Checklist NIS2 de demande de preuves fournisseurs

Un registre opérationnel pour demander, suivre et escalader les preuves de sécurité auprès de vos fournisseurs directs et prestataires de services au titre de NIS2 (directive (UE) 2022/2555), article 21(2)(d) et article 21(3) : registre des fournisseurs, grille de criticité (T1/T2/T3), dix catégories de preuves avec fréquences, et processus d'escalade documenté.

Ce PDF est le compagnon d'impression et de revue. Le fichier de travail est le XLSX (listes déroulantes, registre des fournisseurs, checklist des preuves, grille de criticité) ; une variante Markdown lisible par machine est fournie pour les agents IA. Les trois sont gratuits sur orbiqhq.com/templates/nis2-supplier-evidence-request-checklist — sans e-mail requis.

Base juridique : directive (UE) 2022/2555, art. 21(2)(d) et 21(3) ; règlement d'exécution (UE) 2024/2690 ; ENISA Technical Implementation Guidance (juin 2025) et Good Practices for Supply Chain Cybersecurity (juin 2023). Ce modèle constitue une information générale, pas un avis juridique.

Registre des fournisseurs

Référence des champs (le XLSX les porte en colonnes ; exemples issus de la ligne 1) :

Colonne	Conseils	Exemple
Nom du fournisseur		Northcloud ApS
Service fourni	Décrivez le service que vous consommez, pas le catalogue du fournisseur	Hébergement IaaS de la plateforme de production (EU-West)
Réf. contrat		MSA-2024-011
Responsable commercial		J. Meyer
Évaluateur sécurité		A. Kraus
Contact sécurité du fournisseur		security@northcloud.example
Niveau d'accès	Le niveau le plus élevé applicable	production
Catégories de données		Données personnelles clients, identifiants
Pays / localisation des données		Danemark / UE
Sous-traitants divulgués		oui
Niveau de criticité	Évaluez d'abord avec la feuille Grille de criticité	T1
Dernière évaluation complète		2026-03-14
Prochaine revue prévue	Dérivée de la fréquence du niveau : T1 annuel, T2 annuel, T3 tous les 3 ans / au renouvellement	2027-03-14
Statut		actif
Notes		SOC 2 Type II reçu ; prochain résumé de test d'intrusion attendu T3 2026

Valeurs autorisées — Niveau d'accès : aucun, réseau, données en lecture seule, données en lecture-écriture, production · Sous-traitants divulgués : oui, non, demandé · Niveau de criticité : T1, T2, T3 · Statut : actif, en intégration, en cours de revue, escaladé, en cours de sortie.

Checklist des preuves

Référence des champs (le XLSX les porte en colonnes ; exemples issus de la ligne 1) :

Colonne	Conseils	Exemple
Nom du fournisseur		Northcloud ApS
ID		E2
Catégorie de preuves		Certifications & assurance
Éléments à demander		Certificat/attestation en cours de validité dont le périmètre couvre le service hébergé
Types de preuves acceptables		Certificat ISO/IEC 27001 avec périmètre + date d'expiration ; rapport SOC 2 Type II (+ bridge letter si le rapport date de plus de 12 mois) ; C5 le cas échéant
Référence NIS2		Art. 21(3) — qualité des pratiques
Fréquence (T1 / T2 / T3)		Annuel + alertes d'expiration / Annuel / Tous les 3 ans
Date de demande		2026-02-10

Colonne	Conseils	Exemple
Date de réception		2026-03-01
Statut		revu-accepté
Évaluateur		A. Kraus
Notes		ISO 27001 valide jusqu'à 2027-09 ; le périmètre couvre la région EU-West

Valeurs autorisées — ID : E1 à E10 · Catégorie de preuves : Gouvernance / SMSI, Certifications & assurance, Tests d'intrusion, Vulnérabilités & correctifs, Développement sécurisé, Sous-traitants (4es parties), SLA notification d'incident, Continuité & reprise (PCA/PRA), Accès & cryptographie, Personnel & sensibilisation · Statut : non demandé, demandé, reçu, revu-accepté, revu-rejeté, en retard, escaladé, non applicable.

