AYI NEDJIMI Consultants

NIS 2 Phase Opérationnelle 2026 : Guide Complet de Mise

Catégorie : Conformité Lecture : 10 min Publié le : 19/01/2026 Auteur : Ayi NEDJIMI

Guide exhaustif NIS 2 en 2026 : phase opérationnelle, mesures Article 21, notification incidents, supervision ANSSI, sanctions et plan d. Guide.

01 Rappel de la Directive NIS 2

La directive **NIS 2** (Network and Information Security 2), adoptée le 14 décembre 2022 et transposée en droit français en octobre 2024, représente une refonte majeure du cadre européen de cybersécurité. En 2026, nous entrons dans la **phase opérationnelle** où les contrôles ANSSI deviennent effectifs et les sanctions peuvent être prononcées. Ce guide analyse en profondeur les obligations actuelles et les meilleures pratiques de mise en conformité. Guide exhaustif NIS 2 en 2026 : phase opérationnelle, mesures Article 21, notification incidents, supervision ANSSI, sanctions et plan d. Guide. Le cadre réglementaire européen impose des exigences croissantes aux organisations. Ce guide sur nis 2 phase operationnelle 2026 fournit les clés de compréhension et de mise en conformité. Nous abordons notamment : 01 rappel de la directive nis 2, 02 phase d'identification terminée et 03 les 10 mesures de l'article 21. Les professionnels y trouveront des recommandations actionnables, des commandes prêtes à l'emploi et des stratégies de mise en œuvre adaptées aux environnements d'entreprise.

NIS 2 succède à la directive NIS 1 de 2016 qui avait posé les premières bases d'une approche coordonnée de la cybersécurité au niveau européen. Face à l'évolution des menaces cyber et aux limites constatées du premier texte, le législateur européen a significativement renforcé et élargi le cadre réglementaire.

Les changements majeurs de NIS 2

- **Périmètre élargi** : de 7 à 18 secteurs couverts
- **Plus d'entités** : environ 15 000 en France (contre 500 sous NIS 1)
- **Harmonisation** : règles communes dans toute l'UE
- **Sanctions renforcées** : jusqu'à 10M€ ou 2% du CA mondial
- **Responsabilité des dirigeants** : sanctions personnelles possibles

Le contexte de la menace cyber en 2026

L'année 2025 a confirmé l'intensification des cyberattaques contre les organisations européennes. Les attaques par rançongiciel, les compromissions de supply chain et les campagnes d'espionnage étatique ont touché des secteurs critiques : hôpitaux, collectivités territoriales, entreprises industrielles. NIS 2 vise précisément à élever le niveau de résilience face à ces menaces systémiques.

Les statistiques récentes montrent que :

- Le nombre d'incidents majeurs signalés a augmenté de 40% en 2025
- Le coût moyen d'une violation de données atteint 4,5 millions d'euros en Europe
- 60% des PME victimes de cyberattaques cessent leur activité dans les 6 mois
- Les attaques sur la supply chain ont triplé depuis 2022

Architecture de la directive

NIS 2 s'articule autour de plusieurs piliers fondamentaux :

Identification des entités : Mécanisme d'auto-évaluation et d'enregistrement permettant de déterminer quelles organisations sont soumises aux obligations.

Mesures de sécurité : L'Article 21 définit 10 catégories de mesures obligatoires couvrant l'ensemble du cycle de gestion de la cybersécurité.

Notification des incidents : Obligations de signalement rapide des incidents significatifs aux autorités compétentes.

Supervision et sanctions : Pouvoirs de contrôle renforcés pour les autorités nationales et régime de sanctions dissuasif.

Les quatre piliers de la directive NIS 2

02 Phase d'Identification Terminée

La phase d'identification des entités soumises à NIS 2 s'est achevée fin 2025. Les organisations ont dû s'auto-évaluer et, le cas échéant, s'enregistrer auprès de l'ANSSI. En 2026, cette identification est présumée complète et les contrôles peuvent viser toute entité relevant objectivement du périmètre, qu'elle se soit enregistrée ou non.

