

LIVRE BLANC

NIS2 : le guide pour se préparer

Périmètre, échéances, obligations et sanctions prévus par la directive : le manuel de préparation des PME et ETI françaises, de l'analyse d'écart au plan d'action.

Sedona Radar — audit de sécurité externe automatisé

Sedona AI Lecture ~25 min Édition 2026 sedona-ai.com

Sommaire

01	1. Introduction : pourquoi ce guide, et pour qui
02	2. NIS2 en une page (résumé exécutif dirigeant)
03	3. Comprendre NIS2 sans jargon
04	4. Ce qui change par rapport à NIS1
05	5. Panorama chiffré de la menace (UE et France)
06	6. Le coût réel du risque cyber
07	7. Qui est concerné : entités essentielles vs importantes
08	8. Cartographie des 18 secteurs (annexes I et II)
09	9. Suis-je concerné ? Arbre de décision
10	10. Statut de la transposition française et calendrier
11	11. S'enregistrer : MonEspaceNIS2 et le ReCyF
12	12. Gouvernance et responsabilité des dirigeants (art. 20)
13	13. Les 10 mesures de gestion des risques (art. 21)
14	14. Sécurité de la chaîne d'approvisionnement
15	15. Notification d'incident : 24h / 72h / 1 mois (art. 23)
16	16. Sanctions, contrôles et supervision (art. 31-37)
17	17. Articulation avec RGPD, DORA et les autres cadres
18	18. Méthode pas-à-pas : l'analyse d'écart (gap analysis)
19	19. Construire son plan de conformité (feuille de route 3 ans)
20	20. Spécificités et pragmatisme pour PME/ETI
21	21. Erreurs fréquentes et idées reçues
22	22. Checklist, modèles et où s'adresser

La directive NIS2 fait passer la réglementation cyber européenne de quelques centaines d'organisations à environ 15 000 entités en France (estimation de l'étude d'impact du projet de loi de transposition, octobre 2024). Le texte de transposition n'est pas promulgué : les obligations de la directive, et ses sanctions (jusqu'à 10 M€ ou 2 % du chiffre d'affaires mondial pour les entités essentielles), ne sont donc pas encore en vigueur en France. Pour un dirigeant de PME ou d'ETI, le texte est dense, anxiogène, et souvent mal compris : beaucoup se croient hors champ alors qu'ils seront concernés directement ou via leur chaîne d'approvisionnement. Ce livre blanc transforme un texte juridique de plus de cent articles en une méthode d'action pas-à-pas : comprendre, s'auto-évaluer, prioriser et se préparer sans surinvestir. Toutes les données chiffrées proviennent de sources primaires (EUR-Lex, Commission européenne, ANSSI/CERT-FR, ENISA, IBM, Verizon) publiées entre 2023 et 2026.

À retenir

- NIS2 (directive UE 2022/2555) couvre 18 secteurs et environ 15 000 entités en France (estimation de l'étude d'impact du projet de loi, octobre 2024), réparties en entités essentielles et importantes, contre quelques centaines sous NIS1.
- Selon la directive, les dirigeants sont personnellement responsables : l'organe de direction doit approuver, superviser et se former aux mesures de gestion des risques (art. 20), sous peine de suspension de fonctions.
- Le socle opérationnel tient en dix mesures minimales (art. 21) et une chronologie de notification d'incident stricte : 24h / 72h / 1 mois (art. 23).
- La directive prévoit des sanctions allant jusqu'à 10 M€ ou 2 % du CA mondial pour une entité essentielle, 7 M€ ou 1,4 % pour une entité importante (art. 34) ; les montants applicables en France dépendront de la loi de transposition.
- La sécurité de la chaîne d'approvisionnement devient centrale : les tiers sont impliqués dans 30 % des violations, un chiffre qui a doublé en un an (Verizon 2025).
- L'enregistrement des entités est prévu sur la plateforme MonEspaceNIS2 de l'ANSSI, dès que les textes de transposition en fixeront les modalités.
- La bonne méthode : une analyse d'écart honnête, puis une feuille de route à 3 horizons (quick wins 0-3 mois, socle 3-12 mois, maturité 12-36 mois) proportionnée à sa taille et à son risque.

01 1. Introduction : pourquoi ce guide, et pour qui

NIS2 est l'un de ces textes qui produisent deux réactions opposées, également dangereuses : la panique (« il faut tout arrêter et tout refaire ») ou le déni (« ça ne nous concerne pas, on est trop petits »). Les deux se trompent. NIS2 est une directive de proportionnalité : elle demande des mesures adaptées à la taille, au risque et à l'exposition de chaque organisation. Mais elle est aussi contraignante, chiffrée et assortie de sanctions réelles, y compris personnelles pour les dirigeants.

