Mise à jour : 01/03/2026

FORMATION : Fondamentaux de la directive NIS2

PUBLIC	▪ Responsables de la sécurité des systèmes d'information (RSSI) ▪ Directeurs IT ▪ Délégués à la protection des données (DPO) ▪ Responsables conformité ▪ Chefs de projet cybersécurité ▪ Chefs d'entreprise & Directions générales
PRÉREQUIS	Prérequis : • Avoir des connaissances de base en cybersécurité et en gouvernance IT. ▪ 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	35h pour une période de 5 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	3 950€ 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 : ▪ Maîtriser l'ensemble du cadre réglementaire NIS2 et ses implications juridiques ▪ Réaliser un audit de conformité complet de leur organisation ▪ Concevoir et déployer une stratégie de mise en conformité NIS2 ▪ Implémenter les mesures techniques et organisationnelles exigées ▪ Gérer l'ensemble du cycle de vie des incidents de sécurité ▪ Piloter la gouvernance cybersécurité selon les standards NIS2 ▪ Former et sensibiliser les parties prenantes internes

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 :

JOUR 1

Fondamentaux et Cadre Réglementaire

Module 1 : Introduction et Contexte Stratégique (3h)

Contenu :

- Accueil et présentation des participants
- Évolution de la menace cyber en Europe (2020-2025)
- Historique : de NIS1 à NIS2, retour d'expérience
- Analyse des incidents majeurs ayant motivé NIS2
- Objectifs politiques et économiques de la directive
- Articulation avec RGPD, DORA, CER et autres réglementations
- Calendrier de transposition et échéances clés
- Activités pratiques :
- Étude de cas : analyse d'incidents cyber récents
- Discussion interactive sur les enjeux stratégiques pour chaque secteur représenté

Module 2 : Cadre Juridique Approfondi (2h30)

Contenu :

- Texte de la directive 2022/2555 : analyse détaillée
- Transposition en droit français
- Autorités compétentes et leur rôle (ANSSI, CSIRT, ministères sectoriels)
- Régime de sanctions : amendes administratives et pénales
- Responsabilité civile et pénale des dirigeants

Module 3 : Périmètre et Assujettissement (2h30)

Contenu :

- Les 18 secteurs hautement critiques et critiques (détail par secteur)
- Critères quantitatifs : seuils d'effectifs et de chiffre d'affaires
- Critères qualitatifs : criticité et importance
- Entités essentielles vs entités importantes : différences d'obligations
- Cas particuliers : groupes, filiales, établissements secondaires
- Extension aux fournisseurs de services numériques
- Chaîne d'approvisionnement et sous-traitance
- Procédure de déclaration et d'enregistrement

Atelier :

- Cartographie approfondie : identification précise du statut de chaque organisation participante
- Exercice de classification sectorielle
- Analyse de la chaîne de valeur et identification des dépendances critiques

JOUR 2

Exigences Techniques et Organisationnelles

Module 4 : Les 10 Mesures de Cybersécurité (3h)

Contenu détaillé de chaque mesure :

- Politiques d'analyse des risques et de sécurité des systèmes d'information
- Gestion des incidents de sécurité
- Continuité d'activité (PCA/PRA) et gestion de crise
- Sécurité de la chaîne d'approvisionnement

