# Formation « NIS2 Lead Implementer »
# Comprendre et implémenter NIS 2

**Réf : NIS2LI**

## Objectifs

- **Vous doter des connaissances et des compétences nécessaires à la compréhension et à l'implémentation des exigences issues de la directive, vous permettant de planifier, réaliser, gérer, maintenir et mettre à jour votre conformité NIS 2**

## Durée & horaires

- **5 jours soit 35 heures réparties en 31h00 de cours, 2h00 de travail individuel sur les exercices le soir et 3h00 d'examen.**
- **De 9h30 à 13h15 et de 14h15 à 18h00.**

## Nombre de participant

- **Minimum 6 participants – Maximum 24 participants**

## Public visé

- **Professionnel de la cybersécurité ayant à prendre en charge ou à mettre en œuvre la conformité de leur organisme aux exigences issues la directive NIS 2**
- **Décideur soucieux de connaître les exigences issues la directive NIS 2**
- **RSSI et leurs équipes**
- **Personnes responsables de services opérationnels**
- **DSI et leurs équipes**
- **Responsables méthodes et qualité**
- **DPO, DRPO**
- **Juristes et responsables juridiques**

## Pré-requis

- **Avoir une connaissance des principes de sécurité de base (qui ne seront pas réabordés pendant la formation), par exemple avoir suivi la formation SECUCYBER**

## Méthode pédagogique

**La méthode pédagogique se base sur les quatre points suivants :**

- **Un cours magistral fondé sur la directive NIS 2 et ses textes de transposition en droit français (au fur et à mesure de leur adoption), ainsi que sur les textes officiels et normes techniques ayant des interactions fortes avec ce cadre réglementaire (RGPD, DORA, Normes ISO 27XXX, etc.) ;**
- **Enrichi de cas pratiques et d'exemples concrets illustrant les notions explicitées profitant du partage d'expérience des instructeurs HS2 tous avocats ou consultants spécialistes reconnus de ces questions ou implémenteurs des normes 27001 ou encore 27701 ;**
- **Exercices de contrôle des connaissances sur les concepts à connaître pour évaluer le niveau de compréhension et de connaissance ;**
- **Un cas pratique d'implémentation servant de fil rouge à l'ensemble de la formation qui permettra de dérouler un projet complet de mise en conformité.**

## Supports

- **Support de cours au format papier en français**
- **Cahier d'exercices et corrections des exercices**

- **Tous les documents nécessaires à la formation en français ou anglais**
- **Certificat attestant de la participation à la formation**

## Modalité d'évaluation de la formation

- **Fiche d'évaluation remise aux stagiaires à l'issue de la formation afin de recueillir leurs impressions et identifier d'éventuels axes d'amélioration**

## Certification

- **Cette formation prépare à l'examen de certification HS2 NIS 2 Lead Implementer. A l'issue de cette formation, le stagiaire passe l'examen d'une durée de 3h00 en français. L'examen est constitué d'une partie QCM sur les notions de cours et d'une partie rédactionnelle sous forme d'étude de cas.**

## Programme

**Jour 1**

**RGS, LPM, NIS 1 RGPD, DORA, CRA, Cyberscore : contexte et champs d'application de NIS 2**

- Notions juridiques de base et vocabulaire
  - Différence entre Directive et Règlement européen
  - Notion de transpositions et exemple pratique avec NIS 1
- Contexte des réglementations en matière de cybersécurité
  - Évolutions au niveau européen
  - Spécificités issues des lois françaises
  - Données personnelles, données hautement personnelles, notions de données sensibles, données soumises aux secrets : définir pour mieux protéger
- Transposition de NIS 2 en droit français
- A qui s'applique NIS 2 ?
  - Champ d'application direct
  - Champ d'application indirect via l'effet de ruissellement
  - Registre de traitements
- Résumé des principales exigences
  - Notion de formation des dirigeants et des personnels
  - Supervision par l'ANSSI et sanctions
  - Comparatif entre les différentes réglementations et référentiels cybersécurité

**Jour 2**

**Implémenter NIS 2**

- Les processus à mettre en œuvre ou devant évoluer
  - Gouvernance Cybersécurité : rôles et responsabilités, comitologie, implication des décideurs
  - Gestion des relations avec les autorités
  - Gestion des risques et des actifs
  - Gestion de la surveillance, des incidents et des crises
  - Gestion des vulnérabilités et de la conformité techniques
  - Gestion de la chaine d'approvisionnement et des tiers : organisation des responsabilités
  - Gestion de la production et de l'exploitation du système d'information
  - Gestion des développements
  - Gestion de l'audit et des contrôles
  - Gestion de la cryptographie
  - Gestion des ressources humaines
  - Gestion de la sensibilisation et la formation
  - Gestion des identités et des accès
  - Gestion de la résilience et de la continuité d'activité
- La documentation à formaliser ou mettre à jour
  - Politiques de sécurité
  - Exigences vis-à-vis des tiers et Plan d'Assurance Sécurité
  - Programme de contrôles et d'audit
  - Procédures de sécurité
  - Référentiel juridique (détaillée jour 5)

**Jour 3**

**Les principales mesures techniques visées par NIS 2**

- Scénarios d'attaques classiques
- Cartographie des systèmes d'information
- Contrôles d'accès (identification, authentification, droit d'accès, etc.)
- Architecture sécurisée
- Sécurité de l'administration
- Gestion des accès distants
- Journalisation et détection des incidents
- Maintien en condition de sécurité
- Sécurité physique et environnementale
- S'évaluer : les différents types d'audits techniques

**Jour 4**

**Implémenter NIS 2 : La démarche projet autour d'une étude de cas**

- Analyse d'écart : identifier dans l'existant les éléments de conformité, identifier les manques et pouvoir construire et valoriser le plan d'actions
- Présentation des étapes du plan d'actions type
  - Quick-Win vis-à-vis de l'existant
  - Evolution de l'organisation autour de la Cybersécurité
  - Révision de l'appréciation des risques : les scénarios minimums attendus
  - Gérer les évolutions des solutions techniques
  - Mise en œuvre des nouvelles activités
  - Piloter les changements avec les tiers
  - Auditer et contrôler

**Jour 5 matin**

**Implémenter NIS 2 : l'angle juridique**

- Les conséquences sur l'opposabilité des règles en interne : gestion, optimisation ou mise à jour des chartes d'utilisation des outils numériques
  - Cas des salariés
  - Cas des accès privilégiés
  - Respecter la vie privée tout en assurant la cybersécurité : les mécanismes et procédures à mettre en œuvre
  - BYOD et COPE, cloud, réseaux sociaux, décès, IA : intégrer les contraintes
  - Exemples de formulations (et donc de chartes) inapplicables
  - Exigences et cadre des contrôles réalisables
- Les conséquences contractuelles : rapports avec les clients, partenaires et prestataires
  - Choix des prestataires et encadrements contractuels
  - Exigences des régulateurs et de la réglementation dans le rapport avec les prestataires
  - Rendre possible la conformité contractuelle
  - Le cas des clients et des partenaires

**Jour 5 après-midi**

**Examen de certification**