Critères de classification

NIS 2 distingue deux catégories d'entités selon leur importance systémique : Pour approfondir, consultez SecNumCloud 2026 et EUCS : Guide Complet Qualification.

Critère	Entité Essentielle (EE)	Entité Importante (EI)
Taille	Grande entreprise (>250 employés ou >50M€ CA)	Moyenne entreprise (>50 employés ou >10M€ CA)
Secteurs spécifiques	Énergie, Transports, Santé, Eau, Infra numériques, Admin publiques, Espace	+ Services postaux, Déchets, Chimie, Alimentaire, Fabrication, Recherche
Supervision	Ex ante (contrôles proactifs)	Ex post (contrôles sur signalement)
Sanctions max	10M€ ou 2% CA mondial	7M€ ou 1,4% CA mondial

Les 18 secteurs couverts

NIS 2 couvre désormais 18 secteurs d'activité répartis en deux annexes :

Annexe I - Secteurs hautement critiques
Énergie (électricité, pétrole, gaz, hydrogène), Transports (aérien, ferroviaire, maritime, routier), Banque, Infrastructures des marchés financiers, Santé, Eau potable, Eaux usées, Infrastructure numérique, Gestion des services TIC (B2B), Administrations publiques, Espace.

Annexe II - Autres secteurs critiques
Services postaux et de courrier, Gestion des déchets, Fabrication/production/distribution de produits chimiques, Production/transformation/distribution de denrées alimentaires, Fabrication (dispositifs médicaux, informatique, électronique, machines, véhicules), Fournisseurs numériques, Recherche.

Cas particuliers d'assujettissement

Certaines entités sont assujetties indépendamment de leur taille : Les recommandations de CNIL constituent une reference essentielle.

- **Fournisseurs de réseaux de communications électroniques publics**
- **Prestataires de services de confiance qualifiés**
- **Registres de noms de domaine de premier niveau**
- **Fournisseurs de services DNS**
- **Entités identifiées comme critiques par les États membres**

Notre avis d'expert
Comment démontrez-vous l'accountability exigée par le RGPD en cas de contrôle ?

03 Les 10 Mesures de l'Article 21

L'Article 21 de NIS 2 constitue le cœur des obligations techniques et organisationnelles. Il définit **10 catégories de mesures** que les entités doivent mettre en œuvre pour gérer les risques de cybersécurité. Ces mesures doivent être proportionnées au niveau de risque, à la taille de l'entité et à la probabilité et gravité des incidents. Les recommandations de ENISA constituent une reference essentielle.

Les 10 catégories de mesures de sécurité obligatoires selon l'Article 21

Détail des mesures clés

1. Politiques de sécurité et analyse des risques : Établir une PSSI formelle, réaliser des analyses de risques régulières, définir les mesures de traitement et maintenir un registre des risques actualisé.

2. Gestion des incidents : Mettre en place un processus de détection, qualification, réponse et remédiation des incidents. Tenir un journal des incidents et assurer la notification réglementaire.

3. Continuité d'activité : Élaborer des plans de continuité (PCA) et de reprise (PRA), réaliser des sauvegardes régulières testées, et définir les procédures de gestion de crise.

4. Sécurité de la chaîne d'approvisionnement : Évaluer les risques des fournisseurs critiques, intégrer des clauses de sécurité aux contrats, auditer les prestataires sensibles.

5. Acquisition, développement et maintenance : Intégrer la sécurité dans le cycle de développement (DevSecOps), gérer les vulnérabilités, sécuriser la configuration des systèmes.

6. Évaluation de l'efficacité : Réaliser des audits internes et externes, des tests d'intrusion, et des revues de conformité. Améliorer continuellement le dispositif. Pour approfondir, consultez SOC 2 : Guide Complet Conformite pour Organisations.

