Date de publication : 14/10/2024

Formation : DORA (Digital Operational Resilience Act), stratégie de mise en oeuvre

Séminaire - 2j - 14h00 - Réf. DRA
Prix : 2120 CHF H.T.

4,1 / 5

Le référentiel DORA est un cadre réglementaire européen visant à renforcer la résilience opérationnelle des entités financières face aux risques liés aux technologies de l'information et de la cybersécurité. Il impose des exigences strictes en matière de gestion des risques IT, de tests de cybersécurité, de gestion des incidents, et de résilience des infrastructures critiques. En harmonisant les standards à l'échelle de l'UE, DORA assure une protection accrue contre les cybermenaces, limitant les interruptions des services financiers et renforçant la confiance numérique.

Objectifs pédagogiques

À l'issue de la formation, le participant sera en mesure de :

- Comprendre les principaux objectifs et concepts clés du règlement DORA
- Connaître les différents types de cyber-risques
- Identifier les obligations en matière de sécurité des données et de conformité réglementaire
- Appréhender les bonnes pratiques de sécurité numérique et sensibiliser les collaborateurs
- Mettre en place et établir une stratégie de résilience numérique

Public concerné

RSSI et référents sécurité, architectes sécurité, directeurs et responsables informatiques, ingénieurs IT, chefs de projet (MOE, MOA), auditeurs de sécurité et juristes réglementaires IT.

Prérequis

Connaissances de base en cybersécurité et sécurité des systèmes d'information.

Vérifiez que vous avez les prérequis nécessaires pour profiter pleinement de cette formation en faisant ce test.

PARTICIPANTS

RSSI et référents sécurité, architectes sécurité, directeurs et responsables informatiques, ingénieurs IT, chefs de projet (MOE, MOA), auditeurs de sécurité et juristes réglementaires IT.

PRÉREQUIS

Connaissances de base en cybersécurité et sécurité des systèmes d'information.

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.

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.

Programme de la formation

1 Gestion des risques liés aux technologies de l'information et de la communication (TIC)

- Dispositions DORA rappelant la nécessité de mettre en œuvre un dispositif de gestion des risques liés aux TIC.
- Principes et exigences clés en matière de gestion des risques des entités financières.
- Obligations relatives au cadre de gestion des risques liés aux TIC.

2 Gestion, classification et déclaration des incidents liés aux TIC

- Dispositions du règlement DORA visant à harmoniser et à rationaliser la notification des incidents liés aux TIC.
- Classification et notification des incidents liés aux TIC.
- Notification aux autorités compétentes AES (Autorités européennes de surveillance) des incidents majeurs liés aux TIC.
- Notification, à titre volontaire, des cybermenaces importantes aux autorités comme l'EBA, l'EIOPA et l'ESMA.

3 Les tests de résilience opérationnelle numérique

- Tests de résilience opérationnelle numérique sur les parties les plus critiques de leur système d'information.
- Tests avancés basés sur des tests de pénétration fondés sur la menace (Threat-Led Penetration Testing – TLPT).
- Tests en direct à grande échelle sur les menaces, effectués par des organismes testeurs indépendants.

4 Gestion des risques liés aux prestataires tiers de services

- Principes relatifs à la gestion des risques liés aux tiers dans le cadre de la gestion des risques liés aux TIC.
- Dispositions à prendre en compte dans la relation avec les prestataires de services tiers fournissant des services TIC.
- Cadre de surveillance à l'échelle européenne pour les prestataires tiers critiques de services TIC.

5 Dispositions relatives à l'échange d'informations

- Renforcer la résilience opérationnelle numérique des entités financières.
- Échange volontaire d'informations et de renseignements sur les cybermenaces entre les différentes entités financières.

Dates et lieux

CLASSE À DISTANCE

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 formations pratiques, études de cas ou présentation de cas réels pour les séminaires de formation.
• À l'issue de chaque formation 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 participant 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

Pour toute question ou besoin relatif à l'accessibilité, vous pouvez joindre notre équipe PSH par e-mail à l'adresse psh-accueil@orsys.fr.

2026 : 28 mai, 13 oct., 26 nov.