

NIS2 Phase 2 en 2026 : Nouvelles Obligations et Mise

Points essentiels

- ▶ Phase 2 étend NIS2 à de nouveaux secteurs : administrations, spatial, prestataires numériques
- ▶ Chaque entité doit s'auto-identifier puis s'enregistrer auprès de l'ANSSI
- ▶ Dix-huit mesures de sécurité obligatoires s'imposent aux entités essentielles et importantes
- ▶ Les premières procédures de sanction ANSSI approchent : structurer son programme devient urgent

À RETENIR

À retenir

Phase 2 étend NIS2 à de nouveaux secteurs : administrations, spatial, prestataires numériques

Chaque entité doit s'auto-identifier puis s'enregistrer auprès de l'ANSSI

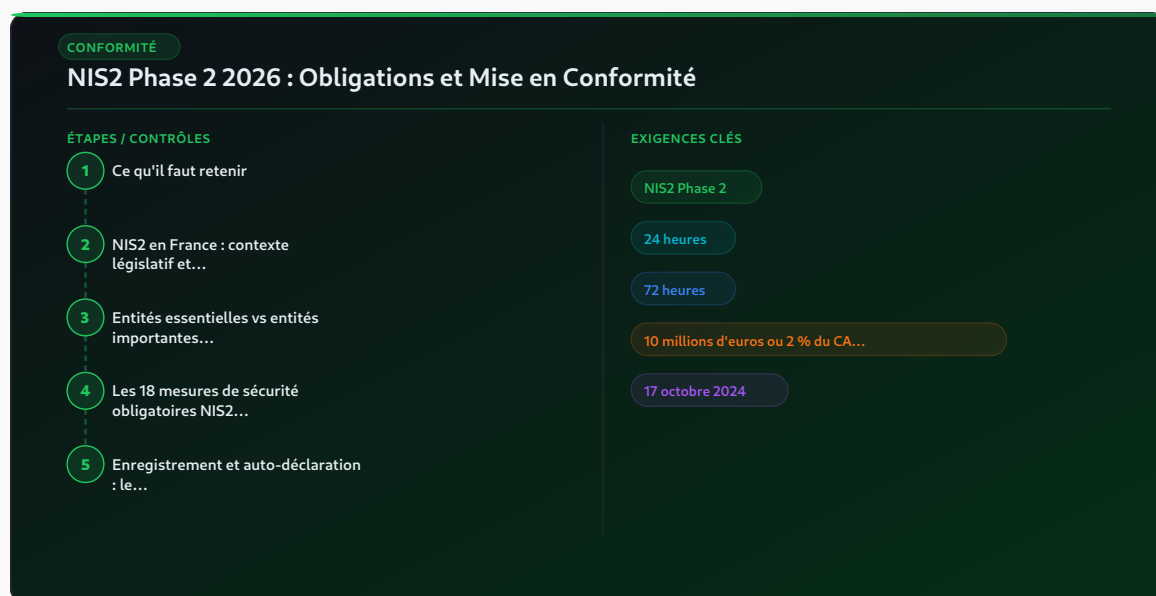
Dix-huit mesures de sécurité obligatoires s'imposent aux entités essentielles et importantes

Les premières procédures de sanction ANSSI approchent : structurer son programme devient urgent

La transposition française de la directive NIS2 franchit un cap décisif en 2026. Après la loi de transposition adoptée fin 2024 et les premiers décrets d'application parus début 2025, la deuxième vague réglementaire — désignée NIS2 Phase 2 par les praticiens — étend son périmètre à plusieurs milliers d'entités essentielles et importantes jusqu'ici épargnées. Collectivités territoriales, sous-traitants industriels, opérateurs de services numériques et acteurs

de la santé découvrent des exigences nettement renforcées : gouvernance du risque cyber validée par la direction, notification d'incident sous vingt-quatre heures, sécurisation contractuelle de la chaîne d'approvisionnement et audits périodiques opposables. Comprendre les nis2 phase 2 obligations conformité devient donc une priorité stratégique, car l'ANSSI dispose désormais de pouvoirs de contrôle et de sanction directement applicables. Ce guide détaille le calendrier, les responsabilités et les chantiers à engager sans délai.

À RETENIR



Ce qu'il faut retenir

NIS2 Phase 2 : les entités essentielles et importantes doivent s'enregistrer auprès de l'ANSSI et déployer les 18 mesures de sécurité obligatoires sans délai.

Le délai de notification d'un incident majeur est de **24 heures** pour l'alerte précoce puis **72 heures** pour le rapport initial auprès de l'ANSSI.

Les sanctions atteignent **10 millions d'euros ou 2 % du CA mondial** pour les entités essentielles en cas de manquement grave à leurs obligations.

L'outil **EBIOS RM** reste la méthode d'analyse de risques recommandée par l'ANSSI pour démontrer la conformité NIS2 lors des contrôles.

La supply chain numérique est désormais dans le périmètre : les fournisseurs ICT critiques doivent être évalués et contractuellement encadrés selon des critères définis.

Le secteur santé et les administrations publiques sont la priorité absolue de supervision ANSSI pour les contrôles 2026 en raison du niveau de risque élevé.

Calendrier NIS2 Phase 2 - France 2025-2027



NIS2 en France : contexte législatif et transposition nationale

La directive européenne NIS2 a été adoptée le 14 décembre 2021 avec une date limite de transposition au **17 octobre 2024**. La France a respecté ce calendrier avec la loi n°2024-1341 du 31 décembre 2024, complétée par des décrets d'application publiés en 2025. L'**ANSSI** est désignée autorité nationale compétente unique, contrairement à d'autres États membres qui ont réparti les compétences sectorielles. Cette centralisation offre une cohérence appréciable mais concentre les ressources de supervision sur un seul acteur face à plus de 15 000 entités à contrôler.