Ce livre blanc s'adresse en priorité aux dirigeants, DSI et RSSI de PME et d'ETI françaises. Il poursuit un objectif simple : vous permettre de comprendre le texte, de déterminer si vous êtes concerné, de vous auto-évaluer, de prioriser, puis de construire un plan de conformité réaliste — sans surinvestir dans des outils avant d'avoir posé la gouvernance.

La posture de ce document

Sedona n'est ni organisme de certification, ni PASSI, ni prestataire de réponse à incident. Ce guide se place en amont : anticipation, pédagogie, cartographie d'exposition et méthode. Il ne se substitue ni à un conseil juridique, ni à un audit de certification, ni à la lecture du texte officiel.

02 2. NIS2 en une page (résumé exécutif dirigeant)

Si vous ne lisez qu'une section, lisez celle-ci. NIS2 est la directive européenne (UE) 2022/2555 qui renforce et élargit la réglementation de cybersécurité issue de NIS1. Elle impose à un large ensemble d'organisations un socle de gouvernance, de mesures techniques et de notification d'incidents, sous supervision d'une autorité nationale — l'ANSSI en France — et sous peine de sanctions financières et personnelles. Au 14/10/2026, la directive n'est pas transposée en droit français : ces obligations et ces sanctions ne sont pas encore opposables en France (voir la section 10).

- Gouvernance et responsabilité personnelle des dirigeants : l'organe de direction approuve, supervise et se forme (art. 20).
- Dix mesures minimales de gestion des risques, dont sauvegardes, gestion des incidents, MFA et sécurité de la supply chain (art. 21).
- Notification des incidents significatifs selon une chronologie stricte 24h / 72h / 1 mois (art. 23).
- Enregistrement de l'entité auprès de l'autorité compétente (MonEspaceNIS2 en France), selon des modalités à fixer par les textes de transposition.
- Sécurité de la chaîne d'approvisionnement et des relations avec les prestataires.

~15 000

Entités concernées par NIS2 en France (estimation), contre quelques centaines sous NIS1.

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

10 M€ ou 2 %

Amende maximale pour une entité essentielle : le montant le plus élevé entre 10 M€ et 2 % du CA annuel mondial (art. 34).

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

Le test des 3 minutes

Mon secteur figure-t-il en annexe I ou II de la directive ? Mon entreprise dépasse-t-elle 50 salariés ou 10 M€ de bilan/CA ? Si oui aux deux, vous êtes très probablement concerné : passez directement aux sections 7 à 9, puis à l'analyse d'écart (section 18).

03 3. Comprendre NIS2 sans jargon

NIS2 poursuit un objectif de résilience collective du marché intérieur européen. L'idée de fond : une chaîne n'est pas plus solide que son maillon le plus faible. En rehaussant le niveau de sécurité d'un grand nombre d'acteurs interdépendants (énergie, santé, transport, numérique, agroalimentaire...), l'Union cherche à réduire l'effet domino d'une cyberattaque sur l'économie et les services essentiels.

Directive vs règlement

Une directive fixe des objectifs communs mais doit être transposée par chaque État membre dans son droit national — d'où des variations d'un pays à l'autre et un calendrier propre à la France. Un règlement (comme le RGPD ou DORA) s'applique directement, sans transposition. NIS2 étant une directive, ce sont la loi française et ses décrets qui en fixent les modalités concrètes.

Terme	Définition simple
Entité essentielle (EE)	Organisation d'un secteur hautement critique et de grande taille, soumise à une supervision proactive.
Entité importante (EI)	Organisation d'un secteur critique, supervisée de manière réactive (après incident ou signalement).
Incident significatif	Incident qui perturbe fortement un service ou peut causer un dommage matériel/immatériel important, déclenchant l'obligation de notification.
CSIRT / CERT-FR	Équipe nationale de réponse aux incidents à laquelle on notifie les incidents (le CERT-FR en France).
Autorité compétente	Organisme de contrôle national — l'ANSSI en France (hors secteur financier relevant de DORA).
Chaîne d'approvisionnement	L'ensemble des fournisseurs et prestataires dont dépend votre système d'information, y compris IT et infogérance.
MonEspaceNIS2	Plateforme officielle d'auto-évaluation et d'enregistrement opérée par l'ANSSI.

04 4. Ce qui change par rapport à NIS1

La Commission européenne a jugé NIS1 insuffisant : périmètre trop étroit, désignation des acteurs laissée à l'appréciation des États, obligations floues et sanctions hétérogènes. NIS2 corrige ces faiblesses en changeant d'échelle et de méthode.

