

Formation DORA, Résilience opérationnelle numérique

Présentation

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.

Durée : 14,00 heures (2 jours)

Tarif INTRA : Nous consulter

Objectifs de la formation

A l'issue de la formation, le stagiaire sera capable de prendre en compte les exigences réglementaires du référentiel DORA en matière de résilience numérique.

- Connaître la réglementation DORA
- Savoir mettre en place les mesures de conformité
- Anticiper les impacts opérationnels dans son organisation

Prérequis

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

Public

RSSI, DSI, ingénieurs IT, chefs de projet, auditeurs de sécurité et juristes réglementaires IT ou toute autre personne impliquée dans la sécurité de son organisation

Programme de la formation



Jour 1

- Présentation du cadre réglementaire DORA : piliers fondamentaux et périmètre d'application.
- Analyse des impacts concrets sur l'organisation et ses métiers.
- Cartographie des obligations DORA.
- Mise en perspective avec les normes ISO 27001, ISO 22301 et les systèmes de management internes (SMI).
- Approche intégrée de la gouvernance de la résilience numérique.

Fil rouge en partant d'un cas fictif d'entreprise : cartographier en sous-groupe les impacts DORA sur plusieurs métiers (IT, projets, juridique)

Module 2 : Gestion des risques TIC et identification des prestations critiques (PCI)

- Application des articles 5 à 9 du règlement DORA relatifs à la gestion des risques TIC.
- Méthodologie d'identification des Prestations Critiques d'Importance (PCI).
- Évaluation des risques basée sur l'usage métier et la dépendance client (et non la technologie seule).
- Corrélation entre PCI, DSI, directions métiers, contrats clients, PCA/PRA.

Fil rouge en partant d'un cas fictif d'entreprise : identifier les PCI de cette entreprise et évaluer les risques associés

Module 3 : Identification et notification des incidents liés aux TIC

- Application des articles 17 à 20 de DORA concernant les incidents TIC.
- Identification d'un incident majeur selon les critères réglementaires.
- Déclinaison du processus de notification : délais, rapports initiaux, intermédiaires et finaux.
- Répartition des responsabilités : organisation, client, autorité régulatrice.

Fil rouge en partant d'un cas fictif d'entreprise : dans le cas d'un incident majeur, qualifier l'incident et préparer le rapport de notification en sous-groupe, puis débrief collectif en intégrant les exigences DORA

Jour 2

- Mise en œuvre d'un programme de test de résilience numérique (articles 24 à 27 de DORA).

- Priorisation des actifs critiques à tester selon l'approche TIBER-EU, Red Team, etc.
- Typologie des tests, critères de sélection et indicateurs clés de pilotage.
- Alignement avec les exigences ISO 22301, bonnes pratiques ANSSI PIA/PRA.

Module 5 : Audit des prestataires et contractualisation DORA

- Approfondissement des articles 28 à 31 de DORA relatifs à la sous-traitance.
- Introduction aux principes de l'ISO 19011 pour la réalisation d'audits internes/externes.
- Analyse des avenants contractuels et identification des écarts de conformité.
- Méthodologie d'audit des prestataires de services TIC et suivi des engagements contractuels.

Fil rouge en partant d'un cas fictif d'entreprise : analyse d'un test pour identifier les points forts et les pistes d'amélioration

Module 6 : Échange sécurisé d'informations sur les cybermenaces

- Mise en place d'un dispositif d'échange volontaire d'informations sur les menaces, conformément aux articles 14 à 16 de DORA.
- Typologie des menaces et définition des responsabilités croisées entre acteurs.
- Utilisation de canaux sécurisés et respect des normes ISO 27010, RGPD et exigences DORA.
- Promotion d'une culture de coopération inter-entreprises pour renforcer la résilience collective.

Fil rouge en partant d'un cas fictif d'entreprise : définir les règles d'un accord d'échange sécurisé d'informations entre entreprises

Module 7 : Bilan de la formation

- Questions / Réponses
- Elaboration d'une feuille de route individuelle : priorités d'actions pour engager son organisation

E-learning « Tout comprendre sur le règlement DORA » mis à disposition post-formation et consultable pendant 1 mois pour renforcer ou réviser ses connaissances (e-learning de 40 minutes)

Organisation

Formateur

Les formateurs de Docaposte Institute sont des experts de leur domaine, disposant d'une expérience terrain qu'ils enrichissent continuellement. Leurs connaissances techniques et pédagogiques sont rigoureusement validées en amont par nos référents internes. Riches de leur expérience sur le sujet, ils sauront accompagner vos collaborateurs dans leur montée en compétences.

Moyens pédagogiques et techniques

- Alternance d'apports théoriques et de mises en pratique contextualisées.
- Progression pédagogique structurée, de la compréhension à la mise en œuvre opérationnelle.
- Pédagogie immersive favorisant une mise en application immédiate des compétences.
- Formation interactive et participative s'appuyant sur des ateliers pratiques, études de cas et échanges collectifs (+ 60 % du temps de formation.)
- Séquences pédagogiques rythmées et évaluations formatives régulières pour renforcer l'ancrage des apprentissages.
- Supports de cours, ressources documentaires et références mis à disposition par le formateur

Dispositif de suivi de l'exécution et de l'évaluation des résultats de la formation

En amont de la formation *(évaluation en ligne dans l'extranet apprenant)*

- Recueil des besoins et des attentes des participants.
- Auto-positionnement permettant d'évaluer le niveau initial des apprenants.

Tout au long de la formation

- Évaluations continues réalisées par le formateur à travers des questions orales, exercices, QCM, études de cas et mises en situation pratiques.

À l'issue de la formation *(évaluations en ligne dans l'extranet apprenant)*

- Auto-positionnement afin de mesurer l'acquisition des compétences visées.

- Validation de l'acquisition des compétences par le formateur
- Questionnaire de satisfaction « à chaud » à l'issue de la formation
- Questionnaire de satisfaction "à froid", 45 jours après la formation afin d'évaluer l'ancrage des acquis et leur mise en application en situation professionnelle.

Accessibilité

Nos formations peuvent être adaptées à certaines conditions de handicap. Nous contacter pour toute information et demande spécifique.