Retour terrain

J'accompagne actuellement plusieurs ETI dans leur préparation à NIS 2. Le point de blocage récurrent est l'article 21 sur la gestion des risques : les entreprises ont souvent une cartographie des actifs incomplète, ce qui rend impossible toute évaluation formelle des risques. J'ai développé une approche en deux temps — inventaire rapide par interview des

responsables métier, puis consolidation avec les outils de découverte réseau — qui permet d'obtenir une vue exploitable en 4 à 6 semaines.

NIS2 ne remplace pas intégralement le dispositif français des **Opérateurs d'Importance Vitale (OIV)** régis par la loi de programmation militaire. La superposition crée une complexité réglementaire que les équipes juridiques et RSSI doivent maîtriser pour éviter des programmes de conformité redondants ou lacunaires. Le texte français va sur plusieurs points au-delà des exigences minimales européennes, notamment sur la responsabilité personnelle des dirigeants et les délais de notification. Les associations professionnelles sectorielles telles que la FBF pour la finance ou la FHF pour les hôpitaux ont publié des guides d'application sectorielle qui complètent la documentation officielle ANSSI et permettent aux RSSI de s'appuyer sur des interprétations partagées au sein de leur secteur d'activité.

Entités essentielles vs entités importantes : critères et enjeux pratiques

NIS2 distingue deux catégories d'entités avec des régimes de supervision et de sanctions différenciés. Les **entités essentielles (EE)** opèrent dans des secteurs hautement critiques (Annexe I) et dépassent les seuils de grande entreprise : plus de 250 salariés ou CA supérieur à 50 millions d'euros et bilan supérieur à 43 millions d'euros. Ces secteurs comprennent énergie, transport, banque, marchés financiers, santé, eau potable, eaux usées, infrastructure numérique, gestion des services ICT, administration publique et espace.

Les **entités importantes (EI)** opèrent soit dans les secteurs Annexe I sous les seuils de grande entreprise (moyenne entreprise : 50-249 salariés, CA 10-49 M€), soit dans les secteurs Annexe II au-delà des seuils de moyenne entreprise : gestion des déchets, fabrication chimique, industrie alimentaire, fabrication industrielle de dispositifs médicaux et produits informatiques, services postaux, fournisseurs numériques et organismes de recherche. L'ANSSI estime que **15 000 à 20 000 entités françaises** seront concernées, contre 700 OSE sous NIS1 — une multiplication par 20 qui représente un défi colossal.

Retour terrain : lors d'une mission d'accompagnement NIS2 chez un groupe industriel de 700 salariés opérant dans l'énergie et la chimie, l'entité était simultanément EE pour ses activités de production énergétique et EI pour ses filiales de fabrication chimique. Deux programmes de conformité distincts mais coordonnés ont dû être construits avec un RSSI de groupe et des référents NIS2 dans chaque filiale — une organisation matricielle qui n'existait pas avant NIS2 et qui a nécessité une refonte de la gouvernance sécurité.

Les 18 mesures de sécurité obligatoires NIS2 décryptées

L'article 21 de la directive NIS2 définit les mesures de gestion des risques que toutes les entités concernées doivent mettre en œuvre proportionnellement à leur exposition au risque. La loi française les a déclinées en **18 mesures obligatoires** couvrant l'intégralité du cycle de vie de la sécurité des systèmes d'information.

Domaine	Mesures clés	EE/EI
Gouvernance	Politique sécurité, rôles définis, implication direction, formation dirigeants obligatoire	EE + EI
Gestion des risques	EBIOS RM, traitement des risques documenté, revue annuelle obligatoire	EE + EI
Gestion des incidents	Détection, notification ANSSI 24h/72h, rapport post-mortem documenté	EE + EI
Continuité d'activité	PCA, PRA, sauvegardes testées, exercices de crise annuels obligatoires	EE + EI
Sécurité supply chain	Évaluation fournisseurs ICT critiques, clauses contractuelles sécurité, audits tiers	EE + EI
Sécurité réseau et SI	Segmentation, chiffrement, contrôle d'accès, MFA généralisée	EE + EI
Gestion des vulnérabilités	Veille CVE, patch management structuré avec SLA définis, scans réguliers	EE + EI
Cryptographie	Politique chiffrement, gestion des clés, algorithmes RGS recommandés par ANSSI	EE + EI
Sécurité RH	Sensibilisation obligatoire, formation continue, vérification des antécédents	EE + EI
Contrôle d'accès	IAM, moindre privilège, revue trimestrielle des droits, MFA administrative	EE + EI

Enregistrement et auto-déclaration : le mécanisme NIS2 expliqué

L'innovation majeure de NIS2 par rapport à NIS1 est le mécanisme d'**auto-identification** : les entités ne sont plus désignées par les autorités mais doivent elles-mêmes déterminer si elles entrent dans le champ d'application et s'enregistrer sur le portail MonEspaceNIS2. Les entités y déclarent leur secteur d'activité avec code NAF, leur taille en effectifs et chiffres financiers, leur classification EE ou EI auto-évaluée, les coordonnées du responsable cybersécurité et les informations sur leurs systèmes d'information essentiels au sens NIS2.