Dimension	NIS1	NIS2
Entités en France	Quelques centaines (OSE désignés)	Environ 15 000 (EE + EI)
Désignation	Auto-désignation / choix des États	Critères objectifs de secteur et de taille
Dirigeants	Peu impliqués	Responsabilité personnelle explicite (art. 20)
Sanctions	Hétérogènes selon les pays	Plafonds harmonisés (art. 34)
Supply chain	Peu traitée	Obligation explicite (art. 21)
Notification	Variable	Chronologie stricte 24h / 72h / 1 mois

Le passage de l'auto-désignation à des critères de taille objectifs est le changement le plus structurant pour les PME et ETI : ce n'est plus à l'État de vous « désigner », c'est à vous de déterminer si vous entrez dans le champ et de vous enregistrer.

05 5. Panorama chiffré de la menace (UE et France)

NIS2 n'est pas une lubie réglementaire : elle répond à une intensification mesurée de la menace. Les autorités observent une hausse continue du volume d'incidents, une professionnalisation des attaquants et un déplacement de la cible vers les organisations de taille intermédiaire, moins protégées que les grands groupes mais plus dépendantes du numérique qu'auparavant.

4 386

Événements de sécurité traités par l'ANSSI en 2024, en hausse de 15 % sur un an.
ANSSI — Panorama de la cybermenace 2024

1 361

Incidents portés à la connaissance de l'ANSSI en 2024, accompagnés de 3 004 signalements.
ANSSI — Panorama de la cybermenace 2024

11 079

Incidents observés à l'échelle de l'Union européenne, dont 322 touchant plusieurs États membres à la fois.

ENISA — Threat Landscape 2024

Le déni est le premier facteur de risque

Les rapports ANSSI et ENISA convergent : DDoS et rançongiciel dominant, les PME/ETI et collectivités sont de plus en plus visées, et la chaîne d'approvisionnement sert de vecteur d'entrée. Se croire « trop petit pour intéresser un attaquant » est précisément le profil ciblé par les campagnes opportunistes automatisées.

06 6. Le coût réel du risque cyber

Le meilleur argument pour investir dans la conformité n'est pas l'amende : c'est le coût d'un incident. Une violation combine arrêt d'activité, remédiation technique, perte de clients, atteinte à la réputation et, souvent, rançon. Pour une PME ou une ETI, un seul incident majeur peut menacer la continuité de l'entreprise.

4,44 M\$

Coût moyen mondial d'une violation de données en 2025 (10,22 M\$ aux États-Unis).

IBM — Cost of a Data Breach Report 2025

44 %

Part des violations de données impliquant un rançongiciel en 2025, en hausse de 37 % sur un an.

Verizon — 2025 Data Breach Investigations Report

88 %

Part des violations touchant les PME qui impliquent un rançongiciel, contre 39 % pour les grandes organisations.

Verizon — 2025 Data Breach Investigations Report

241 jours

Cycle de vie moyen d'une violation en 2025 (181 jours pour détecter, 60 pour contenir).

IBM — Cost of a Data Breach Report 2025

NIS2 comme réduction de risque assurable

Bien pensée, la conformité ne se lit pas comme un coût sec mais comme une baisse de la probabilité et de l'impact d'un sinistre — donc comme un levier sur la continuité d'activité, la confiance client et, de plus en plus, l'assurabilité cyber. Les organisations qui déploient largement automatisation et IA défensive réduisent nettement le cycle de vie d'une violation.

07 7. Qui est concerné : entités essentielles vs importantes

NIS2 distingue deux catégories, qui diffèrent par le régime de supervision et le plafond de sanction. Les entités essentielles (EE) relèvent des secteurs hautement critiques (annexe I) et sont soumises à une supervision proactive, ex ante : l'autorité peut contrôler sans attendre un incident. Les entités importantes (EI) relèvent des autres secteurs critiques (annexe II) et sont supervisées de manière réactive, ex post : les contrôles interviennent surtout après un signalement ou un incident.

Critère	Entité essentielle (EE)	Entité importante (EI)
Secteurs	Annexe I (hautement critiques)	Annexe II (autres critiques)
Supervision	Proactive (ex ante)	Réactive (ex post)
Amende max.	10 M€ ou 2 % du CA mondial	7 M€ ou 1,4 % du CA mondial

Taille	Seuils indicatifs
Moyenne entreprise	≥ 50 salariés OU > 10 M€ de CA/bilan annuel
Grande entreprise	≥ 250 salariés OU > 50 M€ de CA (et > 43 M€ de bilan)

Attention aux exceptions de taille

Certaines entités sont concernées quelle que soit leur taille en raison de leur criticité : fournisseurs de DNS, registres de noms de domaine, certains opérateurs de communications électroniques, administrations publiques, etc. Une petite structure peut donc être dans le champ même sous les seuils. Vérifiez toujours votre cas précis auprès de MonEspaceNIS2.

08 8. Cartographie des 18 secteurs (annexes I et II)

18 secteurs

Secteurs couverts par NIS2, répartis entre secteurs hautement critiques (annexe I) et autres secteurs critiques (annexe II).