04 Notification des Incidents

NIS 2 impose un processus de notification structuré en plusieurs étapes pour les **incidents significatifs**. Ce mécanisme vise à permettre une réponse coordonnée et à alimenter la connaissance collective de la menace. Pour approfondir, consultez ISO 27001:2022 vs ISO 27001:2013 : Differences Cles.

Définition d'un incident significatif

Un incident est considéré comme significatif s'il remplit l'un des critères suivants :

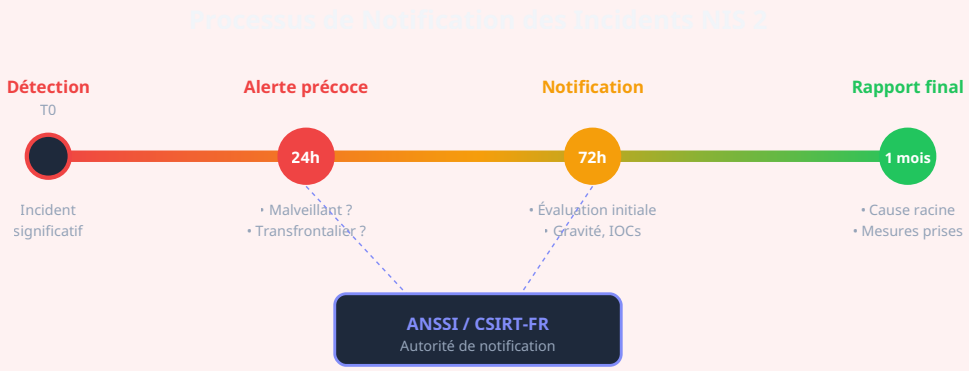
- Cause ou peut causer des **perturbations opérationnelles graves** ou des pertes financières importantes
- Affecte ou peut affecter d'**autres personnes physiques ou morales** en causant des dommages matériels, corporels ou moraux considérables

Processus de notification en 3 étapes

Délais de notification obligatoires

- **Alerte précoce (24h)** : Notification sans délai et au plus tard 24h après prise de connaissance. Indique si l'incident est probablement malveillant ou a un impact transfrontalier.
- **Notification complète (72h)** : Mise à jour avec évaluation initiale, gravité, impact et indicateurs de compromission disponibles.

- **Rapport final (1 mois)** : Description détaillée, cause probable, mesures prises et en cours, impact transfrontalier éventuel.



Les trois phases de notification obligatoire suite à un incident significatif

Canaux de notification

En France, les notifications doivent être adressées à l'**ANSSI** via le portail dédié ou le CSIRT-FR. Pour les incidents affectant des données personnelles, une notification parallèle à la CNIL reste obligatoire au titre du RGPD.

Cas concret
L'entrée en vigueur de NIS2 en octobre 2024 a élargi le périmètre des organisations soumises à des obligations de cybersécurité en Europe. Les secteurs essentiels et importants doivent désormais notifier les incidents significatifs dans les 24 heures et maintenir des mesures de gestion des risques proportionnées.

05 Gouvernance et Responsabilité des Dirigeants

NIS 2 introduit une **responsabilité directe des organes de direction** dans la gouvernance de la cybersécurité. Cette disposition vise à élever la cybersécurité au niveau stratégique et à garantir l'engagement des dirigeants.

Obligations des organes de direction

Les dirigeants doivent :

- **Approuver** les mesures de gestion des risques de cybersécurité
- **Superviser** leur mise en œuvre
- **Suivre une formation** en matière de cybersécurité
- **Encourager** la formation des employés
- **Être informés** régulièrement de l'état de la cybersécurité

Responsabilité personnelle des dirigeants
En cas de manquement grave, les dirigeants peuvent faire l'objet de sanctions personnelles incluant l'**interdiction temporaire d'exercer des fonctions de direction**. Cette disposition vise les cas où le dirigeant a sciemment négligé ses obligations de supervision ou approuvé des mesures manifestement insuffisantes.

