NIS 2 : La cybersécurité devient un impératif stratégique

Décrypter, se situer et agir :
le guide pour les décideurs.

La directive (UE) 2022/2555, ou NIS 2, impose un changement de posture : la sécurité numérique est désormais une responsabilité de la direction, au même titre que les enjeux financiers ou juridiques.

Le paysage des menaces a changé, la réponse européenne aussi.

Une menace en pleine expansion

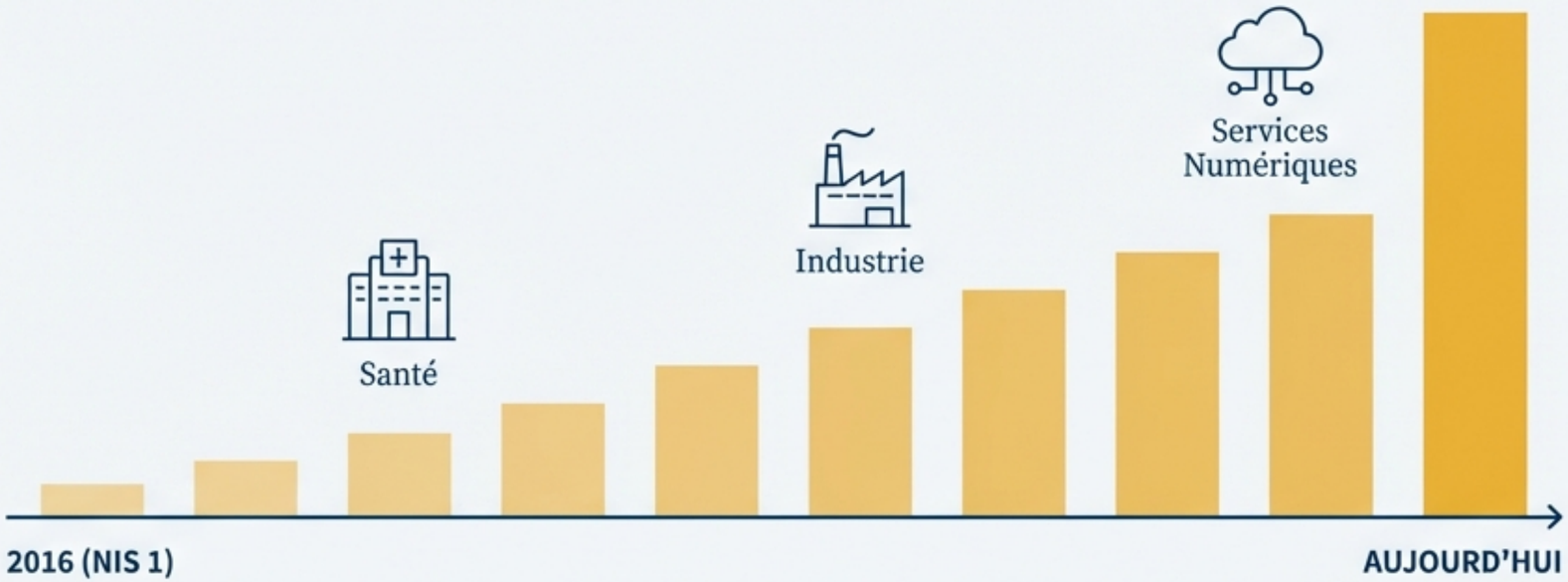
« Le nombre, l'ampleur, la sophistication, la fréquence et l'impact des incidents ne cessent de croître. » (Directive UE 2022/2555, considérant 3)

Des acteurs malveillants mieux outillés

L'ANSSI souligne la professionnalisation des attaquants, qui ciblent des entités de plus en plus nombreuses et souvent mal préparées.

Des interdépendances critiques

Une perturbation locale peut avoir des « effets en cascade plus larges » sur l'ensemble du marché intérieur en raison de l'interconnexion des chaînes de valeur.