Directive (UE) 2022/2555, annexes I et II — EUR-Lex

Annexe I — hautement critiques	Annexe II — autres secteurs critiques
Énergie (électricité, gaz, pétrole, hydrogène)	Services postaux et d'expédition
Transports (aérien, ferroviaire, maritime, routier)	Gestion des déchets
Secteur bancaire et infrastructures de marché	Fabrication, production et distribution de produits chimiques
Santé	Production et distribution de denrées alimentaires
Eau potable et eaux usées	Fabrication (dispositifs médicaux, informatique/ électronique, machines, véhicules)
Infrastructures numériques (cloud, datacenters, DNS, CDN...)	Fournisseurs numériques (places de marché, moteurs de recherche, réseaux sociaux)
Gestion des services TIC (B2B, MSP/MSSP)	Recherche
Administrations publiques ; espace	—

6 secteurs

Secteurs classés en « zone de risque » par l'ENISA, où la criticité dépasse la maturité : gestion de services TIC, espace, administrations publiques, maritime, santé et gaz.

ENISA — NIS360 2024

La cartographie ENISA NIS360 est précieuse pour se situer : la banque, l'électricité et les télécoms figurent parmi les secteurs les plus matures, tandis que six secteurs concentrent un écart préoccupant entre leur criticité et leur niveau de préparation. Si vous relevez de l'un d'eux, l'effort de mise à niveau sera d'autant plus scruté.

09 9. Suis-je concerné ? Arbre de décision

1

Étape 1 — Secteur

Mon activité principale (ou une activité significative) figure-t-elle dans l'annexe I ou II ? Si non, passez à l'étape 4 (exposition indirecte).

2

Étape 2 — Taille

Mon entreprise dépasse-t-elle les seuils (≥ 50 salariés ou > 10 M€ de CA/bilan) ? Vérifiez au niveau du groupe et des filiales, pas seulement de l'entité juridique isolée.

3

Étape 3 — Catégorie

Secteur annexe I + grande taille → probablement entité essentielle. Secteur annexe II, ou annexe I en taille moyenne → probablement entité importante. Confirmez via MonEspaceNIS2.

4

Étape 4 — Exposition indirecte

Hors champ direct mais fournisseur d'une entité concernée ? Vous serez sollicité par vos clients au titre de la sécurité de leur chaîne d'approvisionnement : questionnaires, clauses, exigences contractuelles.

5

Étape 5 — Cas particuliers

Filiales, groupes multi-activités, sous-traitants critiques, entités concernées quelle que soit leur taille : traitez-les explicitement, ne les rangez pas par défaut « hors champ ».

Où trancher officiellement

Le service MonEspaceNIS2 de l'ANSSI est le point d'entrée prévu pour confirmer votre statut et, une fois les textes de transposition publiés, vous enregistrer. Ne restez pas dans l'incertitude : un statut mal évalué est en soi un risque de non-conformité.

10. Statut de la transposition française et calendrier

17 oct. 2024

Date limite de transposition de NIS2 en droit national. La directive est en vigueur depuis le 16 janvier 2023 et abroge NIS1 à compter du 18 octobre 2024.

Commission européenne — NIS2 Directive

En France, la transposition s'opère via le projet de loi « résilience des infrastructures critiques et renforcement de la cybersécurité », adopté en première lecture au Sénat le 12 mars 2025. À la date de rédaction (octobre 2026), il n'a pas été voté par l'Assemblée nationale et n'est pas promulgué. Les décrets d'application et les référentiels de l'ANSSI viendront préciser les modalités concrètes. Comme plusieurs États membres, la France a pris du retard sur la date de transposition (fixée au 17 octobre 2024), ce qui a donné lieu à des procédures d'infraction de la Commission européenne.

Ne pas attendre les décrets pour agir

Le retard réglementaire ne suspend pas le risque cyber ni la pression contractuelle de vos clients. Les organisations qui démarrent tôt lissent l'effort et le budget.

11. S'enregistrer : MonEspaceNIS2 et le ReCyF

L'enregistrement de l'entité auprès de l'autorité compétente est prévu par la directive comme une obligation en soi. En France, le service MonEspaceNIS2, opéré par l'ANSSI, est mis en place pour l'identification et l'enregistrement des entités ; l'ANSSI jouera le rôle d'autorité unique — hormis le secteur financier, qui relève du règlement DORA et des autorités sectorielles (ACPR, AMF).

L'obligation précise et ses modalités seront fixées par les textes de transposition, non encore promulgués.

1

1. S'auto-évaluer

Déterminer, via la plateforme, si l'on est entité essentielle, importante ou hors champ.

2

2. Renseigner l'entité

Fournir les informations d'identification, de contact et de rattachement sectoriel demandées.

3

3. S'enregistrer

Valider l'enregistrement dans les délais fixés par la réglementation nationale.

