Move2Cloud

• WHITE PAPER — ÉDITION 2027

CYBERSÉCURITÉ & CONFORMITÉ

NIS2
Se Mettre en Conformité Avant l'Échéance

Le guide pratique pour les PME et ETI françaises : qui est concerné, ce que la directive exige réellement, et comment structurer une mise en conformité sans mobiliser une équipe dédiée.

11 pages · Grille d'auto-évaluation, calendrier de transposition et feuille de route incluses

15 000
entités françaises concernées, contre environ 500 sous NIS1

10 M€
amende maximale pour une entité essentielle en cas de manquement

2%
du chiffre d'affaires mondial, alternative possible à l'amende fixe

PRÉPARÉ PAR
Move2Cloud — Conseil Cloud & Infrastructure, Paris

PUBLICATION
Septembre 2026

SOMMAIRE

Ce que vous allez trouver dans ce document

Un parcours en six temps, de la question « suis-je concerné ? » à une feuille de route de mise en conformité opérationnelle.

À qui s'adresse ce document ? Dirigeants, DSI et RSSI de PME et ETI qui découvrent, ou soupçonnent, être concernés par NIS2 et cherchent une méthode claire pour objectiver leur situation.

SYNTHÈSE

L'essentiel en une page

NIS2 n'est plus réservée aux grands groupes et aux opérateurs d'importance vitale — elle redéfinit le périmètre de la cybersécurité réglementée en France, et embarque des milliers de PME et ETI qui ne s'y attendaient pas.

La directive européenne NIS2 (2022/2555) élargit considérablement le champ de la précédente directive NIS de 2016. En France, sa transposition prend la forme de la loi relative à la résilience des infrastructures critiques et au renforcement de la cybersécurité, dite « loi résilience », dont l'examen se poursuit alors que le pays a dépassé l'échéance européenne initiale du 17 octobre 2024. Le résultat concret : **environ 15 000 entités françaises seront concernées**, contre environ 500 sous l'ancien régime NIS1 — soit un périmètre multiplié par trente.

Cette extension touche 18 secteurs d'activité, répartis en deux niveaux de criticité, et deux catégories d'entités aux obligations différenciées. Les sanctions, elles, sont dimensionnées pour être dissuasives : **jusqu'à 10 millions d'euros ou 2 % du chiffre d'affaires mondial** pour une entité essentielle en défaut, avec une responsabilité qui peut remonter jusqu'aux dirigeants eux-mêmes.

15 000
entités françaises concernées, contre environ 500 sous NIS1 — un périmètre x30

18
secteurs d'activité couverts, répartis en deux niveaux de criticité

10 M€
amende maximale pour une entité essentielle, ou 2 % du CA mondial

Pour une PME ou une ETI qui n'a jamais eu à se conformer à une réglementation cyber sectorielle, la première question n'est pas « comment me mettre en conformité ? » mais « suis-je réellement concerné, et sous quelle catégorie ? ». Ce document propose une méthode pour y répondre, avant de détailler les obligations concrètes qui en découlent.

SECTION 02

Pourquoi NIS2 change la donne pour les PME et ETI

La directive NIS de 2016 ne couvrait qu'un nombre restreint d'opérateurs jugés critiques — essentiellement de grands groupes dans l'énergie, les transports ou la santé. L'expérience a montré que cette approche laissait de côté une part croissante des chaînes de valeur numériques dont dépendent ces mêmes secteurs critiques.

1. Le périmètre s'étend à toute la chaîne de dépendance

NIS2 ne se limite plus aux grands opérateurs : elle couvre désormais leurs fournisseurs, sous-traitants et prestataires numériques dès lors qu'ils dépassent certains seuils de taille. Une PME de service informatique ou une ETI industrielle peut ainsi se retrouver concernée simplement parce qu'elle fournit un service à une entité elle-même soumise à la directive.

2. Les seuils de taille remplacent la logique de désignation individuelle

Contrairement à NIS1, où chaque État membre désignait individuellement les opérateurs concernés, NIS2 s'appuie sur des seuils objectifs d'effectif et de chiffre d'affaires, appliqués secteur par secteur. Cette automatisation du périmètre explique en grande partie le passage de 500 à 15 000 entités en France.

3. La responsabilité de la gouvernance devient explicite

NIS2 introduit une exigence nouvelle par rapport à NIS1 : l'implication directe des organes de direction dans la gestion des risques cyber, avec une responsabilité qui peut être engagée personnellement en cas de manquement grave et répété.

« NIS2 ne demande pas d'être invulnérable — elle demande de pouvoir démontrer que le risque cyber est géré comme un risque d'entreprise, au même titre que le risque financier ou juridique. »

Pour toute organisation qui fournit des services à un client soumis à NIS2 — même sans être elle-même directement visée par les seuils — la question de la conformité devient également une question commerciale : un client soumis à la directive doit s'assurer que ses prestataires critiques le sont également.

SECTION 03

Suis-je concerné ? Secteurs, seuils, catégories

Trois critères combinés déterminent l'assujettissement à NIS2 : le secteur d'activité, la taille de l'entité, et le niveau de criticité qui en découle.

