

GUIDE

NIS2 : le guide pratique pour PME & ETI

Obligations, calendrier, sanctions et plan d'action concret

Sedona Radar — audit de sécurité externe automatisé

Sedona AI Lecture 11 min Édition 2026 sedona-ai.com

NIS2 doit élargir massivement le cercle des entreprises françaises soumises à des obligations de cybersécurité : d'environ 500 opérateurs sous NIS1 à environ 15 000 entités, selon l'estimation de l'étude d'impact du projet de loi de transposition (octobre 2024). Si vous dirigez une PME ou une ETI dans l'un des 18 secteurs couverts, vous êtes probablement concerné — et la responsabilité personnelle des dirigeants est explicitement engagée. Un point de vigilance essentiel avant tout : à la mi-2026, la loi française de transposition n'est pas encore promulguée. Les exigences ne sont donc pas encore juridiquement applicables et sanctionnables en France, mais leur cadre est connu. Ce guide vous donne l'essentiel factuel et un plan d'action pour prendre de l'avance sereinement, sans attendre le décret.

À retenir

- NIS2 (directive UE 2022/2555) doit élargir massivement le périmètre : d'environ 500 opérateurs sous NIS1 à environ 15 000 entités en France (estimation de l'étude d'impact du projet de loi, octobre 2024), sur 18 secteurs.
- À la mi-2026, la loi française de transposition n'est PAS promulguée : les exigences ne sont pas encore applicables ni sanctionnables en France, et la Commission européenne a saisi la Cour de justice de l'UE contre la France le 8 juillet 2026.
- Deux catégories d'entités (essentiels et importants) déterminées par le croisement secteur (annexe I/II) × taille — la taille seule ne suffit pas : une grande entreprise en annexe II reste « importante ». S'y ajoutent une responsabilité personnelle des dirigeants, des mesures « tous risques » (art. 21) et une notification d'incident à trois paliers : 24 h / 72 h / 1 mois.
- Sanctions différenciées : jusqu'à 10 M€ ou 2 % du CA mondial pour les entités essentielles, 7 M€ ou 1,4 % pour les entités importantes (montants issus de la directive, à confirmer dans le texte français final).
- Agir dès maintenant via un plan en 6 étapes (cartographier, analyser, prioriser, déployer, préparer la notification, piloter) permet d'éviter une mise en conformité dans l'urgence.

01 1. NIS2 en une page

NIS2 est la directive (UE) 2022/2555 du 14 décembre 2022. Elle abroge et remplace la directive NIS1 de 2016 pour relever le niveau de cybersécurité dans l'ensemble de l'Union européenne. Entrée en vigueur en janvier 2023, elle fixait aux États membres une échéance de transposition au 17 octobre 2024.

Ce qui change par rapport à NIS1 : un périmètre beaucoup plus large (18 secteurs contre une poignée d'opérateurs d'importance vitale), deux catégories d'entités régulées avec des régimes de supervision différenciés, des obligations de gestion des risques harmonisées et « tous risques », un régime de notification d'incidents à paliers stricts, et surtout une responsabilisation directe des organes de direction.

Dimension	NIS1 (2016)	NIS2 (2022)
Périmètre France	~500 opérateurs	~15 000 entités estimées
Secteurs	Périmètre restreint (OIV / OSE)	18 secteurs (annexes I et II)
Catégories	Opérateurs de services essentiels	Entités essentielles (EE) et importantes (EI)
Supervision	Ciblée	Ex ante pour les EE, ex post pour les EI
Dirigeants	Peu explicite	Responsabilité engagée, formation obligatoire

Statut juridique en France (mi-2026) : à connaître avant tout

NIS2 n'est PAS encore en vigueur en France. La loi de transposition (projet de loi relatif à la résilience des infrastructures critiques et au renforcement de la cybersécurité, qui transpose aussi la directive REC et la directive (UE) 2022/2556, volet DORA) reste bloquée au Parlement. Adoptée par le Sénat en première lecture les 11-12 mars 2025 et votée en commission spéciale à l'Assemblée nationale les 9-10 septembre 2025, elle n'a pas été inscrite à la session extraordinaire de juillet 2026 (blocage notamment sur l'article 16 bis relatif au chiffrage). Les obligations ne deviendront applicables et sanctionnables qu'une fois la loi ET les décrets/arrêtés promulgués.