4

4. Tenir à jour

Maintenir les informations à jour (points de contact, périmètre) et suivre les évolutions du référentiel.

Le Référentiel Cyber France (ReCyF)

L'ANSSI publie le Référentiel Cyber France, qui traduit les objectifs de sécurité de NIS2 en exigences concrètes et vérifiables. C'est le document de travail à utiliser pour votre analyse d'écart : il fait le pont entre le texte juridique (art. 21) et des mesures opérationnelles.

12. Gouvernance et responsabilité des dirigeants (art. 20)

C'est le changement de paradigme le plus profond de NIS2 : la cybersécurité cesse d'être une affaire strictement technique déléguée à la DSI. L'organe de direction doit approuver les mesures de gestion des risques, en superviser la mise en œuvre, et se former lui-même. En cas de manquement, la responsabilité peut être engagée jusqu'à la suspension temporaire de fonctions dirigeantes.

☐ Approuver formellement la politique et les mesures de gestion des risques cyber.

☐ Superviser leur mise en œuvre (indicateurs, revue périodique).

☐ Suivre une formation cyber au niveau de la direction.

☐ Tracer les décisions cyber dans les comptes rendus de comité de direction / conseil.

☐ Allouer les ressources (budget, compétences) proportionnées au risque.

Modèle d'ordre du jour cyber en comité de direction

1) Exposition et incidents depuis la dernière revue ; 2) État d'avancement du plan de conformité NIS2 ; 3) Risques tiers/supply chain ; 4) Décisions d'arbitrage budgétaire ; 5) Formation et sensibilisation ; 6) Décisions tracées et responsable désigné. Un point cyber trimestriel documenté vaut preuve de gouvernance.

13. Les 10 mesures de gestion des risques (art. 21)

L'article 21 fixe un socle minimal de dix domaines de mesures, à appliquer selon le principe de proportionnalité. En voici la décomposition, avec pour chacun l'objectif et un quick win accessible à une PME/ETI.

Mesure (art. 21)	Objectif	Quick win PME/ETI
1. Analyse de risque & politique SSI	Formaliser risques et règles	Rédiger une politique SSI courte, validée par la direction
2. Gestion des incidents	Détecter, traiter, tracer	Registre d'incidents + procédure d'escalade écrite
3. Continuité & sauvegardes	Reprendre après sinistre	Sauvegardes 3-2-1 testées, PRA documenté
4. Sécurité de la supply chain	Maîtriser le risque tiers	Cartographie des fournisseurs critiques + clauses cyber
5. Sécurité du développement & vulnérabilités	Réduire la surface d'attaque	Processus de patch management + veille CVE
6. Évaluation de l'efficacité	Mesurer ce qui est en place	Audit/scan périodique + indicateurs de suivi
7. Hygiène & formation	Réduire l'erreur humaine	Sensibilisation annuelle + simulations de phishing
8. Cryptographie & chiffrement	Protéger les données	Chiffrement des postes et des sauvegardes
9. Contrôle d'accès & gestion des actifs	Limiter les accès	Inventaire des actifs + principe du moindre privilège
10. MFA & communications sécurisées	Sécuriser l'authentification	MFA généralisée sur tous les accès distants et sensibles

Le principe de Pareto de la conformité

Pour une PME/ETI, quatre mesures couvrent une part disproportionnée du risque réel : MFA généralisée, sauvegardes testées et hors-ligne, gestion des vulnérabilités, et sensibilisation. Commencez par elles avant d'investir dans des outils sophistiqués.

14 14. Sécurité de la chaîne d'approvisionnement

La supply chain est devenue l'angle mort majeur. Un attaquant n'a pas besoin de forcer votre porte s'il peut entrer par celle d'un prestataire disposant d'accès à votre système. NIS2 impose donc de traiter explicitement la sécurité des relations avec les fournisseurs et prestataires (art. 21).

30 %

Part des violations impliquant un tiers en 2025, un chiffre qui a doublé en un an — enjeu direct de sécurité de la chaîne d'approvisionnement.

Verizon — communiqué officiel 2025 DBIR

12 195

Violations de données confirmées analysées dans le DBIR 2025, sur plus de 22 000 incidents étudiés.

Verizon — 2025 Data Breach Investigations Report

- ☐ Cartographier les fournisseurs et prestataires ayant un accès à votre SI ou à vos données.
- ☐ Identifier les dépendances critiques (infogérance, cloud, éditeurs métiers).
- ☐ Intégrer des clauses cyber dans les contrats (obligations, audit, notification).
- ☐ Diffuser un questionnaire de sécurité proportionné aux fournisseurs critiques.
- ☐ Encadrer et journaliser les accès prestataires (comptes nominatifs, MFA, révocation).
- ☐ Réévaluer périodiquement l'exposition de vos tiers.