		▪ Sécurité lors de l'acquisition, du développement et de la maintenance ▪ Politiques et procédures d'évaluation de l'efficacité des mesures ▪ Pratiques de cyberhygiène et formation ▪ Politiques et procédures relatives à la cryptographie ▪ Sécurité des ressources humaines, contrôle d'accès et gestion des actifs ▪ Utilisation de l'authentification multifacteur et des communications sécurisées Atelier : ▪ Pour chaque mesure, analyse des exigences spécifiques et des moyens de mise en œuvre ▪ Benchmark des bonnes pratiques sectorielles **Module 5 : Analyse et Gestion des Risques (2h30)** Contenu : ▪ Méthodologies d'analyse de risques (EBIOS RM, ISO 27005) ▪ Identification des actifs et des scénarios de menaces ▪ Évaluation de la vraisemblance et de l'impact ▪ Traitement des risques : acceptation, réduction, transfert, évitement ▪ Cartographie des risques cyber ▪ Mise à jour continue et réexamen périodique ▪ Documentation et reporting aux dirigeants Travaux pratiques : ▪ Réalisation d'une analyse de risques simplifiée sur un cas d'étude **Module 6 : Mesures Techniques Avancées (2h30)** Contenu : ▪ Architecture de sécurité : principes Zero Trust ▪ Segmentation réseau et micro-segmentation ▪ Gestion des identités et des accès (IAM/PAM) ▪ Authentification multifacteur : technologies et déploiement ▪ Chiffrement : données au repos et en transit ▪ Détection et réponse ▪ Surveillance continue et SIEM ▪ Tests d'intrusion et Red Team ▪ Gestion des vulnérabilités et patch management ▪ Durcissement des systèmes (hardening) Démonstration : ▪ Présentation d'outils et de plateformes de sécurité ▪ Exemples de tableaux de bord SOC
	JOUR 3	**Gouvernance et Organisation** **Module 7 : Gouvernance de la Cybersécurité (3h)** Contenu : ▪ Modèles de gouvernance cyber (frameworks NIST, ISO 27001, COBIT) ▪ Rôles et responsabilités : RACI détaillé ▪ Positionnement du RSSI dans l'organisation ▪ Responsabilité personnelle des organes de direction ▪ Comité de cybersécurité : composition et fonctionnement ▪ Reporting aux instances dirigeantes ▪ Budget cybersécurité : construction et arbitrage ▪ Indicateurs de pilotage (KPI/KRI) ▪ Tableau de bord cybersécurité pour la direction Atelier : ▪ Construction d'un modèle de gouvernance adapté à différents types d'organisations ▪ Élaboration d'un tableau de bord exécutif

		Module 8 : Politiques et Procédures (2h) Contenu : ▪ Structure documentaire ▪ Politique de sécurité des systèmes d'information (PSSI) ▪ Politiques sectorielles obligatoires ▪ Charte informatique et charte BYOD ▪ Procédures de gestion des comptes et des habilitations ▪ Procédure de gestion des changements ▪ Procédure de classification des données ▪ Gestion du cycle de vie documentaire ▪ Communication et diffusion des politiques Exercice : ▪ Rédaction collaborative d'une politique de sécurité type ▪ Revue critique de documents existants _____ **Module 9 : Ressources Humaines et Sensibilisation (2h)** Contenu : ▪ Cyberhygiène : définition et enjeux ▪ Programme de sensibilisation : conception et déploiement ▪ Formation obligatoire des dirigeants ▪ Parcours de formation différenciés par fonction ▪ Campagnes de phishing simulé ▪ Culture de la cybersécurité ▪ Gestion des départs et des arrivées ▪ Clauses de confidentialité et NDA ▪ Sanctions disciplinaires en cas de manquement Atelier : ▪ Conception d'un plan de sensibilisation annuel ▪ Création de supports de communication (posters, vidéos, e-learning) _____ **Module 10 : Sécurité de la Chaîne d'Approvisionnement (1h30)** Contenu : ▪ Cartographie de la chaîne d'approvisionnement numérique ▪ Évaluation des risques fournisseurs ▪ Clauses contractuelles de sécurité obligatoires ▪ Audits de sécurité des fournisseurs critiques ▪ Gestion des accès des tiers ▪ Surveillance continue des prestataires ▪ Plan de continuité en cas de défaillance fournisseur ▪ Cas particulier du cloud et des services managés Cas pratique : ▪ Évaluation d'un fournisseur critique selon les critères NIS2 ▪ Rédaction de clauses contractuelles NIS2-compliant
	JOUR 4	**Gestion des Incidents et Continuité** **Module 11 : Détection et Réponse aux Incidents (3h)** Contenu : ▪ Définition d'un incident de sécurité selon NIS2 ▪ Architecture de détection : logs, SIEM, SOC ▪ Processus de qualification et de triage ▪ Playbooks de réponse par type d'incident ▪ Containment, éradication et récupération ▪ Post-mortem et retour d'expérience ▪ Amélioration continue du processus Exercice pratique : ▪ Simulation d'incident : détection, analyse et premiers pas de la réponse (2h) ▪ Debriefing et analyse des actions menées