Pourquoi agir maintenant malgré tout

La France a manqué l'échéance du 17 octobre 2024 et fait l'objet d'une procédure d'infraction : mise en demeure le 28 novembre 2024, avis motivé le 7 mai 2025, puis renvoi devant la Cour de justice de l'UE annoncé le 8 juillet 2026 (avec l'Irlande, l'Espagne et les Pays-Bas). Les entreprises qui structurent leur cybersécurité en amont éviteront une mise en conformité dans l'urgence.

02 2. Suis-je concerné ?

NIS2 distingue deux catégories d'entités régulées — essentielles et importantes. La catégorie ne dépend pas de la seule taille : elle résulte du croisement du secteur d'activité (annexe I, dite « haute criticité », ou annexe II, « autres secteurs critiques ») avec la taille de l'entreprise. En simplifiant : les grandes entreprises des secteurs de l'annexe I sont essentielles ; les entreprises moyennes de l'annexe I, ainsi que les entreprises moyennes et grandes de l'annexe II, sont importantes. Certaines entités sont par ailleurs concernées quelle que soit leur taille. Le régime de supervision est plus strict et ex ante pour les entités essentielles ; il est ex post (déclenché sur incident ou plainte) pour les entités importantes.

18

Secteurs d'activité couverts par NIS2 (annexes I et II)
Numeum

Taille de l'entité	Secteur annexe I (haute criticité)	Secteur annexe II (autres secteurs critiques)
Grande (≥ 250 salariés, ou > 50 M€ de CA et > 43 M€ de bilan)	Entité essentielle — supervision ex ante	Entité importante — supervision ex post
Moyenne (50 à 249 salariés, ou 10 à 50 M€ de CA / bilan)	Entité importante — supervision ex post	Entité importante — supervision ex post

Comment lire ce tableau

La répartition entre entités essentielles et importantes découle de la directive elle-même : elle croise les annexes I/II avec les seuils de taille issus de la définition européenne des entreprises (50 salariés / 10 M€, 250 salariés / 50 M€ de CA ou 43 M€ de bilan). La France transpose ce cadre et peut y ajouter des entités au niveau national, mais n'invente pas la répartition. Point de vigilance : une grande entreprise relevant d'un secteur de l'annexe II reste « importante », pas « essentielle ». Certaines entités sont par ailleurs concernées quelle que soit leur taille (par exemple certains fournisseurs d'infrastructures numériques ou de services de confiance, ou des administrations). Vérifiez votre situation au cas par cas via le service MonEspaceNIS2.

L'effet ricochet via la chaîne d'approvisionnement : même si votre entreprise n'est pas directement dans le périmètre, vos clients régulés devront sécuriser leur chaîne d'approvisionnement (article 21). Concrètement, ils vous demanderont des garanties contractuelles et des preuves de votre posture de sécurité. NIS2 se diffuse ainsi bien au-delà des seules entités régulées.

~1 500

Collectivités territoriales et organismes rattachés estimés dans le périmètre du projet de loi
Sénat

- ☐ Mon activité relève-t-elle d'un des 18 secteurs des annexes I ou II ?
- ☐ Mon secteur est-il en annexe I (haute criticité) ou en annexe II (autres secteurs critiques) ? Cela conditionne ma catégorie autant que ma taille.
- ☐ Ai-je au moins 50 salariés OU plus de 10 M€ de CA / bilan ?
- ☐ Suis-je fournisseur d'une entité régulée qui va me demander des garanties de sécurité ?
- ☐ Suis-je une entité pouvant être concernée indépendamment de ma taille (infrastructure numérique, service de confiance, administration) ?
- ☐ Ai-je vérifié ma situation via MonEspaceNIS2 (cyber.gouv.fr) ?

03 3. Vos obligations

Les obligations NIS2 s'organisent autour de quatre grands blocs : la gouvernance et la responsabilité des dirigeants, les mesures de gestion des risques de l'article 21, la notification d'incidents à paliers, et l'enregistrement auprès de l'ANSSI.

Gouvernance et responsabilité personnelle des dirigeants (article 20) : les organes de direction doivent approuver les mesures de gestion des risques de cybersécurité et suivre des formations dédiées. Leur responsabilité est explicitement engagée. La cybersécurité cesse d'être un sujet purement technique : elle devient un enjeu de gouvernance au niveau de la direction.

Mesures de gestion des risques (article 21) : la directive impose une approche « tous risques » avec des mesures techniques, opérationnelles et organisationnelles proportionnées à l'exposition de l'entité.

