Mise à jour : 01/03/2026

FORMATION : DORA (Digital Operational Resilience Act)

PUBLIC	Cette formation est à destination des RSSI, Responsables informatiques, Ingénieurs IT, Chefs de projet, Architectes sécurité, Auditeurs de sécurité et Juristes réglementaires IT.
PRÉREQUIS	Prérequis : ▪ Avoir les connaissances de base en cybersécurité et sécurité des systèmes d'information. ▪ Aucune expertise technique approfondie requise. Matériel requis : ▪ Ordinateur portable avec accès Internet, accès administrateur pour les ateliers. ▪ Accès au système d'information (SI) de l'organisation (optionnel mais recommandé pour les ateliers).
MODALITÉS ET DÉLAIS D'ACCÈS	En présentiel : ⇨ Formation en présentiel : lieu de formation communiqué en amont de la formation. ⇨ Inscription à réaliser 1 mois avant le démarrage de la formation. En distanciel : ⇨ Formation individuelle ou collective à distance sous la forme de visioconférence participative. ⇨ Inscription à réaliser 1 mois avant le démarrage de la formation.
DURÉE	28H pour une période de 4 jours
DATES	À définir avec l'organisme de formation
HORAIRES	⇨ Les horaires de formation sont : 9H à 12H et de 13H à 17H ⇨ Le monitoring et l'assistance pédagogique sont disponibles du lundi au vendredi de 9H à 18H.
LIEU	En présentiel : ⇨ Sur site ⇨ Au siège de Tricolor Expertise ⇨ Autre adresse En distanciel : ⇨ Formation à distance – visioconférence **Pour les personnes en situation de handicap : Nous adaptons nos formations en fonction de votre handicap et nous mettrons tout en œuvre pour vous accueillir ou pour vous réorienter si besoin.** **Vous pouvez nous contacter au 06 34 31 28 65**
TARIF	3 250€ par personne
NOMBRE DE PARTICIPANTS	En présentiel : Jusqu'à 12 personnes En distanciel : Jusqu'à 5 personnes
OBJECTIF DE LA FORMATION ET COMPÉTENCES VISÉES	À l'issue de la formation, le participant sera capable de mettre en œuvre les compétences suivantes : ▪ Comprendre pourquoi DORA existe et ce qu'il change. ▪ Mettre en place une gouvernance conforme aux exigences DORA. ▪ Mettre en place un dispositif de gestion et de notification des incidents. ▪ Concevoir et mettre en œuvre un programme de tests conforme à DORA. ▪ Maîtriser les exigences DORA sur la gestion des tiers, notamment les fournisseurs cloud. ▪ Intégrer le partage d'informations dans la stratégie de résilience. ▪ Construire et piloter un programme de mise en conformité DORA.
MODALITÉS D'ÉVALUATION D'ATTEINTE DES OBJECTIFS DE LA FORMATION	⇨ Évaluation individuelle du profil, des attentes et des besoins du participant avant le démarrage de la formation ⇨ Évaluation des connaissances & compétences en début et en fin de formation via un QCM ⇨ Tests de contrôle de connaissances et validation des acquis à chaque étape ⇨ Travaux pratiques et mises en situation ⇨ Echange avec le formateur ou la formatrice par visioconférence (webinar), téléphone et mail ⇨ Questionnaire d'évaluation de la satisfaction en fin de formation

