Oo2 Formations & Consulting

# La directive NIS2

## National Information System

Concevoir et gérer un programme de cybersécurité aligné sur la nouvelle réglementation européenne

PECB AUTHORIZED TITANIUM PARTNER

NIS2 Directive

Qualiopi processus certifié

RÉPUBLIQUE FRANÇAISE

La certification qualité a été délivrée au titre de la catégorie d'action suivante : ACTIONS DE FORMATION.

# Directive NIS 2 :

## Un nouveau cadre pour renforcer la cybersécurité et la résilience à l'échelle de l'Union Européenne

Face à la montée des cybermenaces et aux vulnérabilités critiques des infrastructures numériques, la directive NIS 2 établit un cadre renforcé pour garantir la sécurité des réseaux et systèmes d'information. Adoptée par l'Union européenne, cette directive impose des mesures obligatoires aux entités critiques pour améliorer leur résilience face aux incidents de cybersécurité, protéger les infrastructures essentielles et assurer la continuité des services. La formation NIS 2 Directive Lead Implémenter vous prépare à concevoir, mettre en œuvre et gérer un programme de cybersécurité conforme à cette directive, tout en protégeant vos actifs numériques et votre réputation.

## Objectifs, secteurs concernés et obligations majeures

01. **Renforcer la cybersécurité dans l'UE**
La directive NIS 2 (sécurité des réseaux et des systèmes d'information) vise à améliorer la cybersécurité des infrastructures critiques, économiques et administratives des États membres de l'UE.

02. **Entités concernées**
La directive distingue deux catégories d'entités :
- Entités essentielles (EE)
- Entités importantes (EI)

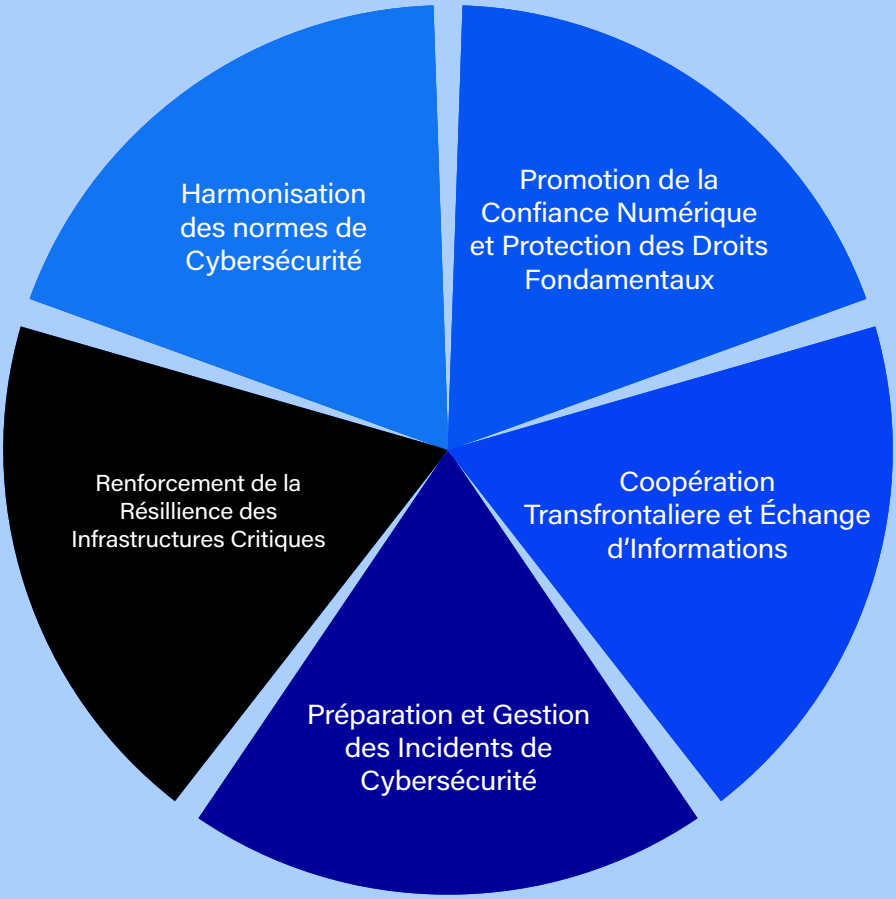
Ces distinctions se basent sur la taille, l'importance critique et le chiffre d'affaires des organisations.

03. **18 secteurs d'activités concernés**
Plus de 10 000 entités, réparties sur 18 secteurs essentiels, tels que les collectivités territoriales, les administrations et les entreprises de taille moyenne ou grande, doivent s'aligner sur ces nouvelles exigences.

04. **Obligations majeures des entités**
Les entités concernées devront :
- Fournir des informations spécifiques à l'ANSSI.
- Mettre en œuvre des mesures adaptées de gestion des risques.
- Déclarer les incidents de cybersécurité.

En cas de non-conformité, des sanctions financières (jusqu'à 2 % du chiffre d'affaires mondial) pourront être appliquées.

