

DORA Lead Manager, certification PECB

Cours Pratique de 5 jours - 35h

Réf : DLM - Prix 2024 : 3 960CHF HT

A compter du 17 janvier 2025 les entités financières devront se conformer aux exigences de la DORA. Cette formation vous permettra d'acquérir les compétences nécessaires pour accompagner et superviser la mise en œuvre de stratégies de résilience opérationnelle numérique auprès des établissements financiers.

OBJECTIFS PÉDAGOGIQUES

À l'issue de la formation l'apprenant sera en mesure de :

Comprendre le paysage réglementaire et les exigences en matière de conformité du règlement DORA.

Mettre en œuvre des stratégies pour améliorer la résilience opérationnelle dans les institutions financières.

Identifier, analyser, évaluer et gérer les risques liés aux TIC qui concernent les entités financières.

Développer des cadres robustes de gestion des risques, des plans de réponse, des plans de continuité et de reprise.

Favoriser la collaboration et la communication avec les principales parties prenantes.

Utiliser des outils et des méthodologies pour suivre, évaluer et gérer les risques et les vulnérabilités liés aux TIC.

CERTIFICATION

L'examen disponible uniquement en anglais, se déroule en ligne et consiste à répondre à un QCM de 80 questions à livre ouvert pendant 3 heures maximum.

À l'issue du cours, une attestation de suivi de la formation de 31 crédits de FPC (Formation professionnelle continue) sera délivrée.

Les candidats ayant suivi la formation mais échoué à l'examen peuvent le repasser gratuitement une seule fois dans un délai de 12 mois à compter de la date initiale de l'examen.

LE PROGRAMME

dernière mise à jour : 10/2024

1) Introduction des concepts et exigences de DORA

- Le contexte et les enjeux du règlement DORA.
- Le périmètre d'application et les parties prenantes.
- Les principes fondamentaux et les objectifs de DORA.
- Analyse détaillée des 5 piliers DORA

2) Gestion des risques et incidents liés aux TIC

- Le cadre de gestion des risques liés aux TIC : identification, analyse, évaluation et traitement des risques.
- Les méthodes d'évaluation des risques liés aux TIC : analyse de l'impact sur les activités, scénarios de défaillance...
- La mise en œuvre de mesures de contrôle et de plans de remédiation adaptés.
- Les processus de gestion des incidents liés aux TIC : détection, classification, enquête, réponse et récupération.
- Les plans de continuité des activités et de reprise après sinistre pour les systèmes d'information critiques.

PARTICIPANTS

Cadres supérieurs et décideurs des institutions financières, professionnels des TI, consultants et conseillers spécialisés dans la réglementation financière et la cybersécurité...

PRÉREQUIS

Avoir une compréhension fondamentale des concepts de sécurité de l'information et de cybersécurité, ainsi qu'une familiarité avec les principes de gestion des risques des TIC.

COMPÉTENCES DU FORMATEUR

Les experts qui animent la formation sont des spécialistes des matières abordées. Ils ont été validés par nos équipes pédagogiques tant sur le plan des connaissances métiers que sur celui de la pédagogie, et ce pour chaque cours qu'ils enseignent. Ils ont au minimum cinq à dix années d'expérience dans leur domaine et occupent ou ont occupé des postes à responsabilité en entreprise.

MODALITÉS D'ÉVALUATION

Le formateur évalue la progression pédagogique du participant tout au long de la formation au moyen de QCM, mises en situation, travaux pratiques...

Le participant complète également un test de positionnement en amont et en aval pour valider les compétences acquises.

MOYENS PÉDAGOGIQUES ET TECHNIQUES

- Les moyens pédagogiques et les méthodes d'enseignement utilisés sont principalement : aides audiovisuelles, documentation et support de cours, exercices pratiques d'application et corrigés des exercices pour les stages pratiques, études de cas ou présentation de cas réels pour les séminaires de formation.
- À l'issue de chaque stage ou séminaire, ORSYS fournit aux participants un questionnaire d'évaluation du cours qui est ensuite analysé par nos équipes pédagogiques.
- Une feuille d'émargement par demi-journée de présence est fournie en fin de formation ainsi qu'une attestation de fin de formation si le stagiaire a bien assisté à la totalité de la session.

MODALITÉS ET DÉLAIS D'ACCÈS

L'inscription doit être finalisée 24 heures avant le début de la formation.

ACCESSIBILITÉ AUX PERSONNES HANDICAPÉES

Vous avez un besoin spécifique d'accessibilité ? Contactez Mme FOSSE, référente handicap, à l'adresse suivante psh-accueil@orsys.fr pour étudier au mieux votre demande et sa faisabilité.

3) Gestion des risques liés aux prestataires tiers et partage des informations

- L'identification et l'évaluation des risques associés aux fournisseurs de services tiers.
- La mise en place de procédures rigoureuses de contrôle et de contractualisation.
- La surveillance continue des prestataires de services et les mesures de contrôle adaptées.
- L'importance des échanges d'informations et de renseignements entre les acteurs financiers.
- Les méthodes de communication et de coopération en cas d'incident ou de crise.
- Le rôle des autorités de surveillance et des organisations des marchés financiers.

4) Réévaluation et amélioration continue

- L'importance de la réévaluation et de l'amélioration continue du cadre de gestion de la résilience opérationnelle.
- La mise en place de processus de suivi et d'indicateurs de performance.
- Les audits internes et externes pour garantir la conformité à DORA.
- Les bonnes pratiques en matière de résilience opérationnelle.
- L'évolution future de la réglementation et les questions émergentes.
- Les attentes et les défis liés à la mise en place de DORA.

5) Certification

- Domaines de compétences couverts par l'examen :
- Domaine 1 : Concepts fondamentaux de la gestion des risques liés aux TIC et de la résilience opérationnelle numérique.
- Domaine 2 : Préparation et planification pour la mise en œuvre du projet DORA.
- Domaine 3 : Gestion des risques et incidents liés aux TIC.
- Domaine 4 : Tests de la résilience opérationnelle numérique et gestion des risques liés aux prestataires tiers des TIC.
- Domaine 5 : Réévaluation et amélioration continues.

LES DATES

CLASSE À DISTANCE

2025 : 24 févr., 23 juin, 08 sept.,
17 nov.