L'ANSSI dispose d'un pouvoir de correction : si elle estime qu'une entité s'est mal classifiée ou a omis de s'enregistrer, elle peut imposer la classification et engager une procédure de mise en

demeure. Les **sanctions pour non-enregistrement** atteignent 1,4 % du CA mondial pour les EI et 2 % pour les EE — des montants applicables même en l'absence d'incident de sécurité. Le décret d'application précise que les **organes de direction** des entités essentielles doivent personnellement suivre une formation en cybersécurité et approuver formellement les mesures de gestion des risques — une responsabilisation sans précédent dans le droit français de la cybersécurité qui crée une obligation personnelle pour les membres du conseil d'administration et du comité exécutif.

Notification des incidents : le régime 24h/72h en détail

Le processus de notification NIS2 se déroule en trois étapes avec des délais stricts qui exigent une préparation organisationnelle avancée. **Alerte précoce (24 heures)** : dès la prise de connaissance d'un incident significatif, l'entité notifie l'ANSSI avec les premières informations disponibles, en précisant si l'incident est suspecté malveillant et s'il a un impact transfrontalier potentiel. **Notification initiale (72 heures)** : rapport avec évaluation préliminaire de la gravité et de l'impact, indicateurs de compromission disponibles et première analyse de la cause probable. **Rapport final (1 mois)** : analyse post-mortem complète avec mesures correctives déployées et leçons apprises documentées.

La notion d'**incident significatif** recouvre toute perturbation opérationnelle grave, perte financière significative, accès non autorisé à des données sensibles affectant un nombre important de personnes, ou impact sur la disponibilité du service au-delà de seuils sectoriels définis. Le **CERT-FR** joue un rôle d'intermédiaire opérationnel pour l'analyse technique des incidents notifiés. Notre avis tranché sur ce point : le délai de 24 heures est techniquement tenable mais organisationnellement très exigeant lors d'un incident ransomware, où les premières heures sont consacrées à la gestion de crise immédiate. Sans procédures de notification rodées et exercices de crise réguliers incluant le processus réglementaire, la plupart des équipes ne pourront pas respecter ce délai dans les conditions d'un incident réel.

Nouveaux secteurs couverts par NIS2 Phase 2 en France

La Phase 2 étend considérablement le périmètre sectoriel par rapport à NIS1. Le **secteur spatial** fait son entrée dans le dispositif : opérateurs d'infrastructures au sol pour les services spatiaux, fournisseurs de données de navigation GNSS et prestataires de services de télémétrie et télécommande de satellites. L'ANSSI travaille avec le CNES et les acteurs industriels pour définir les critères précis d'identification dans ce secteur à fort enjeu stratégique et géopolitique.

L'**administration publique** entre massivement dans le dispositif NIS2 : administrations centrales de l'État, collectivités régionales et locales au-delà de seuils de population définis par décret, et établissements de santé. Plusieurs milliers d'entités publiques françaises qui n'étaient pas soumises à des obligations formelles de cybersécurité rejoignent le périmètre. Les **fournisseurs de services numériques** à grande échelle (places de marché, moteurs de recherche, réseaux sociaux) au-delà de seuils d'utilisateurs européens sont intégrés en qualité d'entités importantes.

La **gestion des déchets** et les **services postaux et de messagerie** surprennent de nombreux acteurs qui ne se percevaient pas comme des infrastructures critiques. Exemple concret issu de nos missions : un grand groupe français de collecte et traitement de déchets industriels a découvert lors d'un audit de périmètre que ses systèmes SCADA de pilotage des centres de tri automatisés étaient pleinement dans le périmètre NIS2 — une prise de conscience tardive qui a conduit à lancer un programme d'urgence de sécurisation des systèmes OT sans attendre les contrôles ANSSI.

EBIOS RM : la méthode de référence pour la conformité NIS2

EBIOS Risk Manager est la méthode d'analyse de risques cyber publiée par l'ANSSI en 2018. Recommandée mais non obligatoire légalement, elle constitue de facto la référence attendue lors des contrôles ANSSI. EBIOS RM structure l'analyse en cinq ateliers successifs : cadrage et socle de sécurité (atelier 1), identification des sources de risques (atelier 2), construction des scénarios stratégiques ou chemins d'attaque (atelier 3), développement des scénarios opérationnels avec techniques d'attaque détaillées (atelier 4), définition du traitement du risque et des mesures

résultantes (atelier 5). Cette structuration couvre l'ensemble des exigences de l'article 21 NIS2 et permet de documenter une démarche proportionnée au niveau de risque de l'entité.

Des guides sectoriels publiés en 2023-2024 adaptent EBIOS RM aux spécificités OT/ICS, santé et cloud. Pour les organisations déjà certifiées [accompagnement ISO 27001](#), l'intégration dans le SMSI existant est possible : la [certification](#) couvre environ 70-75 % des exigences NIS2, les 25-30 % restants portant spécifiquement sur la notification réglementaire d'incidents, la responsabilité personnelle des dirigeants et l'évaluation supply chain selon les critères NIS2. Notre [guide ISO 27001 complet](#) détaille la mise en correspondance des contrôles ISO 27001 avec les 18 mesures NIS2 — un livrable attendu lors des contrôles ANSSI qui facilite la démonstration de conformité pour les organisations déjà certifiées.

Sécurité de la chaîne d'approvisionnement numérique : l'obligation la plus difficile

La gestion de la **chaîne d'approvisionnement numérique** est l'obligation NIS2 la plus difficile à opérationnaliser et la plus fréquemment sous-estimée par les entités qui débutent leur programme de conformité. Chaque entité EE ou EI doit : évaluer la maturité cybersécurité de ses fournisseurs ICT critiques proportionnellement à leur criticité pour les services essentiels, intégrer des clauses contractuelles de sécurité dans tous les nouveaux contrats et lors du renouvellement des contrats existants, cartographier les dépendances critiques et identifier les points de défaillance uniques, et maintenir un processus d'audit ou d'évaluation régulière documenté.