		_____ **Module 12 : Notification Obligatoire aux Autorités (2h30)** Contenu : ▪ Incidents soumis à notification obligatoire : critères précis ▪ Alerte précoce (24h) : contenu et modalités ▪ Rapport d'incident (72h) : éléments requis ▪ Rapport final : délai et contenu ▪ Autorités destinataires ▪ Confidentialité et protection des informations ▪ Coordination avec d'autres obligations (RGPD, etc.) Atelier : ▪ Rédaction d'une notification d'incident en situation réelle _____ **Module 13 : Continuité et Gestion de Crise (2h30)** Contenu : ▪ Bilan d'Impact sur les Activités (BIA) ▪ Identification des activités critiques ▪ Objectifs de reprise (RTO/RPO) ▪ Plan de Continuité d'Activité (PCA) ▪ Plan de Reprise d'Activité (PRA) ▪ Solutions techniques : sauvegarde, réplication, sites de secours ▪ Cellule de crise cyber : composition et activation ▪ Communication de crise interne et externe ▪ Tests et exercices de crise obligatoires ▪ Coordination avec les autorités en situation de crise majeure Exercice pratique : ▪ Simulation de crise cyber (ransomware) avec activation de la cellule de crise ▪ Gestion des communications et des décisions stratégiques
	JOUR 5	**Audit, Mise en Conformité et Pérennisation** **Module 14 : Audit de Conformité NIS2 (3h)** Contenu : ▪ Méthodologie d'audit complète ▪ Collecte de preuves et documentation ▪ Entretiens avec les parties prenantes ▪ Tests techniques de conformité ▪ Gap analysis approfondie ▪ Cotation de la maturité (modèle de maturité cyber) ▪ Rapport d'audit : structure et contenu ▪ Priorisation des non-conformités (criticité et urgence) Atelier pratique : ▪ Les participants réalisent un audit complet de leur organisation (3h) ▪ Identification précise des écarts et construction d'une matrice de conformité ▪ Présentation croisée et retour d'expérience _____ **Module 15 : Plan de Mise en Conformité (2h30)** Contenu : ▪ Méthodologie de gestion de projet de conformité ▪ Priorisation des chantiers ▪ Construction de la roadmap pluriannuelle ▪ Quick wins vs projets structurants ▪ Estimation des charges et des budgets ▪ Allocation des ressources (internes/externes) ▪ Gestion des risques projet ▪ Jalons et livrables clés ▪ Communication du plan aux instances dirigeantes ▪ Tableaux de bord de suivi d'avancement

	Atelier : ▪ Élaboration d'un plan de mise en conformité personnalisé sur 18-24 mois ▪ Préparation d'une présentation pour le COMEX/CODIR _____ **Module 16 : Contrôles et Audits Réglementaires (1h30)** Contenu : ▪ Pouvoirs de contrôle de l'ANSSI et des autorités sectorielles ▪ Déclencheurs d'un contrôle ▪ Déroulement d'un audit réglementaire ▪ Droits et obligations de l'entité contrôlée ▪ Suite donnée aux contrôles : mise en demeure, sanctions ▪ Contestation et recours ▪ Préparation d'un contrôle : bonnes pratiques ▪ Maintien de la conformité dans le temps Cas pratique : ▪ Simulation d'un contrôle de l'ANSSI avec jeux de rôles _____ **Module 17 : Amélioration Continue et Pérennisation (1h30)** Contenu : ▪ Cycle PDCA (Plan-Do-Check-Act) appliqué à NIS2 ▪ Programme d'amélioration continue ▪ Veille réglementaire et technologique ▪ Évolution des menaces et adaptation des mesures ▪ Revues périodiques obligatoires ▪ Tests réguliers (intrusion, continuité, crise) ▪ Mise à jour de la documentation ▪ Retour d'expérience des incidents ▪ Anticipation de NIS3 et évolutions futures ▪ Intégration dans un système de management (ISO 27001, etc.) Discussion : ▪ Partage de bonnes pratiques entre participants ▪ Constitution d'un réseau d'entraide post-formation _____ **Module 18 : Synthèse et Évaluation Finale (1h30)** Contenu : ▪ Récapitulatif des points clés de la formation ▪ Évaluation des connaissances (QCM de 40 questions)
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.
SUIVI POST-FORMATION	Accompagnement : ▪ Session de questions-réponses à 1 mois (webinaire 2h) ▪ Accès à la communauté d'alumni Actualisation des connaissances : ▪ Webinaires trimestriels sur l'actualité NIS2 (option payante)