18 secteurs, deux niveaux de criticité

La directive distingue les secteurs « hautement critiques » (annexe I) des secteurs « critiques » (annexe II), avec des obligations similaires mais un régime de supervision différent.

SECTEURS HAUTEMENT CRITIQUES	SECTEURS CRITIQUES
Énergie, transport, banque, infrastructures des marchés financiers, santé, eau potable, eaux usées, infrastructure numérique, gestion des services TIC, administration publique, espace	Services postaux, gestion des déchets, substances chimiques, production alimentaire, fabrication (plusieurs sous-secteurs industriels), fournisseurs numériques, recherche

Deux catégories d'entités

CATÉGORIE	SEUIL TYPE	OBLIGATIONS
Entité essentielle (EE)	≥250 salariés, ou CA >50 M€ et bilan >43 M€, sur les secteurs de l'annexe I	Obligations complètes, supervision proactive par l'autorité nationale, sanctions les plus élevées
Entité importante (EI)	≥50 salariés, ou CA >10 M€, sur les annexes I et II ; toute grande entreprise de l'annexe II	Obligations similaires, mais supervision réactive (contrôle a posteriori) et sanctions plafonnées à un niveau inférieur

> **À retenir :** une PME de moins de 50 salariés peut malgré tout être concernée si elle est le seul fournisseur critique identifié d'une entité essentielle, ou si un État membre l'a désignée individuellement — les seuils sont la règle générale, pas une garantie absolue d'exclusion.

SECTION 04

Ce que NIS2 exige concrètement

Au-delà des grands principes, NIS2 liste des mesures précises de gestion des risques que chaque entité concernée doit être en mesure de démontrer.

DOMAINE	CE QUI EST ATTENDU
Analyse de risque	Politique documentée d'analyse des risques et de sécurité des systèmes d'information, révisée régulièrement.
Gestion des incidents	Procédure de détection, traitement et notification des incidents significatifs, avec une alerte précoce à l'autorité compétente sous 24 heures et un rapport détaillé sous 72 heures.
Continuité d'activité	Plan de continuité et de reprise après sinistre, incluant la gestion de crise et la gestion de sauvegardes testées.
Sécurité de la chaîne d'approvisionnement	Évaluation de la sécurité des fournisseurs et prestataires directs, intégrée aux relations contractuelles.
Cyberhygiène et formation	Politiques de contrôle d'accès, chiffrement, authentification multifacteur, et sensibilisation régulière des équipes.
Gouvernance	Implication directe et formation des organes de direction à la gestion des risques cyber, avec approbation formelle des mesures.

Point de vigilance : le délai de notification de 24 heures pour une alerte précoce est particulièrement contraignant pour une organisation qui ne dispose pas encore de procédure de détection formalisée — c'est souvent le premier chantier à engager, avant même l'analyse de risque complète.

SECTION 05

Sanctions et responsabilité des dirigeants

NIS2 aligne le niveau des sanctions cyber sur celui du RGPD — un signal clair de la priorité accordée à la directive au niveau européen.

MANQUEMENT	ENTITÉ ESSENTIELLE	ENTITÉ IMPORTANTE
Défaut de gestion des risques ou de notification	Jusqu'à 10 M€ ou 2 % du CA mondial	Jusqu'à 7 M€ ou 1,4 % du CA mondial
Mesures complémentaires possibles	Suspension de certifications, responsabilité des dirigeants	Injonctions administratives, astreintes

Une responsabilité qui remonte jusqu'à la direction

Point notable par rapport au régime précédent : les organes de direction peuvent voir leur responsabilité personnelle engagée en cas de manquement grave et répété aux obligations de gestion des risques — une évolution qui déplace la cybersécurité d'un sujet purement technique vers un sujet de gouvernance d'entreprise.

> **À retenir :** les autorités nationales privilégient, dans un premier temps, une approche d'accompagnement plutôt que de sanction immédiate pour les entités de bonne foi engagées dans une démarche de mise en conformité — mais cette tolérance n'est ni permanente ni garantie pour les organisations qui n'engagent aucune démarche visible.

SECTION 06

Où en est la France : calendrier de transposition

La France a dépassé l'échéance européenne initiale de transposition, mais le processus législatif se poursuit activement.

La transposition de NIS2 en droit français prend la forme d'un projet de loi relatif à la résilience des infrastructures critiques et au renforcement de la cybersécurité — un texte qui transpose simultanément NIS2, la directive REC (résilience des entités critiques) et s'articule avec le règlement DORA pour le secteur financier. La France ayant dépassé l'échéance du 17 octobre 2024 fixée par la directive européenne, le pays fait l'objet d'une procédure d'infraction ouverte par la Commission européenne — une situation partagée avec plusieurs autres États membres.

> **Ce que cela signifie concrètement :** l'absence de loi définitivement promulguée ne dispense pas de se préparer. Les obligations de fond de la directive européenne sont connues et stables ; seules les modalités précises de mise en œuvre nationale (calendrier d'enregistrement, autorité de contrôle, sanctions graduées) restent à finaliser. Les organisations qui attendent la promulgation pour commencer partent avec un retard qu'elles devront ensuite rattraper dans l'urgence.

