



CHECKLIST

Checklist NIS2 — êtes-vous concerné et par où commencer ?

18 points d'auto-évaluation pour cadrer votre mise en conformité NIS2

Sedona Radar — audit de sécurité externe automatisé

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

La réponse courte : vous êtes probablement concerné par NIS2 si votre organisation exerce dans l'un des 18 secteurs des annexes I et II de la directive ET atteint les seuils de taille européens (au moins 50 salariés ou plus de 10 M€ de chiffre d'affaires). Une nuance de calendrier, essentielle à comprendre : à la mi-2026, la loi française de transposition n'est pas encore promulguée. NIS2 n'est donc pas encore une obligation légale sanctionnable en France — mais les exigences de fond (gouvernance, mesures techniques, notification d'incident) sont déjà connues. Cette checklist de 18 points vous permet de cadrer votre situation et d'engager les chantiers sans attendre la publication des décrets. Cochez, priorisez, agissez.

À retenir

- Vous êtes concerné si vous relevez de l'un des 18 secteurs des annexes I/II ET atteignez les seuils de taille (≥ 50 salariés ou > 10 M€ de CA) — ou si vous êtes dans la chaîne d'approvisionnement d'un opérateur critique.
- Entité essentielle ou importante ne dépend pas de la seule taille : le classement croise la taille ET l'annexe. Une grande entité de l'annexe II reste « importante » ; certaines entités (DNS, télécoms, prestataires de confiance qualifiés) sont « essentielles » quelle que soit leur taille.
- À la mi-2026, NIS2 n'est pas encore en vigueur en France : la loi de transposition reste bloquée au Parlement et la France est renvoyée devant la CJUE. Se préparer maintenant est un choix stratégique, pas une obligation déjà sanctionnable.
- Quatre chantiers structurent la mise en conformité : gouvernance impliquant la direction, socle technique (MFA, correctifs, sauvegardes, journalisation, chiffrage, chaîne d'appro), et capacité de détection/notification 24 h / 72 h / 1 mois.
- Les sanctions prévues par l'article 34 de la directive (jusqu'à 10 M€ ou 2 % du CA pour les EE) ne seront applicables en France qu'après promulgation de la loi ; ne les citez pas comme déjà en vigueur.
- La qualification définitive et les modalités précises passeront par les textes français et le service MonEspaceNIS2 de l'ANSSI : vérifiez votre cas au cas par cas.

01 Où en est NIS2 en France ? (le contexte à connaître avant de cocher)

NIS2 est la directive (UE) 2022/2555 du 14 décembre 2022, qui remplace la directive NIS1 de 2016 pour relever le niveau de cybersécurité dans l'Union. L'échéance de transposition par les États membres était fixée au 17 octobre 2024. La France a manqué cette échéance et fait l'objet d'une procédure d'infraction : la Commission a annoncé le 8 juillet 2026 son renvoi devant la Cour de justice de l'UE, aux côtés de l'Irlande, de l'Espagne et des Pays-Bas.

En France, NIS2 doit être transposée par le 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). Ce texte a été adopté par le Sénat en première lecture les 11-12 mars

2025 et voté en commission spéciale à l'Assemblée nationale les 9-10 septembre 2025, mais il reste bloqué au stade parlementaire — notamment sur l'article 16 bis relatif au chiffrage — et n'a pas été inscrit à la session extraordinaire de juillet 2026.

Point d'honnêteté sur le statut juridique

À la date de rédaction (mi-2026), la loi de transposition n'est PAS promulguée : NIS2 n'est pas encore en vigueur en France. Les obligations concrètes (enregistrement ANSSI, détail des mesures de l'article 21, montants d'amendes en droit français, calendrier d'application aux entités) seront fixées par la loi ET par des décrets et arrêtés non encore publiés. Se préparer maintenant est un choix de bon sens, pas une obligation déjà sanctionnable.