Grille de criticité

Dimension	Question	Score 3	Score 2	Score 1
Dépendance du service	La défaillance du fournisseur perturberait-elle la fourniture de votre service essentiel/important ?	Perturbation immédiate (< 24 h)	Dégradation en quelques jours	Pas d'impact significatif
Accès & données	À quoi le fournisseur peut-il accéder ?	Systèmes de production ou données personnelles sensibles / à grande échelle	Systèmes internes ou données limitées	Aucun accès aux systèmes, pas de données significatives
Substituabilité	En combien de temps pourriez-vous remplacer le fournisseur ?	Plusieurs mois (intégration profonde, peu d'alternatives)	Quelques semaines (des alternatives existent)	Quelques jours (prestation banalisée)
Exposition aux incidents	Une compromission du fournisseur pourrait-elle raisonnablement déclencher pour vous un incident à notifier au titre de l'article 23 de NIS2 ?	Oui, directement	Indirectement / incertain	Non
RÈGLE DE DÉCISION	Total 10–12, ou score 3 à la fois pour « Dépendance du service » ET « Exposition aux incidents » : T1. Total 7–9 : T2. Total 4–6 : T3.	T1 : jeu complet de preuves (E1–E10) ; réévaluation annuelle ; surveillance trimestrielle ; re-demandes déclenchées par événement	T2 : jeu de base (E1–E4, E6–E8) ; revue annuelle	T3 : E2 ou auto-attestation, E6, E7 ; tous les 3 ans / au renouvellement

Instructions

Étape	Action	Où
1	Enregistrez chaque fournisseur direct et prestataire de services : service, contrat, responsables, contacts, niveau d'accès, catégories de données, divulgation des sous-traitants.	Registre des fournisseurs
2	Notez le fournisseur sur les quatre dimensions de la grille et attribuez un niveau (T1/T2/T3) selon la règle de décision. Re-notez à chaque changement significatif ou incident.	Grille de criticité
3	Créez les lignes de preuves applicables au niveau (T1 = E1–E10 ; T2 = E1–E4, E6–E8 ; T3 = E2/attestation, E6, E7) et envoyez les demandes au contact sécurité du fournisseur.	Checklist des preuves
4	Suivez le statut ligne par ligne. Vérifiez le périmètre des certificats, pas seulement leur existence. Rejetez les preuves plus anciennes que la fenêtre de fréquence et redemandez-les en motivant le refus.	Checklist des preuves
5	Escaladez en cas de silence : relance à 10 jours ouvrés ; escalade commerciale à 20 ; mise en demeure invoquant la clause d'audit/de preuves du contrat à 30 ; décision de risque documentée (accepter / compenser / restreindre / résilier) à 45. Consignez chaque étape — la traçabilité est elle-même une preuve de conformité.	Notes de la checklist
6	Actualisez selon la fréquence (T1 annuel + surveillance trimestrielle ; T2 annuel ; T3 tous les 3 ans / au renouvellement) et sur événement déclencheur : incident chez le fournisseur, changement de sous-traitant, expiration de certificat, changement de périmètre, conclusions des évaluations coordonnées des risques au titre de l'article 22(1).	Toutes les feuilles
7	Base juridique : directive (UE) 2022/2555, art. 21(2)(d) et 21(3) ; règlement d'exécution (UE) 2024/2690 ; ENISA Technical Implementation Guidance (juin 2025) et Good Practices for Supply Chain Cybersecurity (juin 2023). Ce classeur constitue une information générale, pas un avis juridique.	—

Gardez les preuves fournisseurs connectées à vos contrôles et à votre Trust Center européen dans Orbiq : orbiqhq.com.