Organisation recommandée

Pour répondre aux exigences de gouvernance, les organisations devraient déployer :

- Un **comité de pilotage cybersécurité** au niveau direction
- Un **reporting régulier** (trimestriel minimum) au COMEX
- Des **indicateurs de performance** (KPIs) cybersécurité suivis au plus haut niveau
- Une **politique de formation** des dirigeants sur les enjeux cyber
- Une **délégation claire** vers le RSSI avec les moyens correspondants

Votre conformité ISO 27001 se traduit-elle par une amélioration réelle de votre sécurité ?

06 Sécurité de la Supply Chain

L'Article 21 accorde une importance particulière à la sécurité de la chaîne d'approvisionnement, reconnaissant que les attaques via les fournisseurs constituent l'un des vecteurs de menace les plus significatifs.

Périmètre de la supply chain

La sécurité de la supply chain couvre :

- **Fournisseurs directs** : prestataires IT, éditeurs de logiciels, hébergeurs
- **Sous-traitants** : entités intervenant indirectement sur les systèmes
- **Produits** : matériels, logiciels, composants intégrés aux SI
- **Services** : maintenance, support, développement externalisé

Exigences de sécurité supply chain

Évaluation des fournisseurs : Configurer un processus d'évaluation des risques de cybersécurité des fournisseurs avant contractualisation et périodiquement ensuite.

Clauses contractuelles : Intégrer des exigences de sécurité dans les contrats : niveau de sécurité minimum, droit d'audit, notification des incidents, continuité de service. Pour approfondir, consultez Cyber-assurance 2026 : Nouvelles Exigences et Guide Complet.

Suivi et audit : Réaliser des contrôles réguliers des fournisseurs critiques, demander des attestations de conformité ou des rapports d'audit indépendants.

Plan de sortie : Prévoir la réversibilité et la capacité à changer de fournisseur en cas de défaillance sécurité.

07 Exercices de Crise Cyber

La préparation aux incidents majeurs passe par la réalisation régulière d'exercices de crise. NIS 2 renforce cette exigence en demandant aux entités de tester effectivement leur capacité de réponse.

Types d'exercices recommandés

Type d'exercice	Fréquence	Participants	Objectifs
Exercice sur table	Annuel minimum	Direction, RSSI, IT, Métiers	Tester la prise de décision, la communication
Exercice technique	Semestriel	Équipes IT/Sécurité	Tester les procédures de réponse technique
Test de restauration	Annuel	IT, Production	Valider les sauvegardes et le PRA
Red Team	Selon maturité	Prestataire externe	Test réaliste de l'ensemble du dispositif

Scénarios types à envisager

- **Rançongiciel** : Chiffrement massif des données et systèmes
- **Compromission de compte privilégié** : Prise de contrôle administrative
- **Exfiltration de données** : Vol de données sensibles
- **Attaque supply chain** : Compromission via un fournisseur
- **DDoS** : Indisponibilité des services critiques

08 Supervision et Contrôles ANSSI

L'ANSSI, en tant qu'autorité nationale compétente pour NIS 2 en France, dispose de pouvoirs de supervision renforcés. En 2026, les contrôles deviennent pleinement opérationnels.