17 octobre 2024

Échéance de transposition de NIS2 fixée aux États membres par la directive (non respectée par la France)

Commission européenne

~15 000

Estimation du nombre d'entités concernées en France par NIS2 (étude d'impact du projet de loi de transposition, octobre 2024), contre ~500 opérateurs sous NIS1

Étude d'impact du projet de loi de transposition de NIS2, octobre 2024

02 Partie 1 — Suis-je concerné ?

Deux critères se combinent : le secteur d'activité (annexes I et II) et la taille de l'entité. Selon le résultat, vous relevez de la catégorie « entité essentielle » (EE) ou « entité importante » (EI), avec des régimes de supervision et de sanction distincts. Cochez chaque point ci-dessous.

☐ Mon secteur figure aux annexes I ou II de NIS2 — La directive couvre 18 secteurs, répartis entre l'annexe I « secteurs hautement critiques » (énergie, transports, banque, santé, eau potable et eaux usées, infrastructures numériques, administration publique, espace...) et l'annexe II « autres secteurs critiques » (services postaux, gestion des déchets, industrie agroalimentaire, fabrication, fournisseurs numériques, recherche...). Vérifiez la liste précise dans les annexes avant toute autre étape.

☐ J'atteins les seuils de taille européens — Sont généralement concernées les moyennes et grandes entreprises : à partir de 50 salariés OU plus de 10 M€ de chiffre d'affaires ou de bilan. En deçà, vous n'êtes en principe pas visé, sauf exception sectorielle.

☐ Je sais si je suis « entité essentielle » (EE) ou « entité importante » (EI) — Le classement croise la taille ET l'annexe, il ne dépend pas de la seule taille. Ordre de grandeur : EE ≈ grandes entités (250+ salariés, ou > 50 M€ de CA / 43 M€ de bilan) relevant de l'annexe I, plus certaines entités essentielles quelle que soit leur taille (DNS, registres de noms de domaine de premier niveau, télécoms, prestataires de services de confiance qualifiés) ; EI ≈ entités moyennes de l'annexe I ET entités de l'annexe II (y compris les grandes, ex. services postaux, gestion des déchets, agroalimentaire, fabrication, fournisseurs numériques, recherche). Une grande ETI industrielle relevant de l'annexe II reste « importante », pas « essentielle ». Le régime de supervision est ex ante pour les EE, ex post (sur incident ou plainte) pour les EI. En cas de doute, reportez-vous aux textes officiels et à MonEspaceNIS2.

☐ J'ai vérifié les exceptions liées à mon rôle ou à mes clients — Certaines entités sont concernées quelle que soit leur taille (ex. infrastructures critiques, DNS, télécoms, prestataires de confiance qualifiés). Si vous êtes sous-traitant ou fournisseur d'un opérateur critique / d'une entité essentielle, vos obligations peuvent découler de la sécurité de leur chaîne d'approvisionnement, même en dessous des seuils.

L'outil officiel de référence

La qualification définitive (concerné ou non, EE ou EI, secteur exact) sera précisée par les textes français et par le service MonEspaceNIS2 de l'ANSSI (cyber.gouv.fr). En cas de doute, ne tranchez pas seul : la répartition précise par secteur et les exceptions seront officialisées par la loi et les décrets.

03 Partie 2 — Gouvernance

NIS2 fait de la cybersécurité une responsabilité de direction (article 20). Les dirigeants approuvent les mesures, suivent des formations et voient leur responsabilité engagée. La gouvernance n'est pas un supplément : c'est le socle.

☐ Ma direction est formée et responsabilisée — Les organes de direction doivent approuver les mesures de gestion des risques et suivre une formation à la cybersécurité. Leur responsabilité peut être engagée. Formalisez cette implication (décision documentée, formation tracée).

☐ J'ai réalisé une analyse de risques — L'article 21 impose une approche « tous risques » : identifier les actifs, les menaces et les impacts, puis prioriser les mesures de manière proportionnée. C'est le document fondateur dont découlent tous les autres.

☐ Je dispose d'une politique de sécurité des systèmes d'information (PSSI) — Une politique écrite, validée par la direction, qui fixe les règles, les rôles et les objectifs de sécurité, et sert de référence pour l'ensemble des mesures techniques et organisationnelles.