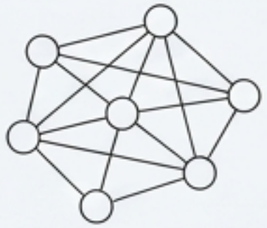


L'impact est réel :

Les incidents récents dans le secteur de la santé (Hôpital Sud Francilien, Hospital Clínic de Barcelona) illustrent la vulnérabilité des services essentiels. Les attaques par rançongiciel comme WannaCry ont démontré l'impact sur des équipements critiques, allant des scanners IRM aux systèmes de production.

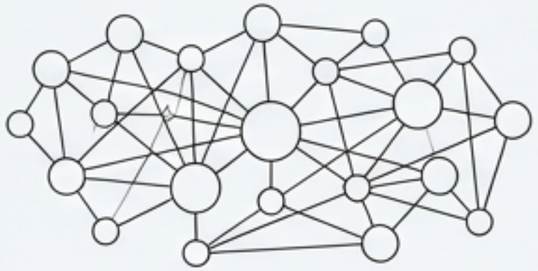
De NIS 1 à NIS 2 : un changement de paradigme pour la cyber-résilience européenne

NIS 1 (2016)



- **Périmètre: Limité** (~4 000 entités) aux Opérateurs de Services Essentiels (OSE) et Fournisseurs de Service Numérique (FSN).
- **Approche: Fragmentée**, laissée à l'appréciation des États membres.
- **Exigences: De haut niveau**, peu prescriptives.
- **Objectif**: Créer des capacités nationales de cybersécurité.

NIS 2 (2022)



- **Périmètre: Massif** (>160 000 entités), avec 18 secteurs minimum et leurs chaînes d'approvisionnement.
- **Approche: Harmonisée**, avec des règles minimales et une coopération renforcée.
- **Exigences**: **Précises et strictes**, incluant gouvernance, gestion de la supply chain et reporting détaillé.
- **Objectif** : Atteindre un niveau élevé commun de cyber-résilience opérationnelle.

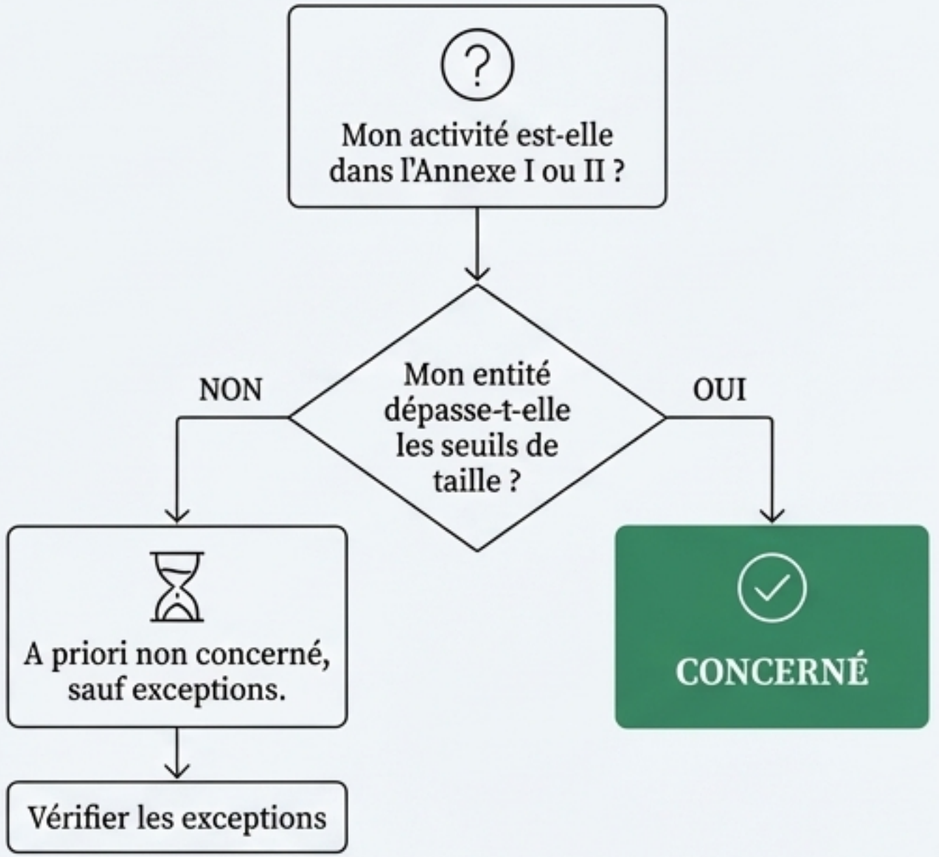
NIS 2 marque le passage d'une logique de conformité nationale à une stratégie de résilience systémique à l'échelle de l'Union.