Régimes de supervision différenciés

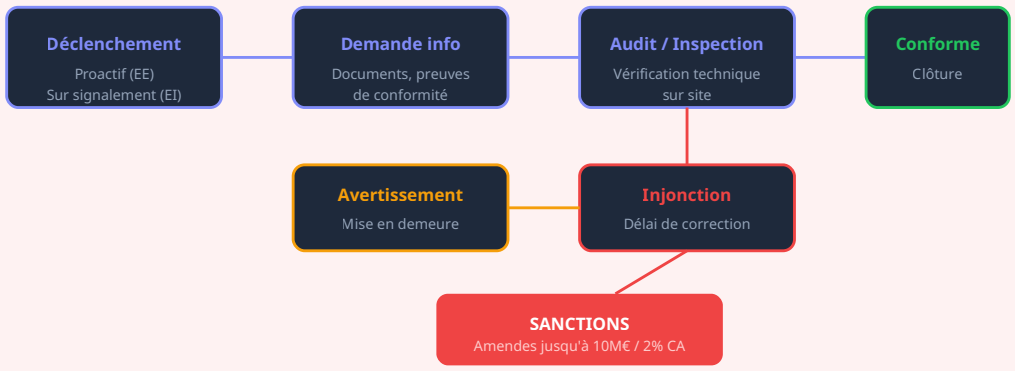
Entités Essentielles - Supervision ex ante : L'ANSSI peut réaliser des contrôles proactifs sans signalement préalable. Audits réguliers, vérifications aléatoires, inspections sur site.

Entités Importantes - Supervision ex post : Contrôles déclenchés sur la base d'indices : signalement d'incident, plainte, information de tiers, analyse de risque sectorielle.

Pouvoirs de l'ANSSI

- **Demande d'information** : Exiger la production de documents, politiques, preuves de conformité
- **Audits** : Réaliser ou faire réaliser des audits de sécurité

- **Scans de sécurité** : Effectuer des analyses techniques des systèmes exposés
- **Inspections sur site** : Accéder aux locaux et aux systèmes
- **Avertissements** : Notifier des manquements et demander des corrections
- **Injonctions** : Ordonner la mise en conformité sous délai
- **Sanctions** : Prononcer des amendes administratives



Processus de contrôle et d'escalade de l'ANSSI

09 Régime de Sanctions

NIS 2 établit un régime de sanctions significativement renforcé par rapport à NIS 1. Les amendes peuvent atteindre des montants comparables au RGPD, reflétant l'importance accordée à la cybersécurité.

Barème des sanctions

Type d'entité	Amende maximale	Alternative % CA
Entité Essentielle	10 000 000 €	2% du CA annuel mondial
Entité Importante	7 000 000 €	1,4% du CA annuel mondial

Le montant le plus élevé entre l'amende fixe et le pourcentage du CA s'applique.

Sanctions complémentaires

- **Publication de la décision** : Name and shame public
- **Injonction de mise en conformité** : Sous astreinte journalière
- **Suspension d'activité** : Pour les manquements les plus graves
- **Interdiction de direction** : Pour les dirigeants défaillants

Facteurs d'appréciation

L'ANSSI tiendra compte de plusieurs facteurs pour moduler les sanctions :

- Gravité et durée du manquement
- Caractère intentionnel ou négligent
- Efforts de mise en conformité
- Coopération avec l'autorité
- Antécédents
- Avantages financiers tirés du manquement

10 Plan d'Action 2026-2028

Pour les organisations entrant en phase opérationnelle NIS 2, voici une feuille de route pragmatique de mise en conformité sur les deux prochaines années.

Phase 1 : Consolidation (2026)

- **Vérifier l'enregistrement** : S'assurer que l'entité est bien enregistrée auprès de l'ANSSI
- **Gap analysis** : Évaluer l'écart entre l'existant et les 10 mesures de l'Article 21
- **Plan de remédiation** : Prioriser les actions selon le risque
- **Gouvernance** : Formaliser le comité cyber et les reportings
- **Procédure de notification** : Établir le processus 24h/72h/1 mois

Phase 2 : Renforcement (2027)

- **Supply chain** : Déployer le programme d'évaluation des fournisseurs
- **Formation** : Former les dirigeants et sensibiliser l'ensemble des collaborateurs
- **Tests** : Réaliser un exercice de crise majeur
- **Audits** : Lancer un audit de conformité NIS 2
- **PCA/PRA** : Tester les plans de continuité

Phase 3 : Maturité (2028)