La Commission Européenne développe des schémas de certification européens comme l'EUCS pour le cloud, qui permettront aux fournisseurs de démontrer leur conformité via une certification reconnue. En attendant, les certifications ISO 27001 et SOC 2 Type II constituent les preuves d'évaluation les plus acceptées lors des contrôles ANSSI. Notre avis tranché et assumé : envoyer des questionnaires de sécurité sans analyse de risques préalable et sans suivi des réponses n'a aucune valeur probante. Cette erreur est pourtant la plus fréquemment observée lors de nos missions d'audit NIS2 — des dossiers volumineux de questionnaires non analysés qui donnent une illusion de conformité sans réduire le risque réel lié aux tiers.

Régime de sanctions NIS2 : montants, procédures et premiers impacts

Pour les **entités essentielles**, les amendes administratives atteignent **10 millions d'euros ou 2 % du chiffre d'affaires annuel mondial**, le montant le plus élevé étant retenu. Pour les **entités importantes**, le plafond est de **7 millions d'euros ou 1,4 % du CA mondial**. Des sanctions supplémentaires peuvent viser les dirigeants personnellement en cas de négligence grave caractérisée, une disposition sans précédent dans l'arsenal réglementaire cyber français antérieur à NIS2.

La procédure suit un schéma progressif : mise en demeure avec délai de remédiation raisonnable, puis injonction de mesures obligatoires, enfin transmission à une commission administrative indépendante pour la sanction financière. Dans les cas graves impliquant des risques immédiats, l'ANSSI peut demander la suspension temporaire de certifications ou l'interdiction d'exercer pour les dirigeants responsables. Contrairement au RGPD où la CNIL cumule régulation et sanction, NIS2 sépare ces fonctions pour garantir l'indépendance du processus de sanction. Les premières décisions financières formelles sont attendues pour 2027, mais les procédures de mise en demeure pourraient démarrer dès fin 2026 pour les cas les plus flagrants de non-enregistrement ou de non-notification d'incidents majeurs.

Plan de conformité NIS2 en 6 phases pour les RSSI français

Phase 1 — Qualification (1-2 mois) : déterminer l'applicabilité, classer EE ou EI selon les critères sectoriels et de taille, cartographier toutes les entités du groupe potentiellement concernées y compris les filiales et prestataires intégrés, et s'enregistrer sur le portail ANSSI.

Phase 2 — Analyse de l'écart (2-3 mois) : audit de conformité NIS2 complet avec mapping formel des 18 mesures, identification des gaps par criticité et estimation des investissements humains, financiers et technologiques nécessaires.

Phase 3 — Gouvernance (1-2 mois) : mise à jour de la politique de sécurité pour intégrer explicitement NIS2, définition formelle des rôles (RSSI désigné, référent NIS2, correspondant

ANSSI), organisation de la formation obligatoire des dirigeants et mise en place des comités de pilotage. **Phase 4 — Technique (6-18 mois)** : déploiement des mesures prioritaires dans l'ordre de criticité — MFA généralisée, chiffrement, segmentation réseau, EDR/XDR/SIEM, patch management avec SLA définis. **Phase 5 — Incidents (2-3 mois)** : procédures de notification ANSSI rodées avec simulation de crise obligatoire, playbooks par scénario, contacts CERT-FR et accord avec prestataire PRIS qualifié. **Phase 6 — Supply chain (ongoing)** : programme d'évaluation fournisseurs, mise à jour des contrats ICT, processus de surveillance continue intégrés dans les achats et le juridique.

Articulation NIS2 avec ISO 27001, DORA et les référentiels sectoriels

L'**ISO 27001** couvre environ 70-75 % des exigences NIS2 : politique de sécurité, gestion des risques, contrôle d'accès, cryptographie, opérations de sécurité, gestion des incidents. Notre [guide ISO 27001](#) détaille la mise en correspondance. Les entités soumises à **DORA** bénéficient d'une exemption partielle — DORA est lex specialis pour les entités financières dans son champ d'application. Notre analyse du [bilan DORA 2026](#) détaille les articulations pratiques.

Pour les entités hébergeant des données de santé, l'articulation avec la **certification HDS** est formalisée dans un référentiel conjoint ANS-ANSSI publié en 2025. Pour les entités soumises à SOC 2, le [guide SOC 2](#) permet de comprendre les complémentarités avec NIS2. La stratégie optimale consiste à construire un programme de conformité intégré couvrant simultanément NIS2 et les référentiels sectoriels applicables, en identifiant les contrôles communs pour éviter les redondances et optimiser les investissements de mise en conformité tout en produisant un socle documentaire cohérent pour les différents auditeurs sectoriels.

Secteur santé et NIS2 : programme CaRE et priorité de supervision

Le secteur santé est **priorité absolue** pour les contrôles NIS2 de 2026. Le CERT-FR a recensé plus de 50 incidents significatifs dans les établissements hospitaliers français entre 2023 et 2025, dont plusieurs ayant conduit à des interruptions cliniques prolongées nécessitant la redirection d'urgences vers des établissements voisins. Tous les CHU, centres hospitaliers régionaux et ESPIC (Établissements de Santé Privés d'Intérêt Collectif) au-delà des seuils définis sont qualifiés d'entités essentielles avec supervision proactive ANSSI.

