NIS2 – Le Guide Complet de Mise en Conformité

Édition 2026 — Ce guide couvre l'intégralité du parcours de mise en conformité à la directive NIS2 : compréhension du cadre réglementaire, identification des secteurs concernés, gouvernance, gestion des risques, mesures techniques, gestion des incidents, audit et annexes pratiques.

ÉDITION 2026 GUIDE COMPLET

Chapitre 1 – Comprendre NIS2

La directive NIS2 (Network and Information Security 2) constitue une refonte majeure du cadre européen de cybersécurité. Elle renforce significativement les exigences imposées aux organisations dites **essentielles** et **importantes**, en élargissant le périmètre de la directive NIS1 à de nombreux nouveaux secteurs et en durcissant les obligations de conformité.

Gouvernance renforcée

NIS2 impose une implication directe des organes de direction dans la supervision de la cybersécurité. Les dirigeants peuvent être tenus personnellement responsables en cas de manquement.

Gestion des risques documentée

Les entités concernées doivent mettre en place une politique formalisée d'analyse et de traitement des risques, avec une documentation complète et régulièrement mise à jour.

Capacité de réponse aux incidents

La directive exige une capacité opérationnelle de détection, de qualification et de notification des incidents de sécurité dans des délais stricts imposés par les autorités compétentes.

Chapitre 2 – Les Secteurs Concernés

NIS2 distingue deux catégories d'entités soumises à ses obligations : les **entités essentielles** (EE) et les **entités importantes** (EI). Le classement dépend du secteur d'activité, de la taille de l'organisation et de son impact potentiel sur la société ou l'économie.

Entités Essentielles

- Énergie (électricité, gaz, pétrole, hydrogène)
- Transports (aérien, ferroviaire, maritime, routier)
- Secteur bancaire et infrastructures des marchés financiers
- Santé (hôpitaux, laboratoires, R&D pharmaceutique)
- Eau potable et eaux usées
- Infrastructures numériques (DNS, IXP, cloud, datacenters)
- Administration publique centrale
- Espace

Entités Importantes

- Services postaux et de messagerie
- Gestion des déchets
- Fabrication de produits critiques (chimie, alimentaire, dispositifs médicaux)
- Fournisseurs numériques (places de marché, moteurs de recherche, réseaux sociaux)
- Recherche

Critères d'éligibilité

En règle générale : **+50 salariés** ou **CA > 10 M€** pour les EI ; **+250 salariés** ou **CA > 50 M€** pour les EE. Une méthode d'auto-évaluation est recommandée pour déterminer son statut avant toute démarche formelle.

Chapitre 3 – Gouvernance

NIS2 place la gouvernance au cœur de la conformité. La directive exige une chaîne de responsabilité claire, depuis le COMEX jusqu'aux fournisseurs, en passant par les équipes opérationnelles. Chaque acteur a un rôle défini et des obligations précises.

COMEX & Direction Générale

Approbation de la politique de sécurité, allocation des budgets, supervision des risques cyber et responsabilité personnelle en cas de non-conformité grave.

RSSI / CISO

Pilotage opérationnel de la conformité NIS2, animation du programme de sécurité, reporting à la direction, coordination avec les autorités compétentes (ANSSI en France).

Équipes IT

Mise en œuvre des mesures techniques, gestion des vulnérabilités, maintien en condition de sécurité des systèmes, participation aux exercices de crise.

Métiers & Fournisseurs

Les directions métiers participent à l'identification des actifs critiques. Les fournisseurs et prestataires sont soumis à des exigences contractuelles de sécurité renforcées.

Chapitre 4 – Gestion des Risques

La gestion des risques constitue le socle opérationnel de NIS2. Elle doit être structurée, documentée et intégrée dans un cycle d'amélioration continue. La directive impose une approche formalisée couvrant l'ensemble du cycle de vie des risques cyber.

Identification des actifs

Recensement exhaustif des systèmes d'information, données sensibles, processus critiques et dépendances tierces. Un registre des actifs formalisé est indispensable.

Cartographie & analyse

Évaluation de la vraisemblance et de l'impact de chaque menace identifiée. Les méthodes EBIOS Risk Manager ou ISO 27005 sont recommandées par l'ANSSI.

Traitement & acceptation

Pour chaque risque : réduction (mesures techniques/organisationnelles), transfert (assurance cyber), évitement ou acceptation formalisée par la direction avec justification documentée.

Suivi continu

Révision périodique du registre des risques, intégration des nouveaux incidents et vulnérabilités, reporting régulier au COMEX et aux autorités compétentes.

Chapitre 5 – Mesures Techniques

NIS2 exige la mise en place d'un ensemble cohérent de mesures techniques proportionnées aux risques identifiés. Ces mesures couvrent l'ensemble de la surface d'attaque de l'organisation, des identités aux infrastructures cloud.

Gestion des identités & accès (IAM / MFA)

Déploiement d'une solution IAM centralisée avec authentification multifacteur (MFA) obligatoire pour tous les accès privilégiés et les accès distants. Principe du moindre privilège appliqué systématiquement.

Détection & réponse (EDR/XDR, SIEM)

Couverture EDR/XDR sur l'ensemble des endpoints. Centralisation des journaux dans un SIEM avec corrélation d'événements et alertes en temps réel. SOC interne ou externalisé recommandé.