Une cartographie d'exposition externe (surface d'attaque, OSINT) aide à révéler les angles morts : actifs oubliés, services exposés d'un prestataire, fuites de données publiques liées à un tiers. Elle éclaire objectivement la conversation avec vos fournisseurs, sans se substituer à leur propre démarche de conformité.

15 15. Notification d'incident : 24h / 72h / 1 mois (art. 23)

24h / 72h / 1 mois

Chronologie de notification d'un incident significatif : alerte précoce sous 24h, notification sous 72h, rapport final sous un mois auprès du CSIRT/CERT-FR (art. 23).

Directive (UE) 2022/2555, art. 23 — EUR-Lex

- 1 Sous 24h — Alerte précoce**
Signaler l'incident dès sa détection : nature suspectée, caractère éventuellement malveillant, impact transfrontière possible.
- 2 Sous 72h — Notification**
Compléter avec une évaluation initiale : gravité, impact, indicateurs de compromission connus.
- 3 Sur demande — Rapport intermédiaire**
Fournir des mises à jour sur l'état du traitement si l'autorité le demande.
- 4 Sous 1 mois — Rapport final**
Décrire l'incident, sa cause racine, les mesures prises et l'impact réel.

Ne pas confondre avec le RGPD

Un même incident peut déclencher deux obligations parallèles : la notification NIS2 au CERT-FR et, si des données personnelles sont concernées, la notification de violation au titre du RGPD à la CNIL (également sous 72h). Préparez une procédure unique qui alimente les deux canaux, pour éviter les oublis sous pression.

Un incident « significatif » est, en pratique, celui qui cause une perturbation opérationnelle importante d'un service ou un dommage matériel/immatériel notable. Les règlements d'exécution européens précisent des seuils pour certains secteurs numériques. Préparez à l'avance une trame de fiche de notification et un arbre de qualification : dans le feu de l'action, l'improvisation coûte des heures précieuses.

16. Sanctions, contrôles et supervision (art. 31-37)

Les autorités disposent d'un arsenal gradué : demandes d'information, audits et inspections, injonctions de mise en conformité, avertissements, astreintes journalières, et amendes administratives. S'y ajoutent, fait marquant, des sanctions visant personnellement les dirigeants.

7 M€ ou 1,4 %

Amende maximale pour une entité importante : jusqu'à 7 M€ ou 1,4 % du CA annuel mondial (art. 34).

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

Régime	Entité essentielle	Entité importante
Type de supervision	Proactive (audits ex ante possibles)	Réactive (après signalement/incident)
Amende maximale	10 M€ ou 2 % du CA mondial	7 M€ ou 1,4 % du CA mondial
Sanctions dirigeants	Possibles (jusqu'à suspension de fonctions)	Possibles selon le droit national

Accompagnement d'abord, sanction ensuite

La doctrine française privilégie l'accompagnement et la mise en conformité progressive avant la répression. Ce qui déclenche réellement un contrôle : un incident notifié, un signalement, une plainte, ou une campagne sectorielle. La meilleure protection reste une trajectoire de conformité documentée et de bonne foi.

17. Articulation avec RGPD, DORA et les autres cadres

NIS2 ne vit pas en silo. Elle recoupe et complète d'autres cadres. La bonne pratique consiste à mutualiser la documentation : une seule politique SSI, un seul registre d'actifs, un seul processus d'incident alimentant plusieurs conformités.

Cadre	Périmètre	Autorité
RGPD	Protection des données personnelles	CNIL
NIS2	Cybersécurité des entités essentielles/importantes	ANSSI (CERT-FR pour les incidents)
DORA	Résilience opérationnelle du secteur financier	ACPR / AMF
LPM / SAIV	Infrastructures et opérateurs d'importance vitale	ANSSI / SGDSN
Cyber Resilience Act	Sécurité des produits numériques	Autorités de surveillance produits

Une politique, plusieurs conformités

Cartographiez une seule fois vos actifs, vos risques et vos incidents, puis mappez ce socle sur les exigences de chaque cadre. Vous éviterez la duplication d'efforts et les contradictions documentaires qui fragilisent une inspection.

18. Méthode pas-à-pas : l'analyse d'écart (gap analysis)

L'analyse d'écart est le cœur de toute démarche NIS2 : elle compare ce que vous faites déjà à ce que le texte (art. 21) et le ReCyF exigent, pour identifier les manques et les prioriser. C'est un exercice honnête, pas un exercice de communication.

1

1. Cadrage du périmètre

Définir les entités juridiques, sites, systèmes et données dans le champ NIS2.

2

2. Inventaire des actifs

Recenser matériels, logiciels, services cloud, accès distants et données sensibles.

3. Évaluation face aux exigences

Confronter chaque mesure de l'art. 21 et du ReCyF à l'existant (en place / partiel / absent).

4. Cotation des écarts

Noter chaque écart par le risque associé (probabilité × impact), pas seulement par sa facilité de correction.