L'ANS (**Agence du Numérique en Santé**) a publié un référentiel sectoriel HDS-NIS2 articulant les exigences de certification Hébergement Données de Santé avec les obligations NIS2, identifiant les contrôles communs et les exigences complémentaires spécifiques à chaque cadre. Le programme **CaRE** (Cybersécurité accélération et Résilience des Établissements), doté de 750 millions d'euros sur 5 ans, finance directement les investissements cyber des établissements de santé dans le cadre de NIS2. Cette opportunité de cofinancement public est à saisir sans délai pour les DSI hospitaliers qui doivent accélérer leur mise en conformité dans un contexte budgétaire structurellement contraint.

NIS2 et sécurité industrielle OT/ICS : approche et contraintes spécifiques

Pour les secteurs énergie, transport et eau, NIS2 s'applique explicitement aux **systèmes de contrôle industriels (OT/ICS/SCADA)**. Ces environnements présentent des défis particuliers qui nécessitent une expertise spécialisée distincte de la sécurité IT classique : disponibilité extrême requise en permanence, cycles de vie de 10 à 30 ans, protocoles sans mécanismes de sécurité natifs (Modbus, DNP3, Profibus), impossibilité de déployer des agents EDR sur de nombreux automates et systèmes embarqués anciens, et sensibilité aux tests de vulnérabilité qui peuvent provoquer des arrêts de production aux conséquences opérationnelles et économiques immédiates.

L'ANSSI recommande ses guides dédiés à la cybersécurité des systèmes industriels et la norme **IEC 62443** comme cadre de référence technique pour les environnements OT, avec une structure en zones de sécurité et niveaux de protection qui permet de démontrer la conformité NIS2 de manière adaptée. Notre article sur la [sécurité OT/ICS et passerelles industrielles](#) détaille les architectures de référence. Des adaptations aux exigences incompatibles avec la disponibilité OT sont possibles et acceptées par l'ANSSI à condition d'être justifiées par des mesures compensatoires documentées dans l'analyse de risques EBIOS RM avec une évaluation du risque résiduel accepté par les dirigeants.

Erreurs classiques dans la mise en conformité NIS2 : retour d'expérience terrain

Sous-estimer le périmètre organisationnel : les filiales, prestataires intégrés, systèmes OT/IoT et entités étrangères du groupe opérant en France sont souvent oubliés lors du périmétrage initial, obligeant à recommencer l'analyse depuis le début. **Traiter NIS2 comme un projet ponctuel** : NIS2 exige une gestion continue avec revues annuelles obligatoires — ce n'est pas un projet à horizon fixe mais un programme permanent intégré dans le fonctionnement de l'organisation avec des KPIs mesurables dans le temps.

Négliger la gouvernance direction : l'implication personnelle des dirigeants est une exigence légale engageant leur responsabilité personnelle, pas une formalité politique. **Ignorer les délais de notification** : sans procédures rodées et exercices réguliers incluant le processus de notification réglementaire, les 24 heures sont impossibles à respecter lors d'un incident réel.

Confondre ISO 27001 et NIS2 comme équivalents : la certification ISO 27001 est un atout majeur mais ne couvre pas les 25-30 % d'exigences spécifiques NIS2. **Négliger la supply chain** : des questionnaires sans analyse de risques et sans suivi des réponses n'ont aucune valeur probante lors d'un contrôle ANSSI — c'est l'erreur la plus commune et la plus risquée observée sur le terrain.

Calendrier et prochaines étapes NIS2 en France pour 2026-2027

Premier semestre 2026 : fin de la période de grâce pour l'enregistrement sur le portail ANSSI et démarrage des contrôles formels sur les EE des secteurs prioritaires. **Second semestre 2026** : premières mises en demeure pour non-enregistrement ou non-notification d'incidents graves — l'ANSSI traitera prioritairement les cas de non-notification d'incidents majeurs pour envoyer un signal clair au marché. **2027** : montée en régime avec extension aux entités importantes, publication des premiers rapports de conformité sectoriels agrégés, premières sanctions financières prononcées par la commission administrative indépendante.

Les entités qui n'ont pas encore initié leur programme NIS2 sont objectivement en retard : une grande organisation nécessite 18 à 36 mois pour atteindre la conformité complète documentée. Commencer en 2026 signifie être prêt au mieux en fin 2027, après les premiers cycles de contrôle ANSSI. L'urgence est réelle et les ressources compétentes en cybersécurité et en conformité NIS2 deviennent de plus en plus rares sur le marché français au fur et à mesure que la demande explose. Anticiper le recrutement ou l'appel à des prestataires qualifiés est une priorité stratégique pour les RSSI et les directions générales des entités concernées.

Ressources officielles et accompagnement pour NIS2

L'ANSSI centralise la documentation NIS2 sur cyber.gouv.fr/la-directive-nis-2 : textes législatifs, guides pratiques sectoriels, FAQ et portail MonEspaceNIS2. L'ENISA publie des lignes directrices européennes complémentaires sur enisa.europa.eu utiles pour comprendre les exigences dans un contexte transfrontalier. Pour l'accompagnement qualifié, la liste ANSSI des prestataires PASSI, PACS, PDIS et PRIS garantit le niveau de compétence requis pour les missions d'audit et de conseil NIS2.

Le réseau des CERT sectoriels offre des échanges d'informations sur les menaces actives valorisés par l'article 23 de NIS2. Le dispositif **MonAideCyber** de l'ANSSI propose un diagnostic gratuit de cybersécurité utilisable comme point de départ pour les PME et ETI. La participation active aux dispositifs de partage d'information sectoriels constitue un signal positif

lors des contrôles ANSSI, démontrant l'engagement de l'entité dans l'amélioration collective de la résilience cyber sectorielle au-delà de la simple conformité réglementaire minimale.