Ce qui est d'ores et déjà engagé

L'enregistrement des entités concernées s'effectue via une plateforme dédiée, et un accompagnement transitoire est prévu avant l'entrée en vigueur pleine des sanctions — généralement de l'ordre de plusieurs années après la publication des textes d'application, le temps que les entités se mettent en conformité. Ce délai n'est pas un motif pour repousser la démarche : les mesures de fond (gestion des risques, notification, continuité) demandent elles-mêmes plusieurs mois à mettre en place correctement.

SECTION 07

Grille d'auto-évaluation de conformité

Avant d'engager un chantier de mise en conformité, vérifiez ces sept points pour objectiver votre situation actuelle.

- [ ] **Avez-vous vérifié si votre secteur figure dans l'une des deux annexes de la directive ?** Le périmètre sectoriel est la première condition d'assujettissement, avant même la taille de l'entité.
- [ ] **Votre effectif ou votre chiffre d'affaires dépasse-t-il les seuils applicables à votre secteur ?** Les seuils diffèrent entre entité essentielle et entité importante, et entre annexe I et annexe II.
- [ ] **Êtes-vous fournisseur direct d'une entité elle-même soumise à NIS2 ?** Une désignation en tant que fournisseur critique peut vous rendre concerné même sous les seuils généraux.
- [ ] **Disposez-vous d'une procédure formalisée de détection et de notification d'incidents ?** Le délai de 24 heures pour l'alerte précoce est l'une des obligations les plus techniquement exigeantes.
- [ ] **Votre plan de continuité d'activité a-t-il été testé au cours des douze derniers mois ?** Un plan non testé ne constitue pas une preuve de conformité opposable en cas de contrôle.
- [ ] **La sécurité de vos fournisseurs et prestataires critiques est-elle évaluée et documentée ?** La sécurité de la chaîne d'approvisionnement fait partie intégrante des obligations NIS2.
- [ ] **Vos dirigeants ont-ils été formés à leurs responsabilités en matière de gestion des risques cyber ?** L'implication de la gouvernance est une exigence explicite, pas une simple recommandation.

> **Comment lire vos réponses :** trois « non » ou plus, en particulier sur les questions de secteur et de seuils, justifient un diagnostic d'assujettissement formel avant toute autre décision — c'est le point de départ incontournable de toute démarche NIS2.

SECTION 08

Feuille de route en 5 étapes

Une démarche progressive, pensée pour transformer une obligation réglementaire en amélioration structurelle de la sécurité de l'organisation.

1

Diagnostiquer l'assujettissement

Déterminer précisément si l'organisation est concernée, sous quelle catégorie (essentielle ou importante), et à partir de quels critères — secteur, seuils, ou statut de fournisseur critique.

2

Cartographier l'existant

Recenser les mesures de sécurité déjà en place face aux exigences de la directive, pour identifier précisément les écarts plutôt que de repartir de zéro.

3

Prioriser par risque et par délai

Traiter en premier les obligations les plus structurantes et les plus longues à mettre en place — notification d'incidents, continuité d'activité, sécurité de la chaîne d'approvisionnement.

4

Impliquer la gouvernance

Former les organes de direction, formaliser leur implication dans l'approbation des mesures, et documenter cette gouvernance pour qu'elle soit opposable en cas de contrôle.

5

Tester et documenter en continu

Mettre en place des exercices réguliers (simulation d'incident, test de continuité) et conserver une trace documentée de la démarche, condition de toute conformité démontrable.

CONCLUSION

NIS2, une contrainte qui peut devenir un avantage

Les organisations qui abordent NIS2 comme un projet de sécurité structurel — plutôt que comme une case à cocher réglementaire — en ressortent avec une gouvernance des risques plus mature, un avantage commercial réel face à des clients eux-mêmes soumis à la directive, et une résilience opérationnelle qui dépasse largement le périmètre de la conformité.

Attendre la promulgation définitive du texte français pour commencer revient à sous-estimer le temps réel que demandent des mesures comme la notification d'incidents ou la continuité d'activité — des chantiers qui se préparent en mois, pas en semaines.

Move2Cloud	est un cabinet de conseil spécialisé en infrastructure, cloud et transformation IT. Nous accompagnons les organisations dans le diagnostic, la mise en conformité et la sécurisation de leur environnement cloud face aux exigences réglementaires.
Contact	Move2Cloud — Paris · move2cloud.fr
Prochaine étape	Un diagnostic d'assujettissement NIS2 permet de répondre en quelques semaines aux sept questions de la page 9, avec un plan de mise en conformité priorisé.

Sources

Directive (UE) 2022/2555 du Parlement européen et du Conseil (NIS2) — Legiscope, « Transposition NIS2 en France : loi, calendrier 2026 et obligations ANSSI » — AdevWeb, « NIS2 : votre PME est-elle concernée ? 18 secteurs, calendrier 2026, sanctions » — documentation ANSSI sur la directive NIS2.