DAWAN

Plan de la formation

www.dawan.fr

Formation Se préparer à l’implémentation du règlement DORA

Durée :	1 jours (7 heures)
Tarifs inter-entreprise :	875,00 € HT (standard) 700,00 € HT (remisé)
Public :	RSSI / CISO - Responsables conformité - DSI et responsables sécurité des organismes concernés par NIS2
Pré-requis :	Bonne compréhension des enjeux de cybersécurité et de la gestion des risques SI dans un contexte financier
Objectifs :	Comprendre le cadre, les principes et les exigences du règlement DORA (Digital Operational Resilience Act) - Acquérir une vision structurée de la gestion des risques TIC, de la réponse aux incidents et de la résilience opérationnelle dans le secteur financier - Savoir réaliser un premier état des lieux de la situation de son entreprise au regard de DORA - Identifier les écarts et définir les grandes lignes d’un plan d’actions de mise en conformité DORA
Modalités pédagogiques, techniques et d’encadrement :	• Formation synchrone en présentiel et distanciel. • Méthodologie basée sur l’Active Learning : 75 % de pratique minimum. • Un PC par participant en présentiel, possibilité de mettre à disposition en bureau à distance un PC et l’environnement adéquat. • Un formateur expert.
Modalités d’évaluation :	• Définition des besoins et attentes des apprenants en amont de la formation. • Auto-positionnement à l'entrée et la sortie de la formation. • Suivi continu par les formateurs durant les ateliers pratiques. • Évaluation à chaud de l'adéquation au besoin professionnel des apprenants le dernier jour de formation.

Sanction :	Attestation de fin de formation mentionnant le résultat des acquis
Référence :	CYB102755-F
Note de satisfaction des participants:	Pas de données disponibles
Contacts :	commercial@dawan.fr - 09 72 37 73 73
Modalités d'accès :	Possibilité de faire un devis en ligne (www.dawan.fr, moncompteformation.gouv.fr, maformation.fr, etc.) ou en appelant au standard.
Délais d'accès :	Variable selon le type de financement.
Accessibilité :	Si vous êtes en situation de handicap, nous sommes en mesure de vous accueillir, n'hésitez pas à nous contacter à referenthandicap@dawan.fr, nous étudierons ensemble vos besoins

Situer le règlement DORA dans le paysage réglementaire financier

Présenter le contexte du Digital Operational Resilience Act et ses objectifs
Comprendre les liens entre DORA, NIS2, le RGPD et les autres textes applicables au secteur financier
Identifier les catégories d'entités financières concernées et les prestataires TIC critiques
Analyser les enjeux de résilience opérationnelle numérique pour les acteurs financiers
Atelier fil rouge : cartographier rapidement les textes clés s'appliquant à son organisme et situer DORA dans cet ensemble

Comprendre le périmètre, les principes et les exigences clés de DORA

Identifier les domaines couverts par DORA : gestion des risques TIC, incidents, tests de résilience, risques liés aux tiers, information sharing
Clarifier les obligations de gouvernance : rôle des organes de direction, intégration du risque TIC dans la gestion globale des risques
Comprendre les notions de résilience opérationnelle numérique et de tolérance aux perturbations
Repérer les grandes différences de logique entre une directive (NIS2) et un règlement directement applicable (DORA)
Atelier fil rouge : à partir d'un résumé des exigences, relier chaque domaine DORA à des pratiques existantes ou à créer

Organiser la gestion des risques TIC, des incidents et des tests de résilience

Structurer un cadre de gestion des risques TIC conforme à DORA : identification, évaluation, traitement et suivi
Mettre en place des processus de gestion et de notification des incidents TIC significatifs
Comprendre les exigences en matière de tests de résilience (tests techniques, scénarios, tests avancés pour certaines entités)
Intégrer les enseignements des incidents et des tests dans l'amélioration continue du dispositif de sécurité et de résilience
Atelier fil rouge : esquisser un cycle de gestion des incidents et des tests de résilience conforme à l'esprit de DORA

Prendre en compte les risques liés aux prestataires TIC et à la chaîne de valeur

Identifier les prestataires TIC critiques et les dépendances clés pour la continuité des services financiers
Analyser les exigences DORA en matière de contrats, de supervision et de gestion du risque de tiers
Prévoir des mécanismes de suivi, de reporting et, le cas échéant, de sortie ou de substitution de prestataires
Articuler les exigences DORA avec les pratiques existantes de gestion des fournisseurs et des sous-traitants
Atelier fil rouge : dresser une première liste de prestataires TIC critiques et identifier les actions prioritaires de mise en conformité

Élaborer un premier plan d'actions de mise en conformité DORA

Réaliser un état des lieux simplifié de la maturité de l'organisation par rapport aux exigences DORA
Identifier les écarts majeurs : gouvernance, gestion des risques TIC, gestion des incidents, tests, tiers, documentation
Définir les grands chantiers de mise en conformité et les responsabilités associées
Structurer un plan d'actions priorisé et un calendrier indicatif de mise en œuvre
Atelier fil rouge final : formaliser une feuille de route DORA synthétique à présenter à la direction risques / conformité / DSI