FAQ — NIS2 Phase 2 2026

Mon entreprise a moins de 50 salariés, est-elle concernée par NIS2 ?

En principe non : microentreprises et petites entreprises sont exclues du champ général de NIS2. Des exceptions importantes existent cependant : si l'entreprise est le seul fournisseur national d'un service essentiel, si elle est désignée explicitement par les autorités pour des raisons de sécurité nationale, ou si elle fait partie de la supply chain d'une entité essentielle qui lui impose contractuellement des obligations équivalentes. Les sous-traitants ICT de grandes entités NIS2 doivent examiner attentivement leurs contrats car leurs clients peuvent leur transférer une partie de leurs obligations de sécurité via des clauses contractuelles dédiées NIS2, créant de facto des obligations de conformité pour des entités théoriquement hors périmètre réglementaire direct.

Quelle différence concrète entre EE et EI pour les obligations NIS2 en France ?

Les 18 mesures de sécurité sont identiques pour les deux catégories. La différence porte sur le régime de supervision : les entités essentielles font l'objet d'audits proactifs initiés par l'ANSSI même en l'absence d'incident, tandis que les entités importantes sont soumises à une supervision réactive déclenchée par des incidents ou des signalements. Les plafonds de sanctions diffèrent (10 M€/2% CA pour EE, 7 M€/1,4% pour EI). La formation obligatoire des dirigeants est formellement plus exigeante pour les EE, avec approbation documentée et traçable des politiques de sécurité par les organes de direction lors des assemblées générales ou des comités de direction exécutifs.

Comment prouver sa conformité NIS2 lors d'un contrôle ANSSI ?

La conformité se démontre par un dossier documentaire structuré et cohérent : rapport EBIOS RM récent avec date de révision de moins de 12 mois, politique de sécurité signée par la direction, registre des incidents avec preuves de notification ANSSI dans les délais, inventaire des fournisseurs ICT avec preuves d'évaluation concrètes, plans de traitement des risques avec KPIs de progression mesurables, et résultats d'audits techniques récents. La certification ISO 27001 en cours de validité est un atout probant mais ne remplace pas ces éléments spécifiques à NIS2 que l'ANSSI attend explicitement lors de ses contrôles sur place.

Quels secteurs sont ciblés en priorité par les contrôles ANSSI en 2026 ?

L'ANSSI a officiellement annoncé ses priorités pour 2026 : énergie, santé et administrations publiques centrales en première vague. Le secteur financier bénéficie d'une approche coordonnée entre ANSSI, ACPR et AMF. Les PME des secteurs élargis comme les déchets, l'agroalimentaire et la chimie ne seront pas soumises à des contrôles systématiques avant 2027-2028 sauf incidents majeurs. Les entités qui s'auto-enregistrent rapidement et maintiennent une communication proactive avec l'ANSSI bénéficient d'un traitement plus favorable que celles qui attendent passivement les contrôles pour agir.

NIS2 s'applique-t-il aux systèmes OT industriels en France ?

Oui, explicitement pour les entités des secteurs énergie, transport et eau. Les systèmes OT/ICS/SCADA sont dans le périmètre NIS2 pour ces secteurs critiques. La norme IEC 62443 et les guides ANSSI dédiés aux systèmes industriels constituent les références techniques. Des adaptations aux exigences incompatibles avec les contraintes opérationnelles de disponibilité sont possibles et reconnues par l'ANSSI, à condition d'être justifiées dans l'analyse de risques avec des mesures compensatoires documentées et proportionnées au risque résiduel accepté par les organes de direction responsables de l'approbation formelle de la politique de sécurité.

Micro-segmentation réseau et Zero Trust dans le contexte NIS2

L'une des mesures techniques les plus structurantes de NIS2 est l'exigence de **segmentation réseau** qui, combinée aux principes du **Zero Trust**, constitue désormais la référence architecturale recommandée par l'ANSSI pour les entités essentielles. La micro-segmentation va au-delà de la simple séparation réseau classique : elle impose que chaque zone applicative soit isolée et que chaque flux inter-zones soit explicitement autorisé, authentifié et journalisé. Cette approche réduit drastiquement la surface d'attaque en cas de compromission initiale, limitant la propagation latérale des attaquants dans le système d'information.

La mise en œuvre du Zero Trust dans un contexte NIS2 implique plusieurs prérequis techniques : un inventaire exhaustif et maintenu à jour de tous les actifs informatiques (serveurs, postes de travail, équipements réseau, applications, services cloud), un système d'authentification forte (MFA) généralisé à l'ensemble des accès y compris les accès internes, une journalisation centralisée des accès et des activités dans un SIEM (Security Information and Event Management), et des mécanismes de détection des anomalies comportementales (UEBA) pour identifier les activités suspectes même provenant de comptes légitimes compromis.

Pour les entités qui ne disposent pas encore d'une architecture Zero Trust, l'approche pragmatique recommandée consiste à prioriser la segmentation des systèmes les plus critiques (Active Directory, systèmes de paiement, systèmes de production) et à déployer progressivement les contrôles d'accès basés sur l'identité plutôt que sur la localisation réseau. Cette approche incrémentale est acceptée par l'ANSSI dans le cadre du plan de traitement des risques NIS2, à condition de démontrer une trajectoire d'amélioration continue avec des jalons définis et mesurables.

Un cas pratique issu de nos missions : un opérateur d'infrastructure critique du secteur énergétique a mis en place une segmentation en zones de confiance (Internet, DMZ, intranet, systèmes OT) avec des pare-feux de nouvelle génération permettant l'inspection applicative des flux. Cette architecture a permis de contenir une tentative d'intrusion via un fournisseur de maintenance externe dans la zone DMZ, empêchant la propagation vers les systèmes SCADA de production. La traçabilité complète des flux inter-zones a également facilité la reconstruction de la chronologie de l'incident et la notification ANSSI dans les délais réglementaires.