Continuité & sauvegardes (PRA/PCA)

Sauvegardes régulières testées et stockées hors ligne (règle 3-2-1). Plan de Reprise d'Activité (PRA) et Plan de Continuité d'Activité (PCA) formalisés, testés annuellement.

Architecture réseau & Zero Trust

Segmentation réseau stricte, micro-segmentation des environnements critiques. Adoption progressive d'une architecture Zero Trust : vérification systématique de chaque accès, quel que soit le réseau d'origine.

Chiffrement, PKI & sécurité Cloud

Chiffrement des données au repos et en transit. Infrastructure à clés publiques (PKI) pour la gestion des certificats. Sécurisation des environnements cloud : CSPM, CASB, gestion des configurations.

Chapitre 6 – Gestion des Incidents

NIS2 impose des obligations strictes en matière de gestion et de notification des incidents de sécurité. Les délais réglementaires sont contraignants : **24h** pour la notification initiale, **72h** pour le rapport intermédiaire, et **1 mois** pour le rapport final auprès de l'autorité compétente (ANSSI en France).

1

Détection & Qualification

Identification de l'incident via SIEM/EDR, qualification de la criticité, activation de la cellule de crise.

2

Confinement & Éradication

Isolation des systèmes compromis, suppression des vecteurs d'attaque, correction des vulnérabilités exploitées.

3

Restauration & Notification

Remise en service contrôlée, notification réglementaire dans les délais imposés, communication interne et externe.

4

Retour d'Expérience (REX)

Analyse post-incident, identification des causes racines, mise à jour des procédures et du registre des risques.

⚠ Délais réglementaires NIS2 : notification initiale sous **24h**, rapport intermédiaire sous **72h**, rapport final sous **1 mois**.

Chapitre 7 – Audit & Conformité

La préparation d'un audit NIS2 nécessite une organisation rigoureuse et une documentation exhaustive. Les autorités compétentes peuvent procéder à des contrôles sur pièces et sur place. Voici les éléments clés à préparer.

Preuves & Documentation attendues

- Politique de sécurité des systèmes d'information (PSSI) approuvée par la direction
- Registre des actifs à jour
- Registre des risques avec traitements documentés
- Procédures de gestion des incidents et preuves de tests
- Rapports de tests d'intrusion et de vulnérabilités
- Contrats fournisseurs avec clauses de sécurité
- Preuves de formation et de sensibilisation du personnel
- Comptes-rendus de revues de direction sur la cybersécurité

Indicateurs de maturité (KPI)

- Taux de couverture MFA sur les comptes privilégiés
- Délai moyen de détection (MTTD) et de réponse (MTTR)
- Taux de patching dans les délais définis
- Nombre d'incidents notifiés vs. détectés
- Taux de couverture des sauvegardes testées

Plan d'amélioration continue

Chaque audit doit déboucher sur un plan d'action formalisé avec des responsables désignés, des échéances précises et un suivi régulier en comité de pilotage cybersécurité. Le plan d'amélioration est lui-même un élément de preuve de la démarche de conformité.

Chapitre 8 – Annexes & Outils Pratiques

Les annexes du guide fournissent des modèles opérationnels directement utilisables pour accélérer la mise en conformité. Ces outils couvrent l'ensemble des domaines exigés par NIS2.

Modèles de politiques

PSSI, politique de gestion des accès, politique de sauvegarde, politique de gestion des vulnérabilités — modèles prêts à personnaliser.

Registre des actifs

Modèle de registre couvrant les actifs matériels, logiciels, données et services tiers, avec niveaux de criticité et propriétaires désignés.

Registre des incidents

Formulaire de déclaration, journal de suivi des incidents, modèle de rapport réglementaire pour notification à l'ANSSI.

Registre fournisseurs

Inventaire des prestataires critiques, questionnaires de sécurité fournisseurs, clauses contractuelles types conformes à NIS2.

Check-lists de conformité

Check-lists thématiques par domaine (gouvernance, technique, incidents, audit) pour auto-évaluer rapidement son niveau de conformité NIS2.

Synthèse & Feuille de Route NIS2

La mise en conformité NIS2 est un projet structurant qui engage l'ensemble de l'organisation. Elle ne se limite pas à un exercice de documentation : elle exige une transformation réelle des pratiques de cybersécurité, portée au plus haut niveau de la direction.

01

Auto-évaluation & périmètre

Déterminer si l'organisation est entité essentielle ou importante. Identifier les systèmes et processus dans le périmètre NIS2.

02

Gouvernance & responsabilités

Désigner le RSSI/CISO, impliquer le COMEX, formaliser la chaîne de responsabilité et allouer les ressources budgétaires.

03

Analyse des risques & mesures

Conduire une analyse de risques formalisée (EBIOS RM), déployer les mesures techniques prioritaires (MFA, EDR, sauvegardes, PRA).

04

Gestion des incidents & notification

Mettre en place les procédures de détection, réponse et notification réglementaire. Tester les procédures par des exercices de crise.

05

Audit & amélioration continue

Préparer la documentation d'audit, suivre les KPI de maturité, mettre en œuvre un plan d'amélioration continue validé par la direction.

La conformité NIS2 n'est pas une destination mais un processus continu. Les organisations qui intègrent la cybersécurité dans leur culture d'entreprise seront les mieux armées face aux cybermenaces de demain.