- Analyse des risques et politiques de sécurité des systèmes d'information
- Gestion des incidents (détection, réponse, traitement)
- Continuité d'activité et gestion des sauvegardes
- Sécurité de la chaîne d'approvisionnement (fournisseurs et prestataires)
- Chiffrement et cryptographie
- Contrôle d'accès et gestion des identités
- Hygiène informatique de base et formation du personnel

Notification d'incidents : NIS2 impose un signalement à l'autorité compétente (l'ANSSI en France) selon trois paliers de temps.

1 Sous 24 h — alerte précoce

Signalement initial indiquant notamment si l'incident est vraisemblablement d'origine malveillante ou susceptible d'avoir un impact transfrontalier.

2 Sous 72 h — notification d'incident

Évaluation initiale : gravité, impact et indicateurs de compromission connus à ce stade.

3 Sous 1 mois — rapport final

Description détaillée de l'incident, cause, mesures de remédiation et impact transfrontalier. Des rapports d'étape intermédiaires peuvent être demandés.

Le délai de 24 h se prépare à froid

Tenir 24 h pour une alerte précoce est impossible à improviser en pleine crise. Préparez dès aujourd'hui une procédure de notification : qui décide, qui rédige, avec quels modèles, vers quel canal ANSSI. C'est l'un des livrables les plus rentables de votre mise en conformité.

Enregistrement auprès de l'ANSSI : les entités concernées devront s'enregistrer. Le service MonEspaceNIS2 (cyber.gouv.fr) est mis en place pour l'identification et l'enregistrement des entités. L'obligation précise et ses modalités seront fixées par les textes de transposition, non encore promulgués à mi-2026.

04 4. Sanctions et risques

Le régime de sanctions de NIS2 est différencié : il est plus élevé pour les entités essentielles que pour les entités importantes, et il prévoit des mesures visant directement les dirigeants. Attention : les montants ci-dessous proviennent de la directive et d'analyses juridiques ; leur transcription exacte en droit français dépendra de la loi finale, non encore promulguée.

10 M€ ou 2 % du CA mondial

Amende maximale pour les entités essentielles (le montant le plus élevé s'applique)
Legiscope

7 M€ ou 1,4 % du CA mondial

Amende maximale pour les entités importantes (le montant le plus élevé s'applique)
Legiscope

Type de mesure	Entité essentielle	Entité importante
Amende maximale	≥ 10 M€ ou 2 % du CA mondial	≥ 7 M€ ou 1,4 % du CA mondial
Supervision	Ex ante (proactive)	Ex post (sur incident/plainte)
Mesures sur dirigeants	Suspension temporaire possible	Cadre plus limité
Certificats / autorisations	Suspension temporaire possible	—

Au-delà de l'amende, le risque le plus sous-estimé est réputationnel et opérationnel. Une suspension temporaire de dirigeant ou d'autorisation pour une entité essentielle, ou la révélation publique d'un incident mal géré, peut fragiliser durablement la confiance des clients, des partenaires et des financeurs. Dans une logique de chaîne d'approvisionnement, un maillon non conforme peut être écarté d'appels d'offres.

Ne pas confondre obligation européenne et sanction immédiate en France

Tant que la loi de transposition n'est pas promulguée, NIS2 n'est pas une obligation légale sanctionnable en France. C'est une obligation européenne dont le délai de transposition est échu depuis le 17 octobre 2024. Vérifiez toujours le texte promulgué avant de citer des montants comme applicables en droit français.

05 5. Plan d'action en 6 étapes

La bonne nouvelle : l'essentiel de NIS2 relève de bonnes pratiques de sécurité que vous pouvez déployer dès maintenant, sans attendre le décret. Voici une trajectoire pragmatique pour PME et ETI, de l'état des lieux au pilotage dans la durée.

1. Cartographier votre surface d'exposition

Recensez vos actifs exposés sur Internet (domaines, sous-domaines, services, IP, applications). On ne protège pas ce qu'on ne connaît pas. C'est le préalable à toute analyse de risque crédible.

2. Analyser les risques

Évaluez vos vulnérabilités et votre écart aux exigences (analyse de risques, incidents, continuité, chaîne d'appro, chiffrement, contrôle d'accès, hygiène). Objectivez la posture plutôt que de l'estimer.

3. Prioriser

Classez les écarts par criticité et par effort. Traitez d'abord les vulnérabilités exposées et exploitables, puis les manques structurants (gouvernance, procédures).

4. Déployer les mesures

Mettez en œuvre les mesures de l'article 21 de façon proportionnée : correctifs, durcissement, sauvegardes testées, gestion des accès, sensibilisation. Faites approuver le plan par la direction (article 20).