Continuité d'activité et cyber-résilience : le PCA cyber obligatoire NIS2

NIS2 rend obligatoire la mise en place d'un **Plan de Continuité d'Activité (PCA)** **spécifiquement adapté aux incidents cyber**, ce qui va au-delà des PCA classiques orientés risques physiques et environnementaux. Le PCA cyber NIS2 doit couvrir les scénarios de ransomware, de déni de service (DDoS), de compromission d'Active Directory et de destruction de données. Ces scénarios ont des caractéristiques très différentes des incidents physiques : ils peuvent affecter simultanément l'ensemble du système d'information, rendre inutilisables les outils de communication habituels (messagerie, téléphonie sur IP) et nécessiter des processus de décision et de restauration spécifiques.

Le **Plan de Reprise d'Activité (PRA) cyber** doit définir des objectifs de reprise réalistes et testés : le RTO (Recovery Time Objective) ou délai de reprise admissible, et le RPO (Recovery Point Objective) ou point de récupération des données. Ces objectifs doivent être cohérents avec les niveaux de criticité définis dans l'analyse de risques EBIOS RM et avec les engagements de service de l'entité vis-à-vis de ses clients et partenaires.

L'exigence de **tests réguliers** du PCA/PRA est une nouveauté importante de NIS2 par rapport aux pratiques antérieures : des exercices de simulation doivent être réalisés au moins annuellement, avec documentation des résultats et des actions correctives. Ces exercices doivent inclure le processus de notification ANSSI pour valider que les délais 24h/72h sont effectivement respectables dans des conditions réalistes d'incident. Les entités dont les sauvegardes n'ont pas été testées depuis plus de 12 mois s'exposent à une non-conformité NIS2 documentable lors d'un contrôle ANSSI, indépendamment du niveau technique de leurs protections préventives.

Un aspect souvent négligé du PCA cyber est la gestion des **communications de crise** : qui prend la parole publiquement, quel est le message en direction des clients et partenaires, comment gérer les demandes médias lors d'un incident majeur ? NIS2 n'impose pas explicitement de plan de communication de crise, mais les entités qui ne l'ont pas anticipé se retrouvent dans des situations très délicates lors d'incidents médiatisés — une atteinte à la réputation pouvant avoir des conséquences économiques parfois plus lourdes que l'incident lui-même.

Gestion des identités et contrôle d'accès : IAM et MFA au cœur de NIS2

La **gestion des identités et des accès (IAM)** est l'une des mesures NIS2 qui mobilise le plus d'investissements dans les organisations qui débutent leur programme de conformité. L'exigence d'**authentification multifacteur (MFA)** généralisée — et non plus seulement sur les accès d'administration — constitue un changement de paradigme important pour des organisations habituées à protéger uniquement leurs systèmes les plus critiques par MFA.

NIS2 impose la MFA pour l'ensemble des accès aux systèmes d'information essentiels : accès administrateurs bien sûr, mais aussi accès des utilisateurs métiers aux applications critiques, accès distants via VPN, accès aux environnements cloud, et accès des prestataires et fournisseurs tiers. Cette généralisation crée des défis d'UX (expérience utilisateur) et d'architecture qui doivent être anticipés pour éviter un déploiement qui pousserait les utilisateurs à contourner les contrôles.

Le principe du **moindre privilège** est une autre exigence centrale : chaque utilisateur, service ou système ne doit disposer que des droits strictement nécessaires à l'exécution de ses fonctions. La mise en œuvre rigoureuse de ce principe impose une revue régulière des droits d'accès — au minimum trimestrielle pour les comptes à privilèges selon les recommandations ANSSI — et un processus de révocation immédiate lors des départs ou des changements de fonction. Les comptes de service dormants ou orphelins constituent l'une des vulnérabilités les plus exploitées par les attaquants pour maintenir une persistance discrète dans les systèmes d'information.

La gestion des **comptes à privilèges (PAM — Privileged Access Management)** mérite une attention particulière dans le cadre NIS2 : l'ANSSI recommande le déploiement d'un coffre-fort de mots de passe pour les comptes administrateurs, la journalisation complète des sessions privilégiées, le cloisonnement des comptes administrateurs des comptes utilisateurs pour les mêmes personnes, et l'utilisation de solutions de jump server ou de bastion pour les accès d'administration. Ces contrôles PAM constituent souvent la priorité numéro un des programmes de mise en conformité NIS2 compte tenu de leur impact direct sur la capacité à détecter et contenir les attaques avancées ciblant les comptes privilégiés.

Pour les organisations utilisant des services cloud (AWS, Azure, GCP), les exigences IAM de NIS2 s'appliquent également aux identités cloud : les rôles IAM doivent respecter le moindre

privilège, les accès aux consoles de gestion cloud doivent être protégés par MFA, et les Service Account avec des droits étendus doivent être inventoriés et revus régulièrement. La configuration de l'authentification fédérée (SAML, OIDC) entre l'annuaire on-premise et les services cloud doit être auditée pour s'assurer qu'une compromission de l'un ne compromet pas automatiquement l'autre — un risque fréquemment sous-estimé dans les architectures hybrides qui constituent pourtant la majorité des environnements des entités NIS2 françaises.

