de mesure

15 - Audit et revue de gestion

- Qu’est-ce qu’un audit ?
- Audit interne du cadre de gestion des risques liés aux TIC
- Collecte et vérification des informations
- Planification des activités d’audit
- Documentation des non-conformités
- Préparation de la revue de gestion
- Conduite des activités de suivi de la revue de gestion

16 - Amélioration continue

- Surveillance continue des facteurs de changement
- Maintien et amélioration du cadre de gestion des risques TIC
- Mise à jour et maintien des informations documentées
- Documentation des améliorations

17 - Clôture de la formation

- Schéma de certification PECB
- Attestation de suivi de formation
- Processus de certification PECB
- Autres services PECB
- Autres formations et certifications PECB

Evaluation

- Pendant la formation, le formateur évalue la progression pédagogique des participants via des QCM, des mises en situation et des travaux pratiques. Les participants passent un test de positionnement avant et après la formation pour valider leurs compétences acquises.
Il est fortement recommandé d'être en possession de la norme pour le passage de l'examen.

Les points forts de la formation

- Programme complet pour maîtriser la mise en conformité avec DORA et renforcer la résilience opérationnelle
- Approche pratique avec études de cas réels et exercices interactifs pour appliquer
- Formation dispensée par des experts en gestion des risques TIC et conformité réglementaire
- Contenus correspondant aux dernières normes et réglementations européennes en matière de cybersécurité

Dates et villes 2026 - Référence MG871

Dernières places disponibles Session garantie

Marseille

du 16 mars au 20 mars	du 24 août au 28 août	du 19 oct. au 23 oct.

Toulouse

du 16 mars au 20 mars	du 24 août au 28 août	du 7 déc. au 11 déc.

A distance

du 16 mars au 20 mars	du 24 août au 28 août	du 7 déc. au 11 déc.
du 8 juin au 12 juin	du 19 oct. au 23 oct.	

Aix-en-Provence

du 16 mars au 20 mars	du 24 août au 28 août	du 19 oct. au 23 oct.

Paris

du 16 mars au 20 mars	du 24 août au 28 août	du 7 déc. au 11 déc.
du 8 juin au 12 juin	du 19 oct. au 23 oct.	

Lille

du 16 mars au 20 mars	du 24 août au 28 août	du 19 oct. au 23 oct.

Nantes

du 8 juin au 12 juin	du 24 août au 28 août	du 19 oct. au 23 oct.

Lyon

du 8 juin au 12 juin	du 19 oct. au 23 oct.	du 7 déc. au 11 déc.

Rennes

du 8 juin au 12 juin	du 24 août au 28 août	du 19 oct. au 23 oct.

Bordeaux

du 8 juin au 12 juin	du 19 oct. au 23 oct.	du 7 déc. au 11 déc.

Rouen

du 8 juin au 12 juin	du 19 oct. au 23 oct.	du 7 déc. au 11 déc.

Sophia Antipolis

du 8 juin au 12 juin	du 19 oct. au 23 oct.	du 7 déc. au 11 déc.

Strasbourg

du 8 juin au 12 juin	du 19 oct. au 23 oct.	du 7 déc. au 11 déc.