- ☐ J'ai désigné un référent cybersécurité — Une personne (interne ou appuyée par un prestataire) clairement identifiée comme point de contact, chargée du pilotage de la conformité, du suivi des mesures et de la relation avec l'ANSSI.

Bonne pratique

Adossez votre PSSI et votre analyse de risques à un référentiel reconnu — le Guide d'hygiène informatique de l'ANSSI est un excellent point de départ pour une PME/ETI, avant d'aller vers ISO 27001 ou les CIS Controls si votre maturité le justifie.

04 Partie 3 — Mesures techniques

L'article 21 énumère les mesures techniques, opérationnelles et organisationnelles minimales : contrôle d'accès, gestion des vulnérabilités, sauvegardes et continuité, journalisation, chiffrement, sécurité de la chaîne d'approvisionnement, hygiène et formation. Voici les six chantiers techniques à cocher.

- ☐ J'ai déployé l'authentification multifacteur (MFA) et le moindre privilège — MFA sur tous les accès sensibles (messagerie, VPN, administration, cloud) et principe du moindre privilège : chaque compte n'a que les droits strictement nécessaires. C'est la mesure au meilleur rapport effort/impact contre la compromission de comptes.
- ☐ Je gère les vulnérabilités et les correctifs — Inventaire des actifs exposés, détection des vulnérabilités, priorisation et application des correctifs dans des délais maîtrisés. La gestion de la surface d'attaque externe et le patch management sont explicitement attendus.
- ☐ Mes sauvegardes sont testées et isolées — Sauvegardes régulières, dont au moins une copie hors-ligne ou immuable, restaurations testées périodiquement. La sauvegarde est le dernier rempart contre le rançongiciel et une composante de la continuité d'activité exigée par l'article 21.
- ☐ Je journalise et je conserve les traces — Collecte et conservation des journaux (systèmes, réseau, authentification) pour détecter les incidents et fournir des preuves. Sans journalisation, ni détection fiable ni notification étayée ne sont possibles.
- ☐ J'ai sécurisé la messagerie et le chiffrement — Protection de la messagerie (anti-hameçonnage, SPF/DKIM/DMARC) et chiffrement des données sensibles en transit et au repos. Le chiffrement figure explicitement parmi les mesures de l'article 21.
- ☐ Je maîtrise la sécurité de ma chaîne d'approvisionnement — Évaluation de la sécurité des fournisseurs et prestataires critiques, clauses contractuelles de sécurité, suivi des risques liés aux tiers. NIS2 étend la responsabilité au-delà du périmètre propre de l'entité.

05 Partie 4 — Détection, notification & preuves

Prévenir ne suffit pas : NIS2 impose de détecter, de notifier dans des délais stricts et de prouver ce qui a été fait. Le régime de notification à l'ANSSI se déroule en trois paliers.

Palier	Délai	Contenu attendu
Alerte précoce	24 heures	Signalement initial indiquant si l'incident est vraisemblablement malveillant ou à impact transfrontalier
Notification d'incident	72 heures	Évaluation initiale : gravité, impact, indicateurs de compromission
Rapport final	1 mois	Description détaillée, cause, remédiation, impact transfrontalier (des rapports d'étape peuvent être demandés)

- ☐ Je dispose d'une capacité de détection d'incident — Moyens (techniques et/ou externalisés) pour repérer un incident de sécurité rapidement : supervision, alertes, corrélation de journaux. On ne notifie que ce que l'on détecte.
- ☐ J'ai une procédure de notification 24 h / 72 h / 1 mois — Un processus écrit et testé pour alerter l'ANSSI dans les délais : qui décide, qui rédige, quelles informations, par quel canal. À préparer avant l'incident, jamais pendant.
- ☐ J'ai un plan de continuité et de gestion de crise — Plan de continuité et de reprise d'activité (PCA/PRA), procédures de gestion de crise et exercices, pour limiter l'impact et restaurer les services. La continuité d'activité est une exigence explicite de l'article 21.
- ☐ Je prépare mon enregistrement ANSSI et ma traçabilité — Anticipez l'enregistrement des entités via MonEspaceNIS2 et tenez à jour les preuves de conformité (analyses, décisions de direction, journaux, tests de restauration). Ces éléments seront votre défense en cas de contrôle.