L'ANSSI recommande également de déployer des solutions de **détection des comportements anormaux (UEBA)** couplées au SIEM pour identifier les accès suspects même réalisés avec des identifiants légitimes. Ces solutions sont particulièrement efficaces pour détecter les attaques de type credential stuffing, les mouvements latéraux post-compromission et les exfiltrations de données progressives qui passent sous le radar des contrôles d'accès classiques basés sur l'identité seule.

Veille et gestion des vulnérabilités dans le cadre NIS2

NIS2 impose un **processus structuré de gestion des vulnérabilités** qui va bien au-delà des pratiques informelles encore répandues dans de nombreuses organisations françaises. La réglementation exige que les entités disposent d'un inventaire exhaustif et maintenu à jour de leurs actifs logiciels (SBOM — Software Bill of Materials pour les applications développées en interne ou acquises), d'un processus de veille sur les vulnérabilités avec des sources de référence (CERT-FR, NVD, ANSSI), et d'un processus de traitement des vulnérabilités avec des délais de correction définis en fonction de la criticité.

Les délais de correction des vulnérabilités critiques sont un point de contrôle important lors des audits NIS2 : l'ANSSI attend généralement la correction des vulnérabilités CVSS ≥ 9 dans les 72 heures sur les systèmes exposés à Internet, et dans les 7 à 30 jours pour les systèmes internes selon leur criticité et leur exposition. Ces objectifs, souvent impossibles à tenir sans une organisation dédiée et des processus de déploiement automatisés (patch management centralisé, pipelines CI/CD sécurisés pour les applications développées en interne), constituent l'un des principaux défis opérationnels des programmes NIS2 pour les organisations de taille intermédiaire.

La **veille sur les menaces actives** (Threat Intelligence) devient également une exigence implicite de NIS2 : les entités doivent être en mesure de détecter et de répondre aux menaces récentes ciblant leur secteur d'activité. Les flux de Threat Intelligence sectoriels proposés par les CERT sectoriels (CERT Santé, CERT Finance, CERT Énergie) constituent un socle indispensable que les entités NIS2 doivent intégrer dans leur processus de gestion des risques et dans la configuration de leurs outils de détection. L'absence de veille sectorielle structurée lors d'un contrôle ANSSI est un signal très négatif qui révèle une posture réactive plutôt que proactive face aux menaces cyber.

La mise en place d'un processus de **divulgestion coordonnée des vulnérabilités (CVD)** est également encouragée par NIS2 pour les entités qui développent des logiciels ou des systèmes utilisés par d'autres entités essentielles ou importantes. Ce processus permet de recevoir et de traiter les signalements de vulnérabilités provenant de chercheurs en sécurité externes de manière organisée, évitant les divulgations publiques non contrôlées qui pourraient mettre en danger les utilisateurs avant que les correctifs soient disponibles. L'ANSSI accompagne les entités dans la mise en place de leur politique CVD et leur déploiement d'un programme de Bug Bounty si nécessaire.

Les entités qui n'ont pas encore formalisé leur processus de gestion des vulnérabilités peuvent s'appuyer sur les référentiels existants tels que la norme ISO 30111 (Vulnerability handling processes) et le standard CVD de l'ENISA pour structurer leur démarche. L'intégration du processus de gestion des vulnérabilités dans le SMSI ISO 27001 (contrôle A.12.6.1 de l'ISO 27001:2013 et contrôle 8.8 de l'ISO 27001:2022) permet de démontrer la cohérence de l'approche lors des audits de certification et des contrôles ANSSI NIS2 simultanément, réduisant la charge de démonstration de conformité pour les équipes déjà mobilisées par les obligations réglementaires multiples.

Pour les organisations des secteurs industriels soumises à NIS2, la gestion des vulnérabilités OT/ICS présente des spécificités particulières : les fournisseurs d'automates et de systèmes SCADA publient leurs bulletins de sécurité sur des canaux distincts des vulnérabilités IT classiques (Siemens ProductCERT, Schneider Electric PSIRT, Rockwell Automation Security Advisory), et les fenêtres de maintenance pour appliquer les correctifs sont beaucoup plus contraintes en raison des exigences de disponibilité continue des processus industriels. L'ANSSI recommande de maintenir une liste des vulnérabilités connues affectant les équipements OT en production et de

définir des plans de remédiation réalistes prenant en compte les contraintes opérationnelles spécifiques à chaque système industriel.

L'adoption d'outils de **scan de vulnérabilités continu** est désormais incontournable pour répondre aux exigences NIS2 : des solutions comme Qualys, Tenable Nessus ou OpenVAS permettent de scanner régulièrement l'ensemble du périmètre exposé (systèmes internes, services cloud, applications web) et de prioriser les vulnérabilités selon leur criticité CVSS et leur exploitabilité réelle dans le contexte de l'entité. La fréquence minimale recommandée par l'ANSSI pour les entités essentielles est un scan complet mensuel et un scan ciblé des systèmes critiques hebdomadaire, avec une remontée immédiate des vulnérabilités critiques nouvellement publiées affectant les systèmes en production. Ces résultats de scan doivent être intégrés dans le processus de reporting au RSSI et, pour les vulnérabilités les plus critiques, présentés à la direction dans le cadre du tableau de bord sécurité NIS2 qui doit être maintenu et présenté régulièrement aux organes de gouvernance conformément aux obligations de responsabilisation de la direction.

Conclusion

La conformité réglementaire n'est pas une destination mais un état à maintenir. Chaque évolution du SI, chaque nouveau fournisseur peut modifier le périmètre. Documentation, audits réguliers et formation des équipes en sont les piliers.

Votre organisation est-elle soumise à NIS 2, ISO 27001 ou DORA ?

[Évaluer votre conformité NIS 2](#) ou [contactez-nous directement](#).