

NIS2 et ReCyF

Apprendre à poser les bonnes questions

Pour un dirigeant, un responsable informatique ou un référent sécurité. Résultat attendu : séparer le périmètre à qualifier, les demandes clients et les contrôles réellement démontrés.

La réponse courte

Vérifier activité, taille, liens avec d'autres entreprises et exceptions. Utiliser l'orientation ANSSI. Un questionnaire client ou une mesure de sécurité ne suffit pas à établir votre statut réglementaire.

Trois cas fictifs, trois prochaines vérifications

Situation	Ce qu'il faut vérifier ensuite
18 salariés ; questionnaire d'un grand client	Décrire l'activité et la clause demandée ; analyser séparément le périmètre de l'entité. Le questionnaire seul ne conclut rien.
12 salariés ; service DNS fourni à des clients	Qualifier exactement le service et examiner les exceptions. Le petit effectif n'exclut pas toutes les situations.
Filiale de 30 salariés	Obtenir les liens capitalistiques et les données pertinentes du groupe avant de conclure sur la taille.

Exercice - repérer les raccourcis

« Nous avons moins de 50 salariés et notre prestataire a installé un pare-feu. Nous sommes donc hors périmètre. »

Quelles données manquent ? Le pare-feu change-t-il le statut ?

Corrigé

Il manque notamment activité, critères financiers, entreprises liées et exceptions. Le pare-feu décrit une mesure technique. La conclusion est « situation à qualifier », puis une liste de pièces à réunir, pas un verdict juridique.

Au 27 septembre 2026, la page ANSSI présente le ReCyF comme un document de travail, par défaut non obligatoire. Il structure la préparation ; il ne constitue pas une certification. Vérifier les sources officielles avant une décision réglementaire.

Une sauvegarde existe. Qu'a-t-on vraiment démontré ?

Une preuve utile décrit un périmètre, une date, un test, un résultat et des limites. Exemple entièrement fictif :

Champ	Fiche de contrôle remplie
Service et objectif	Gestion des devis. Objectif interne : reprise en moins de 4 h ; perte de données au plus 24 h.
Test	Le 25 septembre, restauration isolée de la copie du 24 septembre à 22 h.
Résultat	1 h 20 pour restaurer, puis 20 min pour ouvrir et modifier un devis de test. Total : 1 h 40.
Limites	Mail non testé ; panne générale du site non simulée. L'heure de l'incident simulé reste à documenter.
Suite et preuve	Exploitant : tester le relais mail avant le 2 octobre. Garder rapport, référence de sauvegarde et accord métier.

Ce que cette fiche permet de dire

Le périmètre testé a été restauré en 1 h 40. La reprise complète en moins de 4 h n'est pas encore démontrée. Pour vérifier la perte de données, comparer le point restaurable à l'heure de l'incident simulé et contrôler la cohérence.

Exercice - une exception au MFA

L'objectif concerne dix comptes administrateurs. Neuf disposent du MFA ; un compte utilise une application ancienne. Le tableau indique « MFA activé : oui ». Est-ce un état fidèle ?

Corrigé

Écrire « 9/10 couverts ; un compte en exception ». Documenter risque, restrictions compensatoires, responsable et date de réexamen. Évaluer la mesure compensatoire ; ne pas la considérer automatiquement équivalente au MFA.

Partager la preuve adaptée

Pour un client, préciser service, contrôle, date, résultat et limite. Proposer les justificatifs par un canal convenu. Ne pas transmettre secrets, cartographie détaillée ou données personnelles sans vérifier le besoin et les personnes habilitées.

03 / À REMPLIR ET À CONSERVER

Deux fiches pour commencer

1. Périmètre à qualifier

Information	Votre situation / pièce à obtenir
Entité et activité	Nom / pays / service précis : _____
Taille et liens	Effectifs / CA HT / bilan / exercice : _____ Entreprises liées ou partenaires : _____
Analyse datée	Secteur / exception / source officielle : _____ Orientation / hypothèse / point incertain : _____
Confirmation	Responsable / prochaine vérification / date : _____

2. Contrôle à démontrer

Information	Votre résultat
Service et objectif	Périmètre / responsable / objectif interne : _____
Test et preuve	Date / méthode / résultat / justificatif : _____
Limites et suite	Exception / action / responsable / échéance : _____

Exemple d'organisation interne sur un mois

S1 : qualifier le périmètre. S2 : décrire un service critique et ses accès. S3 : tester restauration et accès sensibles. S4 : exercer la réponse à incident et arbitrer les corrections. Adapter aux urgences : **ce n'est ni un délai légal ni une promesse de conformité.**

Sources officielles, consultées le 27 septembre 2026

ANSSI : NIS2 et statut du ReCyF

FAQ ANSSI : critères de taille et exceptions

EUR-Lex : directive (UE) 2022/2555

Ces fiches organisent les informations et les preuves. Elles ne remplacent pas la qualification juridique ni l'ensemble des exigences applicables.