+33 (0)1 48 10 09 46
formation@ambient-it.net
140 Avenue Jean Lolive 93500 Pantin - France

Mis à jour le 16/01/2025

S'inscrire

Formation : DORA Digital Operational Resilience Act

2 jours (14 heures)

Présentation

Notre formation Digital Operational Resilience Act (DORA) vous permettra de maitriser les tenants et les aboutissants de cette nouvelle réglementation européenne et ainsi vous assurer du bon respect de celle-ci dans votre organisation. Les institutions financières doivent désormais suivre tout un ensemble de règles autour des incidents liés aux nouvelles technologies.

Notre programme vous permettra de comprendre en détail le contexte législatif de l'Union européenne ainsi que les institutions impliquées dans son application. Vous y verrez comment établir un cadre de gestion des risques TIC, les méthodes de détection, les réponses aux incidents et la récupération après un sinistre.

Notre formation vous permettra également de conduire des tests de résilience au sein de votre organisation. Vous y apprendrez le rôle crucial des testeurs dans les tests de pénétration guidés par les menaces (TLPT).

Enfin, le rôle des autorités compétentes et la coopération intersectorielle seront abordés ainsi que la protection des données et le secret professionnel dans le DORA.

Objectifs

- Comprendre les principes du DORA
- Appliquer la réglementation dans son organisation
- Conduire des tests de résilience

Public visé

- **CEO**
- Chefs de projets
- Managers
- DPO

Pré-requis

- Connaissance du secteur des institutions financières

PROGRAMME DE NOTRE FORMATION Digital Operational Resilience Act

INTRODUCTION ET CONTEXTE LÉGISLATIF DE L'UE

- Présentation du Digital Operational Resilience Act (DORA) et de son importance
- Comprendre le processus législatif de l'Union Européenne
- Les institutions clés impliquées dans la création de DORA
- Relation entre DORA et d'autres régulations comme la directive NIS 2
- Vue d'ensemble des actes législatifs européens et leur impact sur DORA

GESTION DES RISQUES TIC

- Établissement d'un cadre de gestion des risques TIC
- Identification, protection et prévention
- Méthodes de détection, réponse et récupération
- Importance des politiques de sauvegarde et des procédures de restauration
- Communication et harmonisation des outils de gestion des risques TIC

GESTION DES INCIDENTS LIÉS AUX TIC

- Processus de gestion des incidents liés aux TIC et classification des incidents
- Reporting des incidents majeurs et notification des menaces cybersignificatives
- Harmonisation des contenus de reporting et templates
- Implications des feedbacks de supervision en cas d'incidents

TESTS DE RÉSILIENCE OPÉRATIONNELLE NUMÉRIQUE

- Exigences générales pour la performance des tests de résilience
- Tests avancés des outils TIC et systèmes
- Importance et rôle des testeurs dans les tests de pénétration guidés par les menaces (TLPT)

GESTION DES RISQUES LIÉS AUX TIERS TIC

- Principes de gestion des risques liés aux tiers TIC
- Évaluation des risques de concentration TIC et dispositions contractuelles essentielles
- Cadre de surveillance des prestataires de services TIC tiers critiques
- Rôles et pouvoirs des surveillants principaux dans le cadre de la surveillance

COOPÉRATION, SANCTIONS ET DISPOSITIONS FINALES

- Rôles des autorités compétentes et coopération intersectorielle
- Exercices financiers transsectoriels et communication
- Mesures de remédiation et sanctions administratives
- Clauses de révision et dispositions transitoires de DORA
- Protection des données et secret professionnel dans le cadre de DORA

FAQ – QUESTIONS / RÉPONSES

Pourquoi la règlementation DORA est devenue nécessaire ?

Avec la multiplication des technologies dans le secteur financier, les failles de vulnérabilités sont devenues également plus nombreuses. Une mauvaise gestion des risques peut avoir des conséquences catastrophiques sur l'économie globale. C'est pour garantir une résilience du secteur financier à l'échelle européenne que la réglementation DORA a été créée.

Comment se déroule la formation DORA ?

Notre formation couvre évidemment les aspects théoriques nécessaires au bon apprentissage de la réglementation, mais elle comporte également des QCM et des mises en situation pour garantir le bon apprentissage de toutes les notions vues.

Que va m'apporter cette Formation DORA ?

À l'issue de cette formation, vous serez en mesure de faire appliquer et de diriger un cadre de gestion des risques liés aux TIC en totale conformité avec les exigences DORA.

Sociétés concernées

Cette formation s’adresse à la fois aux particuliers ainsi qu’aux entreprises, petites ou grandes, souhaitant former ses équipes à une nouvelle technologie informatique avancée ou bien à acquérir des connaissances métiers spécifiques ou des méthodes modernes.

Positionnement à l'entrée en formation

Le positionnement à l'entrée en formation respecte les critères qualité Qualiopi. Dès son inscription définitive, l'apprenant reçoit un questionnaire d’auto-évaluation nous permettant

d’apprécier son niveau estimé sur différents types de technologies, ses attentes et objectifs personnels quant à la formation à venir, dans les limites imposées par le format sélectionné. Ce questionnaire nous permet également d’anticiper certaines difficultés de connexion ou de sécurité interne en entreprise (intraentreprise ou classe virtuelle) qui pourraient être problématiques pour le suivi et le bon déroulement de la session de formation.

Méthodes pédagogiques

Stage Pratique : 60% Pratique, 40% Théorie. Support de la formation distribué au format numérique à tous les participants.

Organisation

Le cours alterne les apports théoriques du formateur soutenus par des exemples et des séances de réflexions, et de travail en groupe.

Validation

À la fin de la session, un questionnaire à choix multiples permet de vérifier l’acquisition correcte des compétences.

Sanction

Une attestation sera remise à chaque stagiaire qui aura suivi la totalité de la formation.