Première question : votre organisation est-elle concernée ?

Le principe général en deux critères cumulatifs

1. Critère Sectoriel
Votre activité appartient-elle à l'un des secteurs « hautement critiques » (Annexe I) ou « autres secteurs critiques » (Annexe II) ?

2. Critère de Taille
Votre entité est-elle une moyenne entreprise ou plus ?
- ≥ 50 employés **OU**
- ≥ 10 M€ de chiffre d'affaires annuel / total de bilan.



Exceptions Clés

Certaines entités sont concernées **quelle que soit leur taille**.

Liste des exceptions principales (basée sur l'Article 2) :
- Fournisseurs de réseaux/services de communications électroniques publics.
- Prestataires de services de confiance qualifiés.
- Registres de noms de domaine de premier niveau (TLD) et fournisseurs de services DNS.
- Entités étant l'unique prestataire d'un service essentiel dans un État membre.

Secteurs et statuts : situez votre entité pour comprendre vos obligations.

Entités Essentielles (EE) : Issues principalement de l'Annexe I. Supervision **proactive** (*ex ante*) et réactive (*ex post*).

Entités Importantes (EI) : Issues principalement de l'Annexe II. Supervision **réactive** (*ex post*).

Entités Essentielles (Annexe I - Secteurs Hautement Critiques)	Entités Importantes (Annexe II - Autres Secteurs Critiques)
Énergie : Électricité, Pétrole, Gaz, Chaleur, Hydrogène...	**Services postaux et d'expédition**
Transports : Aérien, Ferroviaire, Maritime, Routier...	**Gestion des déchets**
Secteur Bancaire & Infrastructures des marchés financiers **Santé** : Prestataires de soins, laboratoires de référence, R&D pharmaceutique... **Eau potable et eaux usées**	**Chimie** (fabrication, distribution) **Agroalimentaire** (production, transformation)
Infrastructure numérique : DNS, TLD, Cloud, Datacenters...	**Fabrication** : Dispositifs médicaux, produits informatiques, équipements électriques, véhicules...
Gestion des services TIC (B2B) : Fournisseurs de services gérés (MSP), de sécurité gérée (MSSP).	**Fournisseurs numériques** : Places de marché, moteurs de recherche, réseaux sociaux.
Administration publique (centrale/régionale)	**Recherche**
Espace	

La gouvernance au cœur du dispositif : la direction est directement responsable.