CONTENU	Dans cette formation, le participant aura accès au programme suivant :	
	MODULE 1	**Contexte et fondements de DORA (4h)** 1. Historique et contexte réglementaire européen : de la directive NIS à NIS2, en passant par TIBER-E 2. Les crises systémiques dans le secteur financier liées au numérique 3. Objectifs du règlement : harmonisation, résilience opérationnelle numérique 4. Champ d'application : entités concernées (banques, assurances, PSP, CCP, PSTN, gestionnaires d'actifs…) 5. Relations avec d'autres réglementations : RGPD, NIS2, Bâle III, Solvabilité II 6. Calendrier d'entrée en vigueur et rôle des autorités de supervision (BCE, EIOPA, ESMA, ABE)
	MODULE 2	**Gouvernance et cadre de gestion du risque ICT (4h)** 1. Le cadre de gestion du risque lié aux TIC (ICT Risk Management Framework) 2. Responsabilités de l'organe de direction : rôle du conseil d'administration et de la direction génér 3. La stratégie de résilience numérique : définition, documentation, révision annuelle 4. Politiques et procédures attendues par DORA 5. Identification et classification des actifs TIC critiques 6. Tolérance au risque, appétit au risque et indicateurs de suivi (KRI) Atelier pratique : cartographie des responsabilités et rédaction d'une politique ICT
	MODULE 3	**Gestion des incidents liés aux TIC (4h)** 1. Définitions : incident TIC, incident majeur, cybermenace significative 2. Critères de classification des incidents selon les RTS (Regulatory Technical Standards) 3. Processus de gestion des incidents : détection, enregistrement, classification, notification, résolutio 4. Les délais et formats de notification aux autorités compétentes (rapport initial, intermédiaire, final 5. Notification volontaire des cybermenaces 6. Coordination avec les CSIRT nationaux et les autorités (BCE, ACPR, AMF…) Atelier pratique : simulation de classification et de notification d'un incident majeur
	MODULE 4	**Tests de résilience opérationnelle numérique (4h)** 1. Les différents types de tests prévus par DORA : tests de base vs tests avancés (TLPT) 2. Tests de base : revues, analyses de vulnérabilités, tests d'intrusion, scénarios de continuité 3. Threat-Led Penetration Testing (TLPT) : principes, périmètre, fréquence (tous les 3 ans) 4. Référentiel TIBER-EU et son alignement avec DORA 5. Rôle des prestataires tiers dans les TLPT 6. Critères d'exemption et proportionnalité selon la taille de l'entité Atelier pratique : construction d'un plan de tests pluriannuel
	MODULE 5	**Gestion du risque lié aux prestataires tiers TIC (4h)** 1. Le risque de concentration tiers : enjeux systémiques 2. Registre des contrats TIC : contenu obligatoire, mise à jour, transmission aux superviseurs 3. Exigences contractuelles minimales imposées par DORA (clauses obligatoires) 4. Due diligence : évaluation initiale et continue des prestataires critiques 5. Stratégie de sortie : réversibilité, plans de transition 6. Le cadre de supervision directe des prestataires tiers critiques (CTPPs) par les ESAs Atelier pratique : audit d'un contrat cloud au regard des exigences DORA
	MODULE 6	**Partage d'informations et intelligence sur les menaces (4h)** 1. Le cadre de partage d'informations prévu par l'article 45 de DORA 2. Communautés de partage : ISAC financiers (FS-ISAC, CERT-FIN…), arrangements entre entités 3. Threat Intelligence : définition, cycle de vie, standards (STIX/TAXII, MISP) 4. Cas d'usage : détection précoce, amélioration des scénarios de tests, réponse coordonnée 5. Conditions de participation : confidentialité, protection des données, gouvernance 6. Articulation avec NIS2 et les obligations de signalement

		Atelier pratique : analyse d'un rapport de threat intelligence et utilisation pour un scénario TLPT
	MODULE 7	**Mise en conformité, supervision et feuille de route (4h)** 1. Les normes techniques de réglementation (RTS) et d'exécution (ITS) : état d'avancement et contenu 2. Gap analysis : méthode et outils pour évaluer son niveau de maturité 3. Feuille de route de mise en conformité : priorisation, jalons, ressources 4. Rôle des fonctions clés : RSSI, CRO, DSI, Risk Management, Compliance, Audit interne 5. Supervision par les autorités nationales compétentes (ANC) et les ESAs 6. Sanctions et mesures correctives prévues par DORA 7. Retours d'expérience de premières mises en conformité dans le secteur Atelier final : présentation d'une feuille de route de conformité DORA par groupe
MOYENS PERMETTANT LE SUIVI ET L'APPRÉCIATION DES RÉSULTATS		**Suivi de l'exécution :** ⇨ Feuilles de présences signées par les participants et le formateur ou la formatrice par demi-journée ⇨ Attestation de fin de formation mentionnant les objectifs, la nature et la durée de l'action et les résultats de l'évaluation des acquis de la formation. **Appréciation des résultats :** ▪ Recueil individuel des attentes du stagiaire ▪ Questionnaire d'auto-évaluation des acquis en début et en fin de formation ▪ Évaluation continue durant la session ▪ Remise d'une attestation de fin de formation ▪ Questionnaire d'évaluation de la satisfaction en fin de formation
MOYENS PÉDAGOGIQUES ET TECHNIQUES D'ENCADREMENT DES FORMATIONS		**Modalités pédagogiques :** ▪ Évaluation des besoins et du profil du participant ▪ Apport théorique et méthodologique : séquences pédagogiques regroupées en différents modules ▪ Contenus des programmes adaptés en fonction des besoins identifiés pendant la formation ▪ Réflexion et échanges sur cas pratiques ▪ Questionnaires, exercices, ateliers et étude de cas ▪ Tests de contrôle de connaissances et validation des acquis à chaque étape ▪ Retours d'expériences **Éléments matériels :** ▪ Mise à disposition de tout le matériel pédagogique nécessaire (pour les formations en présentiel) ▪ Support de cours au format numérique projeté sur écran et transmis au participant par mail à la fin de la formation **Référent pédagogique et formateur/formatrice :** Chaque formation est sous la responsabilité de la directrice pédagogique de l'organisme de formation ; le bon déroulement est assuré par le formateur ou la formatrice désigné(e) par l'organisme de formation.