CYBERSÉCURITÉ

Directive NIS2 : comprendre, anticiper et se préparer

La transposition française s'appuie sur le Référentiel de Cybersécurité Français (ReCyF) et impose une approche pilotée, proportionnée et démontrable.

NIS2 ne se limite pas à une mise en conformité : c'est un cadre pour structurer la gouvernance, la maîtrise des risques, la réaction aux incidents et la continuité d'activité.

EE

Entités Essentielles

Périmètre à criticité élevée

Les entités essentielles sont soumises aux exigences les plus strictes de la directive : gouvernance renforcée, supervision plus exigeante, obligations structurées de notification et niveau d'attente élevé sur la démonstration de conformité.

Ce que cela implique

· Exigences maximales de sécurité et de pilotage
· Supervision proactive et audits potentiels
· Notification d'incidents structurée
· Implication explicite de la direction

Niveau d'exigence élevé

EI

Entités Importantes

Exigences proportionnées au risque

Les entités importantes relèvent d'un cadre exigeant mais proportionné à leur exposition au risque. Les attendus de gouvernance, de protection et de réaction restent pleinement applicables, avec une logique de supervision davantage a posteriori.

Ce que cela implique

· Exigences graduées selon le risque
· Supervision réactive
· Notification d'incidents obligatoire
· Gestion documentée des incidents et des preuves

Approche proportionnée

À faire en premier : vérifiez votre statut sur le simulateur ANSSI pour confirmer si votre organisation relève du périmètre EE ou EI.

Le cadre structurant de la conformité NIS2

Le ReCyF traduit les exigences NIS2 en objectifs opérationnels : gouverner, protéger, détecter et résister.
Cette lecture aide à piloter la conformité comme un programme de transformation.

1 Gouvernance

· Implication des dirigeants et validation des orientations sécurité
· Maîtrise de l'écosystème, des services et des systèmes d'information
· PSSI, cartographies, rôles et responsabilités formalisés
· Pilotage des risques et logique de preuve

Piloter et engager la direction

2 Protection

· Sécurisation des accès, des identités et des droits
· Architecture, segmentation, administration et accès distants
· Protection contre les malwares et gestion des vulnérabilités
· Réduction de l'exposition et du risque d'impact

Réduire l'exposition

3 Défense

· Détection, qualification et réaction aux incidents
· Organisation de la notification réglementaire
· Supervision de sécurité renforcée pour les entités essentielles
· Capacité à traiter vite et à démontrer la réponse

Détecter et réagir

4 Résilience

· Sauvegardes, restauration et tests réguliers
· Continuité, reprise d'activité et dépendances critiques
· Gestion de crise cyber et exercices
· Capacité à poursuivre l'activité malgré un incident majeur