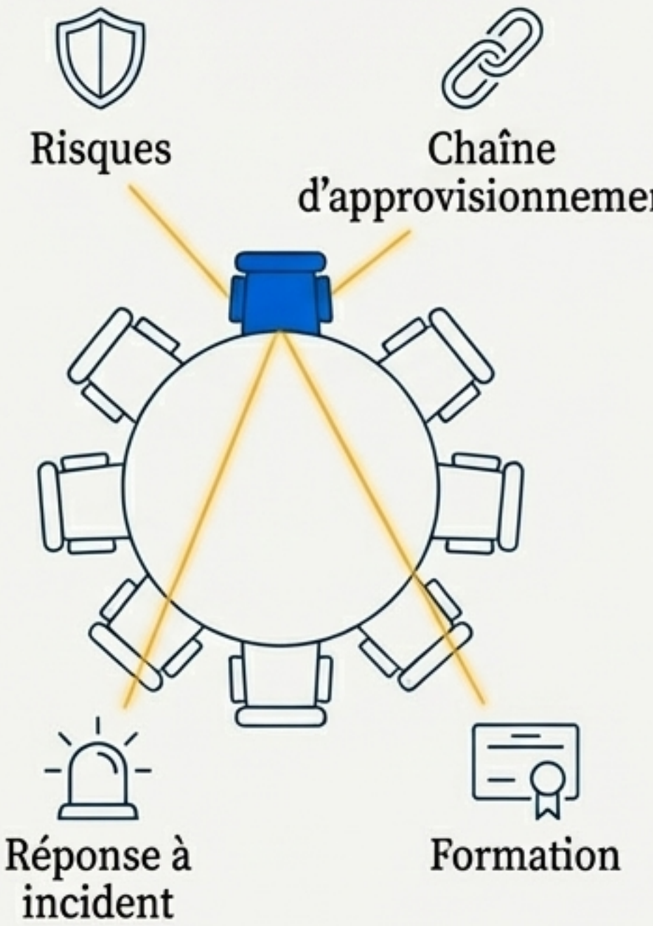
Implications concrètes

Fin du « risque délégué »
La cybersécurité n'est plus un sujet purement technique. Elle doit être intégrée à la stratégie et pilotée au plus haut niveau.

Responsabilité personnelle
La non-conformité peut exposer les dirigeants à des sanctions, incluant une interdiction temporaire d'exercer (Article 32.5).

Obligation de formation
Les dirigeants sont tenus de suivre une formation pour acquérir les compétences nécessaires à l'évaluation des risques et des pratiques de cybersécurité (Article 20.2).

> Les organes de direction des entités essentielles et importantes doivent **approuver** les mesures de gestion des risques en matière de cybersécurité, **superviser** leur mise en œuvre et peuvent être **tenus responsables** de la violation de ces obligations.
>
> *Article 20, Directive (UE) 2022/2555*



Les 10 mesures socles de gestion des risques (Article 21)

NIS 2 impose une approche "tous risques" visant à protéger les systèmes d'information ET leur environnement physique. Ces 10 domaines d'action constituent le standard minimum attendu.

Analyse de risques & PSSI :
Politiques de sécurité formalisées.

Gestion des incidents :
Procédures de détection, d'analyse et de réponse.

Continuité d'activité :
Gestion des sauvegardes, plan de reprise (PRA), gestion de crise.

Sécurité de la chaîne d'approvisionnement :
Évaluation et gestion des risques liés aux fournisseurs et prestataires.

Sécurité du cycle de vie des SI :
Acquisition, développement et maintenance sécurisés, gestion des vulnérabilités.

Évaluation de l'efficacité :
Audits, tests de pénétration et évaluations régulières.

Cyber-hygiène de base & Formation :
Pratiques fondamentales et sensibilisation des collaborateurs.

Cryptographie & Chiffrement :
Politiques d'utilisation des technologies de chiffrement.

Sécurité des RH & Contrôle d'accès :
Gestion des accès et des actifs informationnels.

Authentification forte :
MFA/continue et sécurisation des communications d'urgence.

