DAWAN

Plan de la formation

www.dawan.fr

Formation DORA – Mise en œuvre avancée de la résilience opérationnelle numérique

Durée :	2 jours (14 heures)
Tarifs inter-entreprise :	1 575,00 € HT (standard) 1 260,00 € HT (remisé)
Public :	RSSI / CISO du secteur financier - Responsables conformité / risques opérationnels - DSI, responsables IT ou responsables de la résilience opérationnelle dans les entités financières ou leurs prestataires TIC
Pré-requis :	Bonne connaissance des fondamentaux de la cybersécurité et des enjeux réglementaires du secteur financier. Avoir suivi la formation « Se préparer à l'implémentation du règlement DORA » ou disposer d'un niveau équivalent est vivement recommandé.
Objectifs :	Approfondir la compréhension opérationnelle du règlement DORA et de ses exigences - Structurer un cadre de gestion des risques TIC conforme à DORA - Concevoir des processus de gestion et de notification des incidents TIC significatifs - Mettre en place un dispositif de tests de résilience opérationnelle numérique adapté à son organisation - Piloter les risques liés aux prestataires TIC et aux fournisseurs critiques - Définir des indicateurs, tableaux de bord et preuves de conformité pour les organes de direction et les autorités
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 :	CYB102756-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

Structurer le programme DORA dans l’organisation

Clarifier les responsabilités des organes de direction et des fonctions clés dans la mise en œuvre de DORA
Définir le périmètre d’application : entités juridiques, services, systèmes et prestataires concernés
Positionner le programme DORA par rapport aux dispositifs existants (gestion des risques, PCA/PRA, sécurité, conformité)
Organiser la gouvernance du projet : comités, rôles, instances de validation et de suivi
Atelier fil rouge : formaliser une fiche de cadrage “programme DORA” pour un établissement financier ou un cas d’école

Construire le cadre de gestion des risques TIC conforme à DORA

Revoir les attentes de DORA en matière de gestion des risques TIC et de résilience opérationnelle numérique
Cartographier les actifs TIC essentiels : systèmes, données, processus métiers, interconnexions, dépendances externes

Définir une méthodologie de gestion des risques TIC alignée sur DORA : identification, évaluation, traitement, suivi
Intégrer les risques TIC dans le dispositif global de gestion des risques de l'entreprise (appétence, seuils, reporting)
Atelier fil rouge : réaliser une analyse de risques TIC simplifiée sur un service critique et définir les options de traitement

Concevoir les processus de gestion et de notification des incidents TIC

Traduire les exigences DORA en processus concrets de gestion des incidents TIC significatifs
Définir les critères de criticité, les seuils de notification et les circuits d'escalade internes
Organiser la collecte des informations nécessaires : logs, preuves, catégorisation, chronologie des événements
Préparer la notification aux autorités compétentes : délais, contenu, interlocuteurs, coordination avec la conformité
Atelier fil rouge : dessiner un workflow de gestion d'un incident TIC majeur et rédiger une trame de notification conforme à l'esprit de DORA

Mettre en place les tests de résilience opérationnelle numérique

Comprendre les différentes catégories de tests de résilience exigées par DORA (tests techniques, scénarios, tests avancés)
Identifier les systèmes, services et processus à prioriser pour les tests de résilience opérationnelle
Concevoir des scénarios de tests réalistes : pannes TIC, cyberattaques, indisponibilité de prestataire, perte de données
Articuler les tests DORA avec les exercices existants (PCA/PRA, gestion de crise, simulations cyber)
Atelier fil rouge : construire un plan de tests de résilience pour un périmètre TIC donné, incluant objectifs, scénarios et critères de succès

Piloter les risques liés aux prestataires TIC et aux fournisseurs critiques

Identifier les prestataires TIC critiques au sens de DORA et leurs services associés
Intégrer les exigences DORA dans les contrats : clauses de sécurité, continuité, audit, réversibilité
Mettre en place un dispositif de suivi des prestataires : indicateurs, revues de performance, rapports de conformité
Prévoir des stratégies de sortie et de substitution en cas de défaillance ou de non-

conformité d’un prestataire critique
Atelier fil rouge : établir une fiche de gestion des risques pour un prestataire TIC critique, incluant exigences, contrôles et plans de secours

Définir les indicateurs, tableaux de bord et preuves de conformité DORA

Déterminer les indicateurs clés liés aux risques TIC, aux incidents, aux tests de résilience et aux prestataires
Construire des tableaux de bord à destination des organes de direction et des fonctions risques / conformité
Identifier les preuves de conformité à conserver : politiques, analyses de risques, rapports d’incidents, comptes rendus de tests
Organiser l’archivage et la traçabilité pour répondre aux demandes des autorités de supervision
Atelier fil rouge : concevoir un mini-tableau de bord DORA et une checklist de preuves à maintenir à jour

Inscrire DORA dans la durée : amélioration continue et culture de résilience

Mettre en place un cycle d’amélioration continue : bilans annuels, revues des risques TIC, actualisation des plans
Articuler DORA avec les programmes de sensibilisation internes et la culture de résilience numérique
Tracer les décisions, arbitrages et plans d’actions pour renforcer la responsabilité et la transparence
Définir un plan de progression pour les équipes (formations complémentaires, exercices, retours d’expérience)
Atelier fil rouge final : élaborer une feuille de route sur 12 à 24 mois pour faire vivre le dispositif DORA au-delà du seul projet de conformité