Mise à jour : 17/10/2026

FORMATION : Comprendre la réglementation de l'UE : Cyber Resilience Act

PUBLIC	▪ Professionnels de la cybersécurité voulant comprendre la réglementation européenne. ▪ Dirigeants d'entreprise souhaitant améliorer la sécurité des produits et à répondre aux exigences du marché. ▪ Développeurs, responsables qualité, chefs de produits, ingénieurs sécurité, responsables de la conformité des produits numériques. ▪ Toute personne concernée par les questions de conformité, cybersécurité : DPO, informatique et juridique : reconversion professionnelle, évolution de carrière…
PRÉREQUIS	Prérequis : ▪ Avoir les connaissances de base des concepts de cybersécurité. ▪ Aucune expertise technique approfondie requise. Matériel requis : ▪ Ordinateur portable avec accès Internet, accès administrateur 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	Les tarifs de cette formation (individuel, inter-entreprises, intra) sont consultables à tout moment sur sa fiche en ligne : https://tricolorexpertise.fr/formation-cyber-resilience-act/ Des conditions tarifaires spécifiques peuvent s'appliquer selon le partenaire prescripteur ; elles sont précisées dans le devis et la convention de formation.
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 le cadre, la portée et les objectifs du Cyber Resilience Act. ▪ Identifier les exigences clés en matière de cybersécurité pour les produits numériques. ▪ Appréhender les impacts du Cyber Resilience Act sur la chaîne de fabrication et de distribution. ▪ Découvrir les étapes à suivre pour garantir la conformité des produits aux normes du Cyber Resilience Act. ▪ Préparer la mise en conformité de ses produits dès la phase de conception/développement et tout au long de leur cycle de vie.

	▪ Développer des compétences pratiques pour créer des produits numériques sécurisés et gérer les vulnérabilités. ▪ Organiser la certification de ses produits et services.
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	**Introduction à la loi européenne sur la cyber-résilience – 1h** • Contexte et historique • Définitions, calendrier et sanctions
MODULE 2	**Connaitre les produits concernés – 2h** • Définitions et PEN • Produits importants, produits critiques et produits exclus
MODULE 3	**Identifier les acteurs concernés – 2h** • Fabriquant, importateur et revendeur
MODULE 4	**Distinguer les différents types de contrôles de conformité – 4h** • Contrôle interne • Contrôle par un organisme notifié de la conception du produit • Contrôle par un organisme notifié du système qualité • Certification de cybersécurité
MODULE 5	**Respecter les obligations du fabricant – 7h** S'assurer du respect des exigences essentielles de cybersécurité : • Être mis sur le marché sans vulnérabilité exploitable connue ; • Comporter une configuration de sécurité par défaut ; • Être conçu de manière que les vulnérabilités puissent être corrigées par des mises à jour de sécurité ; • Assurer une protection face aux accès non autorisés ; • Protéger la confidentialité et l'intégrité des données, au repos ou en transit ; • Assurer la minimisation des données ; • Réduire les répercussions négatives qui pourraient être générées par le produit ; • Limiter les surfaces d'attaques ; • Limiter l'exploitation de failles ; • Enregistrer les activités internes pertinentes ; • Donner la possibilité aux utilisateurs de supprimer leurs données facilement ; Gérer et notifier les vulnérabilités et les incidents graves : • Recenser et documenter les vulnérabilités et les composants du produit ; • Gérer et corriger les vulnérabilités ; • Tester régulièrement du produit ; • Communiquer sur les vulnérabilités corrigées ; • Mettre en place une politique de divulgation coordonnée de vulnérabilité ; • Favoriser le partage d'informations sur les vulnérabilités potentielles du produit et des composants ; • Prévoir des mécanismes de distribution sécurisé des mises à jour ; • Diffuser les correctifs de sécurité sans retard ; • La notification des vulnérabilités activement exploitées (VAE) et des incidents graves ; • Définitions, CSIRT, ENISA et Utilisateurs.

	MODULE 6	**Mettre en place des processus de mise en conformité – 3h** • Mettre en place le cadre de gouvernance • Catégorisation des produits • Sécuriser dès la conception • Mettre en œuvre un cycle de développement sécurisé • Gérer les vulnérabilités • Évaluer la conformité et gérer des incidents • Diffuser une mise à jour de sécurité
	MODULE 7	**Mise en situation – 7h** • Appliquer les méthodes et concepts appris **Livrables : Plan d'action détaillé et processus – 1h** Évaluation : correction des livrables
MOYENS PERMETTANT LE SUIVI ET L'APPRÉCIATION DES RÉSULTATS		<u>Suivi de l'exécution :</u> ⇨ 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. <u>Appréciation des résultats :</u> ▪ 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		<u>Modalités pédagogiques :</u> ▪ 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 <u>Éléments matériels :</u> ▪ 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 <u>Référent pédagogique et formateur/formatrice :</u> 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.