Continuité, résilience et reprise

DORA (Digital Opérationnel Résilience Act), mettre en place une stratégie de résilience numérique

Vous allez apprendre à

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

Public visé

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

Les Objectifs de la formation

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

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.

Les prérequis de la formation

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

Programme de la formation

Module 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.

Module 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.

Module 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

Module 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.

Module 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.

2 Jours
14 Heures

2 090 € HT

+33 1 89 62 34 30

formation@acgcybersecurity.fr

Campus Cyber, Tour Eria, 5 Rue Bellini 92800 Puteaux, FRANCE

Toutes nos formations sont accessibles aux personnes en situation de handicap.