06 Les sanctions : ce que dit la directive

NIS2 prévoit un régime de sanctions plus élevé pour les entités essentielles que pour les entités importantes, et des mesures visant directement les dirigeants (jusqu'à la suspension temporaire pour les EE). Ces plafonds sont fixés par l'article 34 de la directive (UE) 2022/2555. Attention : 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 des deux)

Directive (UE) 2022/2555, art. 34 (EUR-Lex)

7 M€ ou 1,4 % du CA mondial

Amende maximale pour les entités importantes (le montant le plus élevé des deux)

Directive (UE) 2022/2555, art. 34 (EUR-Lex)

À vérifier avant de citer ces montants

Ces plafonds sont issus de l'article 34 de la directive européenne. Les montants applicables en France ne seront fixés qu'à la promulgation de la loi de transposition. Ne les présentez pas comme des sanctions déjà applicables en droit français.

07 Par où commencer concrètement

1 Statuer sur votre éligibilité

Croisez votre secteur (annexes I/II) et vos seuils de taille. Déterminez si vous êtes potentiellement EE ou EI — en tenant compte de l'annexe et non de la seule taille — ou concerné via la chaîne d'approvisionnement d'un opérateur critique.

2 Poser la gouvernance

Faites approuver la démarche par la direction, lancez l'analyse de risques, rédigez ou actualisez la PSSI et désignez un référent.

3 Mesurer votre surface d'attaque et vos écarts

Cartographiez vos actifs exposés, identifiez vos vulnérabilités et évaluez votre écart aux mesures de l'article 21 (MFA, correctifs, sauvegardes, journalisation, chiffrage, chaîne d'appro).

4 Prioriser et remédier

Traitez d'abord les risques critiques (comptes exposés sans MFA, vulnérabilités exploitables, absence de sauvegarde testée), puis déroulez le reste du plan de manière proportionnée.

5 Préparer la détection et la notification

Mettez en place la journalisation, une capacité de détection et la procédure de notification 24 h / 72 h / 1 mois. Anticipez l'enregistrement MonEspaceNIS2 dès que les modalités seront publiées.

Comment Sedona Radar s'inscrit dans cette démarche

Sedona Radar est un audit de sécurité externe automatisé : il analyse ce que votre domaine expose sur Internet et donne des indicateurs de maturité sur six référentiels, dont NIS2. Il éclaire les étapes 3 et 4 (mesure des écarts, priorisation). Point d'honnêteté : Radar ne certifie rien, et il n'existe aucune certification NIS2.

1. EUR-Lex — Directive (UE) 2022/2555 (NIS2), texte consolidé (dont art. 34 sanctions) — <https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX:32022L2555>
2. Commission européenne — NIS2 Directive (digital-strategy) — <https://digital-strategy.ec.europa.eu/en/policies/nis2-directive>
3. 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>
4. 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/>
5. Sénat — Projet de loi 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>
6. Numeum — Directive NIS2 : nouvelles exigences — <https://numeum.fr/cybersecurite/directive-nis2-quelles-nouvelles-exigences-pour-les-organisations-en-france/>
7. Meldis — Entité essentielle ou importante NIS2 — <https://meldis.fr/blog/nis2-entites-essentielles-importantes/>
8. Leto — Guide NIS2 (UE) 2022/2555 — <https://www.letto.legal/guides/nis-2-definition>
9. ip-label — Directive NIS2 : notifications 24h/72h — <https://ip-label.com/fr/directive-nis2/>
10. Legiscopes — Transposition NIS2 France — <https://www.legiscopes.com/blog/transposition-nis2-france.html>

Voyez ce que vous exposez aujourd'hui

Sedona Radar analyse ce que votre domaine expose sur Internet et remet un rapport en français, avec un plan de correction. Il donne des indicateurs de maturité sur six référentiels dont NIS2, sans jamais certifier. Lancez un scan gratuit pour objectiver votre point de départ.

Lancer mon scan gratuit

sedona-ai.com/scan-gratuit