5. Préparer la notification d'incident

Formalisez la procédure 24 h / 72 h / 1 mois : rôles, modèles de rapport, canal ANSSI, exercices. Testez-la au moins une fois à froid.

6. Piloter dans la durée

Instaurez un suivi continu (scans réguliers, revue des risques, indicateurs pour la direction, formation récurrente des dirigeants). La conformité est un état à maintenir, pas un projet ponctuel.

Documenter au fil de l'eau

Conservez la trace de vos décisions, mesures et exercices. En cas de contrôle ex ante (entités essentielles) ou de plainte (entités importantes), la capacité à démontrer une démarche structurée compte autant que les mesures elles-mêmes.

06 6. Comment Sedona Radar s'inscrit dans votre démarche

Sedona.AI est une société française basée à Perpignan, editrice de Sedona Radar. Nous vous aidons à évaluer et à améliorer votre posture ; nous ne délivrons pas de certification officielle.

Sedona Radar (79 € HT/mois pour le plan Starter) est un audit de sécurité externe automatisé : il analyse ce que votre domaine expose sur Internet et remet un rapport en français, avec un plan de correction. Il donne aussi des indicateurs de maturité sur 6 référentiels : NIS2, RGPD, ISO 27001, ANSSI Hygiène, OWASP Top 10 et Cadre Sedona (grille propre à Sedona, qui n'est pas un référentiel de l'ANSSI). Concrètement, Radar outille les étapes 1, 2 et 6 du plan d'action : cartographier, analyser, suivre dans le temps.

Évaluer n'est pas certifier

Radar donne des indicateurs de maturité : il ne certifie rien, et il n'existe aucune certification NIS2. Si un texte ou un client exige un audit par un prestataire qualifié PASSI, adressez-vous à l'un des prestataires de la liste publiée par l'ANSSI. Sedona.AI n'est ni qualifiée PASSI ni certifiée ISO 27001.

- Audit OSINT des dirigeants, audit de surface manuel et simulation de phishing, en complément du produit
- Formations de sensibilisation à la cybersécurité pour vos équipes

Notre conviction : la meilleure façon de préparer NIS2 n'est pas d'attendre le décret, mais de bâtir dès maintenant une posture de sécurité mesurable et pilotable. Le jour où la loi sera promulguée, vous serez prêt plutôt que dans l'urgence.

§ Sources

1. Commission européenne — NIS2 Directive (digital-strategy) — <https://digital-strategy.ec.europa.eu/en/policies/nis2-directive>
2. Commission européenne — Renvoi de la France devant la CJUE (8 juillet 2026) — <https://digital-strategy.ec.europa.eu/en/news/commission-refers-ireland-spain-france-and-netherlands-court-justice-failing-transpose-rules>
3. ANSSI — FAQ MonEspaceNIS2 (avancement de la transposition) — <https://aide.monespacenis2.cyber.gouv.fr/fr/article/avancement-de-la-transposition-de-la-directive-nis-2-1b3j1da/>
4. Sénat — Dossier législatif (résilience des infrastructures critiques et cybersécurité) — <https://www.senat.fr/travaux-parlementaires/textes-legislatifs/la-loi-en-clair/projet-de-loi-relatif-a-la-resilience-des-infrastructures-critiques-et-au-renforcement-de-la-cybersecurite.html>
5. Numeum — Directive NIS2, nouvelles exigences — <https://numeum.fr/cybersecurite/directive-nis2-quelles-nouvelles-exigences-pour-les-organisations-en-france/>
6. Meldis — Entité essentielle ou importante NIS2 — <https://meldis.fr/blog/nis2-entites-essentielles-importantes/>
7. Leto — Guide NIS2 (UE) 2022/2555 — <https://www.letto.legal/guides/nis-2-definition>
8. ip-label — Directive NIS2, notifications 24h/72h — <https://ip-label.com/fr/directive-nis2/>
9. Legiscopes — Transposition NIS2 France — <https://www.legiscopes.com/blog/transposition-nis2-france.html>

Voyez votre exposition, point de départ de votre préparation

Sedona Radar analyse ce que votre domaine expose sur Internet et donne des indicateurs de maturité sur six référentiels dont NIS2. Un point de départ concret pour votre plan d'action : une évaluation, pas une certification. Lancez un scan gratuit.

Lancer mon scan gratuit

sedona-ai.com/scan-gratuit