- **Amélioration continue** : Cycle PDCA de la cybersécurité
- **Automatisation** : Outiller la détection et la réponse
- **Certification** : Envisager ISO 27001 si pertinent
- **Veille** : Suivre les évolutions réglementaires (actes délégués, jurisprudence)

Checklist de conformité NIS 2

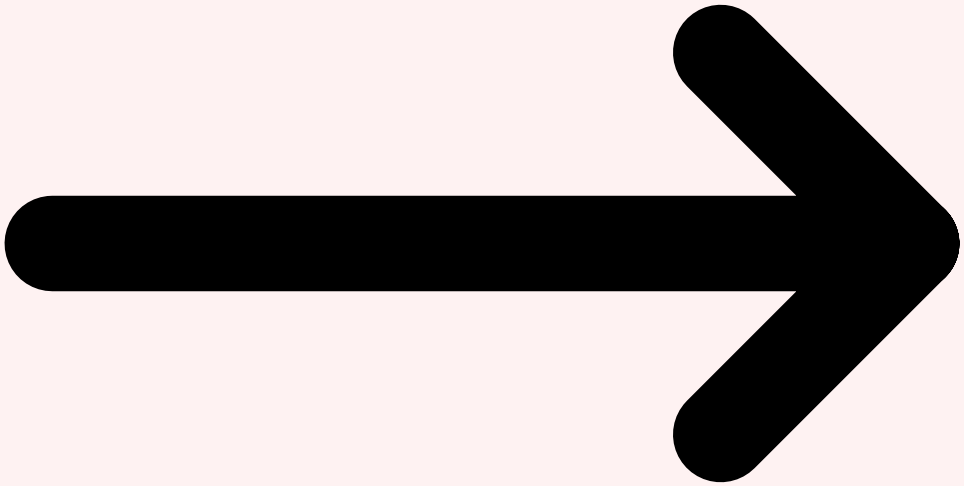
- Entité enregistrée auprès de l'ANSSI
- PSSI formalisée et approuvée par la direction
- Analyse de risques actualisée
- Procédures de gestion des incidents en place
- PCA/PRA testés

- Programme de sécurité supply chain déployé
- Formation cybersécurité des dirigeants réalisée
- Exercice de crise effectué dans l'année
- Processus de notification opérationnel
- Indicateurs cybersécurité suivis au COMEX

Besoin d'accompagnement NIS 2 ?

Nos consultants spécialisés vous accompagnent dans votre mise en conformité NIS 2 : diagnostic initial, plan de remédiation, mise en œuvre des mesures et préparation aux contrôles ANSSI.

Évaluer ma conformité NIS 2



Pour approfondir ce sujet, consultez notre outil open-source rgpd-compliance-checker qui facilite la vérification automatisée de conformité RGPD.

Questions frequemment posees

Quels sont les delais de mise en conformite pour NIS 2 Phase Opérationnelle 2026 ?

Les delais de mise en conformite dependent du niveau de maturite initial de l'organisation et de la complexite de son systeme d'information. En general, un projet de mise en conformite complet necessite entre six et dix-huit mois, incluant l'analyse d'ecart initiale, la definition du plan d'action, l'implementation des mesures correctives et la preparation de la documentation necessaire pour l'audit de certification.

Quel est le délai réaliste pour se mettre en conformité avec NIS 2 Phase Opérationnelle ?

Comptez entre 6 et 18 mois selon la maturité de votre SI. Les entreprises qui partent de zéro doivent prévoir 12 mois minimum avec un accompagnement externe dédié.

Combien coûte la mise en conformité NIS 2 Phase Opérationnelle pour une PME ?

Le budget varie de 15 000 à 80 000 euros selon la taille et la complexité de l'organisation. Le poste le plus important est souvent l'accompagnement conseil et la formation des équipes.

Sources et références : CNIL · ANSSI

Conclusion

Ayi NEDJIMI Consultants — Expert cybersécurité offensive & intelligence artificielle

ayinedjimi-consultants.fr · ayi@ayinedjimi-consultants.fr