5. Priorisation

Classer les actions par ratio risque réduit / effort, en isolant les quick wins à fort impact.

6. Formalisation

Consigner l'état des lieux, les écarts et les décisions dans un document validé par la direction.

Objectiver l'état des lieux par l'extérieur

Une cartographie d'exposition externe (surface d'attaque, OSINT, services exposés) alimente l'inventaire et la cotation des écarts avec des faits mesurés depuis l'extérieur — ce que voit un attaquant. Elle complète l'auto-déclaration interne sans la remplacer, et ne constitue pas un audit de certification.

19. Construire son plan de conformité (feuille de route 3 ans)

L'analyse d'écart produit une liste ; le plan de conformité en fait une trajectoire. Structurez-le en trois horizons pour lisser l'effort et le budget, avec un responsable et une échéance par action, et des indicateurs de suivi présentés en comité de direction.

Horizon	Priorité	Exemples d'actions
0-3 mois — Quick wins	Réduire le risque immédiat	MFA généralisée, sauvegardes testées, registre d'incidents, sensibilisation, enregistrement MonEspaceNIS2
3-12 mois — Socle	Structurer la conformité	Politique SSI, gestion des vulnérabilités, clauses fournisseurs, PRA, procédure de notification
12-36 mois — Maturité	Ancrer et mesurer	Gouvernance board formalisée, évaluation d'efficacité, audits réguliers, amélioration continue

Modèle de PACS

Formalisez un Plan d'Action de Conformité et de Sécurité (PACS) : pour chaque écart, une action, un responsable, une échéance, un budget et un indicateur de clôture. Pour une ETI de 300 salariés, une trajectoire réaliste combine des quick wins peu coûteux la première année et un investissement structurant étalé sur trois ans, plutôt qu'un « big bang » budgétaire intenable.

20. Spécificités et pragmatisme pour PME/ETI

NIS2 repose sur la proportionnalité : on n'attend pas d'une ETI de 200 personnes le dispositif d'un opérateur d'importance vitale. La conformité doit être adaptée à la taille, aux ressources et au risque. L'enjeu, pour une PME/ETI, est d'obtenir le maximum de réduction de risque avec des moyens contraints.

- Prioriser les 20 % de mesures qui couvrent 80 % du risque (MFA, sauvegardes testées, patch management, sensibilisation).
- Mutualiser : réutiliser une seule politique et un seul registre pour plusieurs conformités.
- Externaliser de façon raisonnée (SOC managé, infogérance) sans déléguer la gouvernance, qui reste au board.
- Automatiser la détection et la veille pour compenser des équipes réduites.
- Documenter la bonne foi et la trajectoire : c'est ce que regarde l'autorité en priorité.

Combattre l'idée reçue « c'est pour les grands groupes »

Avec environ 15 000 entités concernées en France et une pression contractuelle croissante des donneurs d'ordre sur leurs fournisseurs, les PME et ETI sont au cœur du dispositif — directement ou via la supply chain. Attendre d'être « désigné » n'existe plus : la charge d'auto-évaluation vous incombe.

21. Erreurs fréquentes et idées reçues

Erreur / idée reçue	Le bon réflexe
« On est trop petits, on n'est pas concernés »	Vérifier secteur + taille + exposition indirecte sur MonEspaceNIS2
Confondre conformité et sécurité réelle	Viser la réduction de risque, pas la case cochée
Négliger la supply chain	Cartographier les tiers et contractualiser la sécurité
Oublier de former le board	Formaliser un point cyber récurrent et tracé en comité
Sous-estimer les délais de notification	Préparer trame + arbre de qualification à l'avance
Attendre les décrets pour agir	Démarrer les quick wins dès maintenant
Acheter un outil avant de poser la gouvernance	Gouvernance et analyse d'écart d'abord, outils ensuite

Le piège de l'outil-miracle

Aucun logiciel ne « rend conforme » à lui seul. La conformité NIS2 est d'abord une affaire de gouvernance, de processus et de preuves. Les outils accélèrent et objectivent, mais ne remplacent ni la décision de direction, ni la documentation, ni la trajectoire.

22. Checklist, modèles et où s'adresser

- ☐ Statut déterminé (EE / EI / hors champ) et enregistrement effectué sur MonEspaceNIS2.
- ☐ Gouvernance : point cyber récurrent tracé, dirigeants formés (art. 20).
- ☐ Analyse de risque et politique SSI formalisées et validées.
- ☐ Sauvegardes testées, hors-ligne, avec PRA documenté.
- ☐ MFA généralisée sur les accès distants et sensibles.
- ☐ Gestion des vulnérabilités et patch management en place.
- ☐ Cartographie des fournisseurs critiques + clauses cyber contractuelles.
- ☐ Procédure de notification 24h/72h/1 mois prête (trame + arbre de qualification).
- ☐ Sensibilisation annuelle + simulations de phishing.
- ☐ Plan de conformité (PACS) à 3 horizons, avec responsables et indicateurs.