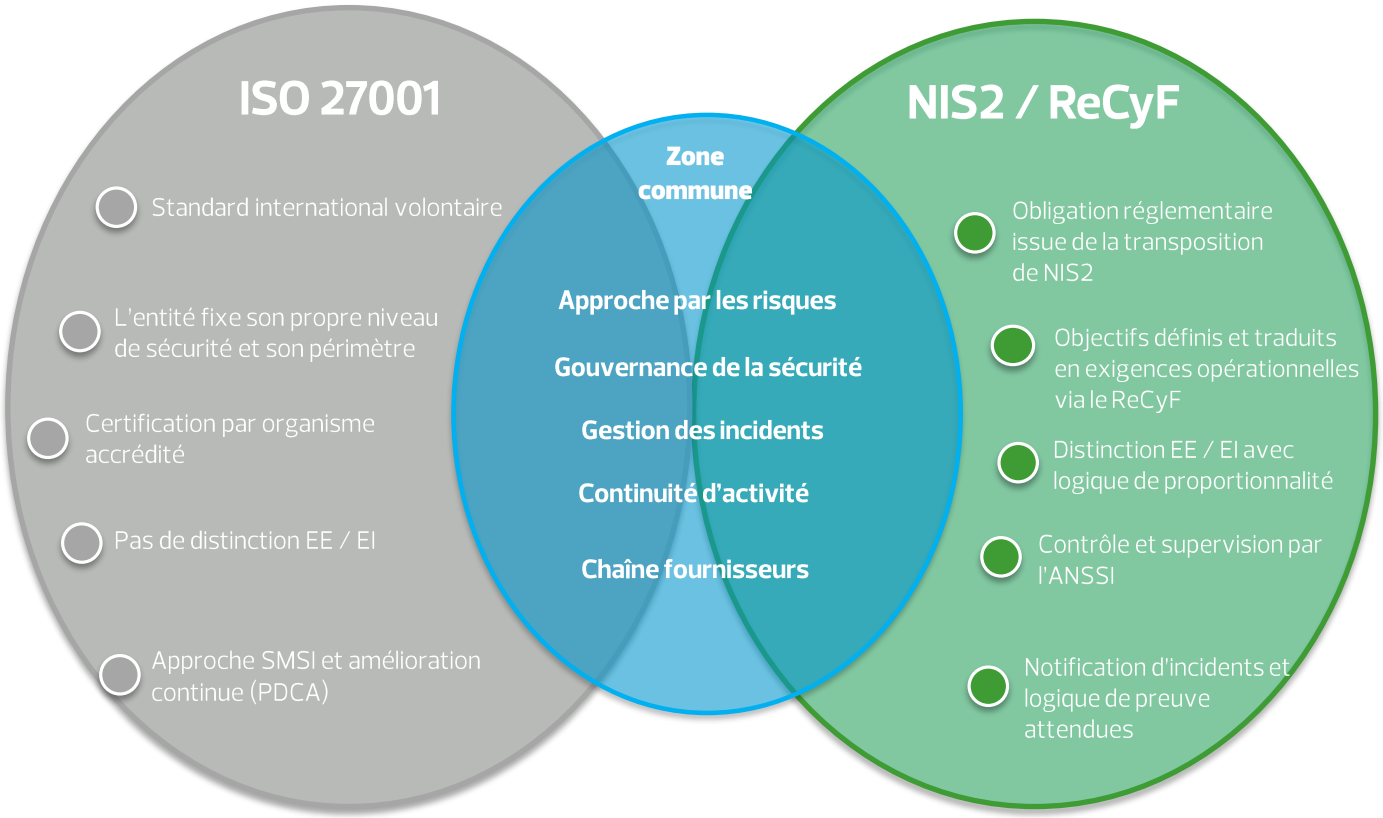
Continuer à opérer

Message de fond : la conformité NIS2 n'est pas un projet purement technique. Elle suppose une organisation capable de piloter la sécurité, de réduire ses risques, de réagir aux incidents et de continuer à fonctionner.

LEVIER DE CONFORMITÉ

ISO 27001 et ReCyF NIS2 : socle commun et différences structurantes

ISO 27001 constitue un excellent point d'appui pour se préparer à NIS2. Le ReCyF va toutefois plus loin sur le caractère prescriptif, le périmètre couvert et la logique de démonstration réglementaire.



Lecture simple : ISO 27001 apporte une base robuste ; le ReCyF NIS2 ajoute un cadre réglementaire plus prescriptif, plus large en périmètre et plus démontrable.

ISO 27001 facilite la structuration, l'auditabilité et la gouvernance du SMSI.

Le ReCyF attend des mesures plus explicitement cadrées, testées et démontrées sur l'ensemble du SI.

RSM vous accompagne

Une feuille de route claire, priorisée et adaptée à votre maturité

Une trajectoire de transformation simple à expliquer à la direction, pilotable dans le temps et suffisamment concrète pour engager les chantiers de mise en conformité.

Objectif : transformer un cadre réglementaire dense en une trajectoire de conformité compréhensible, priorisée et soutenable pour la direction comme pour les équipes opérationnelles.

1 Déterminer l'assujettissement

Confirmer le statut EE / EI, le périmètre réglementaire et les principales obligations applicables à l'organisation.

2 Désigner un pilote NIS 2

Cette responsabilité clarifie les rôles et facilite la coordination

3 Cartographier le SI et l'écosystème

Identifier les actifs, services critiques, dépendances métiers, prestataires et points de contact indispensables.

4 Évaluer les écarts ReCyF

Mesurer la maturité sur les quatre piliers, objectiver les écarts et qualifier le niveau de risque associé.

5 Prioriser les chantiers

Construire une trajectoire réaliste : gouvernance, accès, supervision, sauvegardes, continuité et gestion de crise.

6 Tester, formaliser et piloter

Documenter, tester régulièrement, démontrer la mise en œuvre et installer un pilotage durable avec indicateurs.

Diagnostic d'assujettissement, gap assessment ReCyF et feuille de route de mise en conformité.

RSM vous aide à passer d'un cadre réglementaire complexe à un plan d'action concret, pilotable et adapté à votre maturité.