

REGU-002 – Gouvernance cyber pour dirigeants

NIS2, risques et pilotage stratégique

Programme de formation de 14 heures destiné aux dirigeants, membres du COMEX/CODIR, DSI, RSSI et responsables conformité.
Aucun prérequis technique requis.

Informations générales

Champ	Détail
Code	REGU-002
Durée	14 heures (2 jours)
Modalité	Présentiel ou distanciel
Effectif	4 à 10 participants
Niveau	Direction / pilotage stratégique
Prérequis	Aucun prérequis technique
Financement	Plan de Développement des Compétences (PDC) – OPCO de la branche

Référentiels mobilisés

- Directive NIS2 (UE) 2022/2555
- Norme ISO/CEI 27001
- Méthode EBIOS Risk Manager (ANSSI)

Organisme

Telemach Learning – NDA 11 92 27843 92

Formateur

Alexandre BOIGUES

Objectifs pédagogiques

À l'issue de la formation, le participant sera capable de :

1 Déterminer l'éligibilité NIS2

Déterminer si son organisation est concernée par NIS2 et sous quel statut.

2 Identifier les obligations

Identifier les obligations de gouvernance et de gestion des risques imposées par NIS2.

3 Comprendre le SMSI

Comprendre les principes d'un système de management de la sécurité de l'information (SMSI / ISO 27001).

4 Maîtriser EBIOS RM

Utiliser les grands principes de la méthode EBIOS Risk Manager.

5 Structurer la gouvernance cyber

Structurer la gouvernance cyber de son organisation.

6 Construire une feuille de route

Construire une feuille de route de mise en conformité NIS2 et un plan de gestion de crise cyber.

Module 1 – NIS2 : champ d'application et obligations

DURÉE : 2H30

Pourquoi NIS2 ?

Ce qui change par rapport à NIS1 et les raisons de cette évolution réglementaire majeure.

Entités essentielles vs importantes

Distinction des catégories d'entités, secteurs visés et critères d'inclusion.

Transposition en droit français

Autorité de contrôle : l'ANSSI. Cadre légal national et calendrier de mise en œuvre.

Notification d'incident

24h – alerte initiale

72h – rapport intermédiaire

1 mois – rapport final

Sanctions

Jusqu'à **10 M€** ou **2 % du CA mondial** en cas de non-conformité.

Module 2 – Gouvernance et responsabilité des dirigeants

DURÉE : 2H



Implication directe des organes de direction

La directive NIS2 engage personnellement les dirigeants dans la supervision de la cybersécurité. Comprendre les mécanismes d'implication directe des organes de direction.



Comité de pilotage cybersécurité

Structurer un comité de pilotage cybersécurité efficace : composition, fréquence, ordre du jour type et indicateurs de suivi.



Reporting sécurité au COMEX/CA

Mettre en place un reporting sécurité adapté au niveau COMEX et Conseil d'Administration : tableaux de bord, KPI et communication des risques.



Responsabilité juridique du dirigeant

Comprendre l'étendue de la responsabilité juridique personnelle du dirigeant en matière de cybersécurité dans le cadre de NIS2.

Module 3 – Principes ISO 27001

DURÉE : 2H30

Introduction aux fondements du Système de Management de la Sécurité de l'Information (SMSI) selon la norme ISO/CEI 27001.

Le SMSI : logique PDCA

Le SMSI repose sur le cycle d'amélioration continue **Plan – Do – Check – Act**, encadré par une politique de sécurité et un périmètre clairement définis.

Contenu du module



Politique de sécurité et périmètre

Définir le cadre et les limites du SMSI au sein de l'organisation.



Les mesures de l'annexe A

Panorama des 93 mesures de sécurité organisationnelles, humaines, physiques et technologiques.



Auditer sa maturité cybersécurité

Méthodes et outils pour évaluer le niveau de maturité actuel de l'organisation.

Module 4 – Principes d'EBIOS Risk Manager

DURÉE : 3H

La méthode EBIOS Risk Manager, développée par l'ANSSI, est la référence française pour l'analyse et le traitement des risques cyber. Elle s'articule autour de **5 ateliers** structurés.



Chaque atelier produit des livrables concrets permettant de documenter les risques identifiés, d'évaluer leur vraisemblance et leur impact, puis de définir les mesures de traitement adaptées au contexte de l'organisation.

Module 5 – Gestion de crise cyber

DURÉE : 2H

Plan de continuité et de reprise d'activité

Concevoir et maintenir un PCA/PRA adapté aux cybermenaces : objectifs de reprise, scénarios de crise, tests et exercices.



Cellule de crise et communication

Organiser la cellule de crise cyber : rôles, responsabilités, chaîne de commandement et stratégie de communication interne et externe.



Notification d'incident NIS2 et RGPD

Maîtriser les obligations de notification : délais NIS2 (24h/72h/1 mois) et articulation avec les exigences RGPD de notification à la CNIL.



En cas d'incident, le non-respect des délais de notification NIS2 expose l'organisation à des sanctions pouvant atteindre 10 M€ ou 2 % du CA mondial.

Module 6 – Feuille de route et plan d'action

DURÉE : 2H

Ce module conclusif permet à chaque participant de repartir avec une feuille de route personnalisée et opérationnelle pour sa mise en conformité NIS2.



Diagnostic de maturité

Évaluer le niveau de maturité cybersécurité actuel de l'organisation à l'aide d'un outil d'autodiagnostic structuré.



Prioriser les actions

Identifier et hiérarchiser les actions à mener selon leur impact, leur urgence et les ressources disponibles.



Feuille de route à 12 mois

Construire une feuille de route de mise en conformité NIS2 sur 12 mois, jalonnée et adaptée au contexte de l'organisation.

Méthodes pédagogiques, formateur et contact

Méthodes pédagogiques

La formation alterne apports théoriques et mises en pratique concrètes :

	Apports théoriques Illustrés de cas réels issus du terrain.
	Atelier autodiagnostic NIS2 Évaluation de l'éligibilité de l'organisation à NIS2.
	Atelier EBIOS RM simplifié Ébauche d'un scénario de risque selon la méthode EBIOS Risk Manager.
	Atelier feuille de route Construction d'une feuille de route personnalisée de mise en conformité.

Votre formateur

Alexandre BOIGUES

Formateur indépendant spécialisé en conformité numérique et gestion des risques – NDA 11 92 27843 92.
Certification ISO 27001 Lead Implementer en cours d'obtention (2026).

Contact et tarifs

Telemach Learning

24 Rue Chanzy, 92600 Asnières-sur-Seine

www.telemach-learning.fr

Tarif intra-entreprise

Sur devis. Financement OPCO / Plan de Développement des Compétences (PDC).