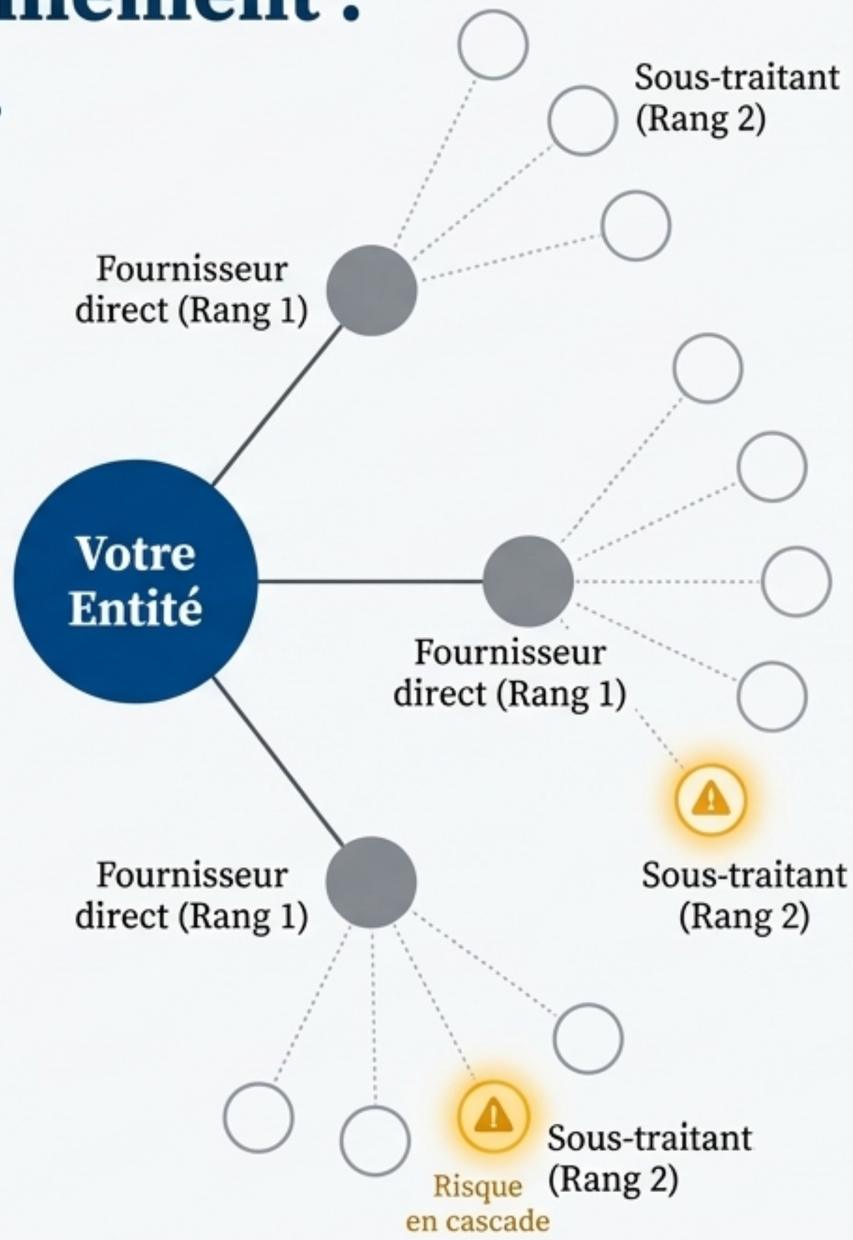
La sécurité de la chaîne d’approvisionnement : votre périmètre de risque s’est élargi.

L’exigence fondamentale

Article 21.3 : « Les entités doivent évaluer et prendre en compte les vulnérabilités propres à chaque fournisseur et prestataire direct, ainsi que la qualité globale de leurs produits et pratiques de cybersécurité. »

Ce que cela signifie en pratique

- ✓ **Audit des fournisseurs :** Ne plus se contenter de clauses contractuelles ; il faut évaluer la maturité réelle des partenaires critiques.
- ✓ **Exigences contractuelles :** Intégrer des clauses de sécurité spécifiques et des droits d’audit dans les contrats.
- ✓ **Vision étendue :** Prendre en compte les risques liés aux sous-traitants de vos fournisseurs (« risques en cascade »).
- ✓ **Vigilance accrue** sur les prestataires de services de sécurité gérés (MSSP), qui représentent un point d'accès privilégié pour les attaquants (considérant 86).



La notification d’incidents importants : une procédure stricte en 3 temps.

Cause une **perturbation opérationnelle grave** ou des **pertes financières**.
Affecte d’autres personnes en causant des **dommages considérables**. (Article 23.3)

< 24 HEURES

Alerte précoce

Notification initiale de l’incident. Indication si une origine malveillante est suspectée et s’il y a un impact transfrontalier.

< 72 HEURES

Notification d’incident

Mise à jour de l’alerte. Évaluation initiale de la gravité, de l’impact et des indicateurs de compromission disponibles.

< 1 MOIS

Rapport Final

Analyse détaillée : cause racine, description complète, mesures d’atténuation appliquées et prévues.

« Le simple fait de notifier un incident n’accroît pas la responsabilité de l’entité qui est à l’origine de la notification. » (Article 23.1)

Les sanctions : un niveau de dissuasion comparable au RGPD.