## Les principaux objectifs de la directive NIS 2




## Quels sont les principaux changements apportés par la directive NIS 2 ?

- Élargissement du champ d'application
- Renforcement des sanctions
- Approche harmonisée à l'échelle européenne
- Responsabilités accrues des dirigeants
- Gestion des chaînes d'approvisionnement

## Les avantages pour votre organisation

Adopter une stratégie de cybersécurité robuste est essentiel pour protéger votre organisation contre les menaces actuelles tout en renforçant votre crédibilité auprès de vos partenaires. Voici les principaux avantages que vous pouvez en retirer :

- Réduction des risques de cyberattaques : Anticipez les menaces et renforcez vos systèmes critiques.
- Conformité réglementaire : Évitez les sanctions et optimisez vos processus pour répondre aux exigences de NIS 2.
- Restructuration organisationnelle : Mettez en œuvre des solutions de gouvernance efficaces et conformes.
- Crédibilité accrue : Gagnez la confiance de vos clients et partenaires grâce à une stratégie de cybersécurité robuste.

# Formation NIS 2 Directive Lead Implementer : concevoir et gérer un programme de cybersécurité avec certification

**Code : NIS2-DLI-FR** **Durée : 4,5 jours**

## Relevez les défis de la cybersécurité avec la directive NIS 2

### Objectifs

- Acquérir une compréhension approfondie des exigences légales, des principes et des objectifs de la directive NIS 2.
- Maitriser les stratégies et les outils utilisés pour implémenter et gérer un programme de cybersécurité conforme à la NIS 2.
- Identifier et comprendre les exigences du NIS 2 en fonction des spécificités d'une entreprise.
- Initier et piloter un projet de mise en conformité NIS 2 en utilisant la méthodologie PECB et d'autres bonnes pratiques.
- Mettre en place un processus de suivi et d'amélioration continue du programme de cybersécurité.
- Accompagner une entreprise dans la planification, la mise en œuvre, la gestion, le suivi et le maintien d'un programme de cybersécurité conforme NIS 2.
- Réussir l'examen PECB Certified NIS 2 Directive Lead Implementer et obtenir l'une des 4 certifications associées.

### Programme

**Jour 1 : introduction à la directive NIS 2**

- Présentation de la formation : objectifs, déroulement et attentes.
- Les normes et les réglementations en vigueur dans le domaine de la cybersécurité.
- Présentation de la directive NIS 2 (historique, enjeux et portée).
- Les exigences clés de NIS 2.
- Les premières étapes de mise en œuvre d'un programme de cybersécurité conforme à la NIS 2.
- L'analyse du contexte spécifique de chaque organisation.

**Jour 2 : analyse approfondie d'un programme de cybersécurité NIS 2**

- La gouvernance de la cybersécurité (rôles, responsabilités et organisation).
- La gestion des actifs (identification, classification et protection des actifs informationnels).
- L'évaluation et la gestion des risques (méthodologies et outils).

**Jour 3 : renforcement des défenses et préparation aux crises**

- Les contrôles de sécurité (mise en œuvre et évaluation de leur efficacité).
- La sécurité de la chaîne d'approvisionnement (enjeux et bonnes pratiques).
- La gestion des incidents de sécurité (phases et procédures).
- La gestion de crise : (plans d'urgence et exercices).

**Jour 4 : optimisation et pérennisation du programme de cybersécurité**

- La continuité d'activité (plans de reprise d'activité et de secours).
- La sensibilisation et la formation du personnel.
- La communication en interne et en externe, en cas d'incident.
- Les tests de sécurité (vulnérabilités, tests d'intrusion, etc.).
- L'audit interne (évaluation de la conformité et identification des points d'amélioration).
- La mesure des performances (KPI et tableaux de bord).
- L'amélioration continue du programme de cybersécurité.

**Jour 5 : préparation à l'examen PECB NIS 2 Directive Lead Implementer**

- Révision des points clés abordés tout au long de la formation.
- Présentation détaillée de l'examen (structure, format et thématiques abordées).
- Conseils et astuces pour réussir l'examen (méthodologie, gestion du temps, etc.).

## Examen de certification NIS 2

Durée : 3 heures
Langues disponibles : Français, anglais
Format : 80 questions à choix multiples (QCM)
Taux de réussite requis : 70 % de bonnes réponses

## Prérequis

- Avoir des connaissances de base dans le domaine de la cybersécurité.

## Public

- Professionnel de la cybersécurité (DSI, RSSI, auditeur, consultant)
- Responsable conformité
- Autorité gouvernementale et organisme de contrôle

# Pourquoi choisir Oo2 ?

- Formateurs certifiés et expérimentés : Des experts en cybersécurité et conformité NIS 2.
- Approche immersive : Basée sur des études de cas concrets et des scénarios interactifs.
- Examen de certification compris dans le prix de la formation.

**en savoir +**

## France


- **Agence Paris**
  128, rue de la Boétie
  75008 Paris
- **Agence Bordeaux**
  162 cours du Maréchal Gallieni
  33400 Talence

+33 (0)188 24 70 33
+33 (0)188 24 70 34

contact@oo2.fr


## Belgique


- **Agence Bruxelles**
  Rue de la Colonne 1A
  1080 Bruxelles

+32 28.08.51.75

contact@oo2.be

**www.oo2.fr**