Besoin	Interlocuteur
S'auto-évaluer et s'enregistrer	MonEspaceNIS2 (ANSSI)
Cadre réglementaire et référentiels	ANSSI — cyber.gouv.fr
Notifier / traiter un incident	CERT-FR
Violation de données personnelles	CNIL
Panorama de menace européen	ENISA

Le rôle de Sedona, en toute honnêteté

Sedona se positionne en amont de la conformité : Sedona Radar analyse ce que votre domaine expose sur Internet et donne des indicateurs de maturité (il ne certifie rien, et il n'existe aucune certification NIS2) ; en complément, un audit OSINT des dirigeants, un audit de surface manuel, des formations de sensibilisation et des simulations de phishing. Sedona n'est ni qualifiée PASSI, ni certifiée ISO 27001, ni prestataire de réponse à incident : nous éclairons votre analyse d'écart et votre plan d'action, sans nous substituer à un conseil juridique. Si un client ou un texte exige un audit par un prestataire qualifié PASSI, adressez-vous à l'un des prestataires de la liste publiée par l'ANSSI.

§ Sources

1. EUR-Lex — Directive (UE) 2022/2555 (NIS2), texte consolidé — <https://eur-lex.europa.eu/eli/dir/2022/2555/oj>
2. Commission européenne — NIS2 Directive (Shaping Europe's digital future) — <https://digital-strategy.ec.europa.eu/en/policies/nis2-directive>
3. EUR-Lex — Règlement d'exécution (UE) 2024/2690 (mesures techniques secteurs numériques) — https://eur-lex.europa.eu/eli/reg_impl/2024/2690/oj
4. ANSSI — La directive NIS 2 (cyber.gouv.fr) — <https://cyber.gouv.fr/reglementation/cybersecurite-systemes-dinformation/directives-nis-nis2-et-dispositif-saiv/directive-nis-2/>
5. ANSSI — The NIS 2 Directive (version anglaise) — <https://cyber.gouv.fr/en/regulations/the-nis-2-directive/>
6. MonEspaceNIS2 — plateforme officielle de l'ANSSI — <https://monespacenis2.cyber.gouv.fr/>
7. ANSSI — Panorama de la cybermenace 2024 (actualité) — <https://cyber.gouv.fr/actualites/panorama-de-la-cybermenace-2024-mobilisation-et-vigilance-face-aux-attaquants/>
8. CERT-FR / ANSSI — Panorama de la cybermenace 2024 (rapport PDF, CERTFR-2025-CTI-003) — <https://www.cert.ssi.gouv.fr/uploads/CERTFR-2025-CTI-003.pdf>
9. ENISA — NIS360 2024 (maturité et criticité des secteurs) — <https://www.enisa.europa.eu/publications/enisa-nis360-2024>
10. ENISA — Threat Landscape 2024 — <https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024>
11. ENISA — Threat Landscape (page thématique) — <https://www.enisa.europa.eu/topics/cyber-threats/threat-landscape>
12. IBM — Cost of a Data Breach Report 2025 — <https://www.ibm.com/reports/data-breach>
13. IBM Think / X-Force — analyse du rapport 2025 — <https://www.ibm.com/think/x-force/2025-cost-of-a-data-breach-navigating-ai>
14. Verizon — 2025 Data Breach Investigations Report (DBIR) — <https://www.verizon.com/business/resources/reports/dbir/>
15. Verizon — communiqué officiel 2025 DBIR (surge tiers) — <https://www.verizon.com/about/news/2025-data-breach-investigations-report>
16. ANSSI — Les directives NIS / NIS 2 et le dispositif SAIV — <https://cyber.gouv.fr/reglementation/cybersecurite-systemes-dinformation/directives-nis-nis2-et-dispositif-saiv/>
17. beta.gouv.fr — startup d'État MonEspaceNIS2 — <https://beta.gouv.fr/startups/nis2.html>
18. Vie-publique.fr — projet de loi résilience des infrastructures critiques et cybersécurité (suivi parlementaire) — <https://www.vie-publique.fr/loi/295752-projet-de-loi-resilience-infrastructures-critiques-cybersecurite>

Préparez NIS2 en voyant d'abord ce que vous exposez

Sedona Radar analyse ce que votre domaine expose sur Internet et donne des indicateurs de maturité sur six référentiels, dont NIS2. Il éclaire votre analyse d'écart et votre plan d'action ; il ne certifie rien et ne remplace pas un audit réalisé par un prestataire qualifié. Commencez par voir ce qu'un attaquant voit déjà de vous.

Lancer mon scan gratuit

sedona-ai.com/scan-gratuit