Entités Essentielles (EE)

Jusqu'à 10 M€

ou

Jusqu'à 2% du chiffre d'affaires annuel mondial.

(Le montant le plus élevé est retenu).

Entités Importantes (EI)

Jusqu'à 7 M€

ou

Jusqu'à 1,4% du chiffre d'affaires annuel mondial.

(Le montant le plus élevé est retenu).

Au-delà des amendes (Articles 32 & 33) :

- Instructions contraignantes avec astreintes.
- Suspension de certifications ou d'autorisations.
- **Responsabilité personnelle** : possibilité d'interdire temporairement aux dirigeants d'exercer leurs fonctions.

« Les dirigeants sont en première ligne : ils ont une responsabilité directe et peuvent faire l'objet de sanctions personnelles en cas de défaillance. »

L’écosystème de la régulation NIS 2 en France.

ANSSI (Agence Nationale de la Sécurité des Systèmes d’Information)

Rôle : Autorité nationale compétente et coordinateur national.
Missions :

- **Supervision et Contrôle :** Mène les audits et les inspections.
- **Point de Contact Unique (PCU) :** Assure la liaison avec les autres États membres.
- **Autorité de gestion de crise :** Pilote la réponse nationale aux incidents majeurs.

CSIRT National (opéré par l’ANSSI)

Rôle : Centre de réponse aux incidents de sécurité informatique.
Missions :

- **Réception des notifications :** Point d'entrée pour les déclarations d'incidents.
- **Assistance technique :** Fournit des orientations et un soutien.
- **Veille et Alerte :** Surveille les menaces et diffuse des informations.

Groupe de Coopération

(Niveau stratégique)

Réseau EU-CyCLONe

(Gestion de crise opérationnelle)

L’ANSSI participe activement à ces réseaux pour une réponse coordonnée à l’échelle de l’UE.

Votre feuille de route vers la conformité NIS 2 en 5 étapes.

1. Cadrage & Éligibilité

Action : Valider formellement votre statut (EE/EI) et le périmètre des services/activités concernés.

Livrable : Note de cadrage validée par la direction.

2. Diagnostic & Analyse d'Écarts

Action : Mener un audit pour évaluer votre maturité par rapport aux 10 mesures de l'Article 21. S'appuyer sur des référentiels (ISO 27001, guides ANSSI).

Livrable : Rapport d'audit avec cartographie des risques et des écarts.

3. Plan d'Action & Validation

Action : Construire une feuille de route de remédiation priorisée, chiffrée et planifiée. La faire approuver par l'organe de direction.

Livrable : Plan d'action validé avec budget et planning.

4. Mise en Œuvre Opérationnelle

Action : Déployer les mesures techniques et organisationnelles. Rédiger les politiques (PSSI, PCA...). Former les dirigeants et les équipes.

Livrable : Preuves de mise en œuvre (configurations, PV de formation...).

5. Pilotage & Amélioration Continue

Action : Définir des indicateurs (KPIs), mener des audits internes réguliers et des exercices de crise. Mettre en place une veille réglementaire.

Livrable : Tableau de bord de conformité.

Au-delà de l’obligation : faire de la conformité NIS 2 un avantage concurrentiel.

La conformité NIS 2 n’est pas une ligne d'arrivée, c’est une nouvelle norme de marché. Les organisations qui l’intègrent pleinement dans leur stratégie en tireront des bénéfices durables.

- **Gagner des marchés :** La conformité devient un critère de sélection incontournable dans les appels d’offres.
- **Renforcer la confiance :** Une posture de sécurité robuste est un gage de fiabilité pour vos clients, partenaires et investisseurs.
- **Améliorer la résilience :** Structurer sa défense, c'est réduire le risque d'interruption d’activité et ses coûts.
- **Valoriser l'entreprise :** Une maturité cyber avérée est un actif stratégique qui augmente la valeur de votre organisation.

La question n’est plus **si* vous devez vous conformer, mais *comment* cette démarche va renforcer votre positionnement et sécuriser votre avenir.