

CHECKLIST GRATUITE · NIS2 · LUXEMBOURG

Checklist NIS2 pour les entreprises au Luxembourg

Savoir où vous en êtes en 10 minutes : 12 points de contrôle sur le champ d'application, les obligations et les mesures — à cocher avec votre équipe.

Base légale	Directive (UE) 2022/2555 (NIS2), transposée au Luxembourg par la loi du 5 mai 2026 relative à des mesures destinées à assurer un niveau élevé de cybersécurité.
Autorités	ILR (Institut Luxembourgeois de Régulation) pour la plupart des secteurs · CSSF pour le secteur financier.
Enregistrement	Auto-enregistrement des entités concernées via le portail de l'ILR (guichet.ilr.lu).
Notification d'incident	Alerte précoce sous 24 heures, notification sous 72 heures, rapport final sous un mois — via la plateforme SERIMA de l'ILR.
Sanctions	Jusqu'à 10 M€ ou 2 % du chiffre d'affaires mondial pour les entités essentielles — avec une responsabilité personnelle de la direction.

Comment utiliser cette checklist

Cochez chaque point que votre entreprise remplit aujourd'hui de manière démontrable. « Démontrable » signifie : il existe un document, un processus ou un journal — pas seulement une impression.

À la fin, comptez vos coches et lisez l'évaluation en dernière page.

A · Déterminer si vous êtes concerné

☐

1. Secteur vérifié

Votre activité a été comparée aux annexes I/II de la directive NIS2 (énergie, transport, santé, infrastructure numérique, industrie manufacturière, poste, déchets, alimentaire, chimie, etc.).

☐

2. Seuil de taille vérifié

Vous savez si vous dépassez le seuil : à partir de 50 salariés ou plus de 10 M€ de chiffre d'affaires ou de total de bilan (exceptions : certains services critiques quelle que soit la taille).

☐

3. Chaîne d'approvisionnement vérifiée

Vous avez vérifié si des clients eux-mêmes soumis à NIS2 vous imposent contractuellement des exigences de sécurité — NIS2 touche souvent les non-concernés via la chaîne d'approvisionnement.

B · Gouvernance & obligations

☐

4. Direction responsabilisée

La direction a approuvé les mesures de cybersécurité, en surveille la mise en œuvre et est elle-même formée — NIS2 prévoit ici une responsabilité personnelle.

☐

5. Enregistrement effectué

Votre entité est enregistrée comme « essentielle » ou « importante » auprès de l'ILR (guichet.ilr.lu), ou de la CSSF si vous relevez du secteur financier.

☐

6. Processus de notification défini

Il est établi qui notifie les incidents significatifs, quand et comment : alerte précoce sous 24 h, notification sous 72 h, rapport final sous un mois (plateforme SERIMA).

C · Mesures techniques & organisationnelles

☐

7. Analyse des risques & politiques

Une analyse des risques documentée et des politiques de sécurité existent et leur efficacité est contrôlée régulièrement.

☐

8. Sauvegarde & plan d'urgence

Un concept de sauvegarde (p. ex. règle 3-2-1-1-0) avec restaurations testées ainsi qu'un plan de continuité d'activité et de gestion de crise sont en place.

☐

9. Accès & chiffrement

Authentification multi-facteurs, gestion propre des droits et chiffrement des données et communications sensibles sont utilisés.

☐

10. Vulnérabilités & détection

La gestion des correctifs est systématique et les attaques sont détectées — par une supervision, voire une surveillance 24/7 (SOC/XDR).

D · Humain & fournisseurs☐**11. Sensibilisation**

Tous les collaborateurs sont régulièrement formés au phishing et aux comportements sûrs — avec justificatifs.

☐**12. Sécurité des fournisseurs**

Les exigences de sécurité envers vos prestataires IT et fournisseurs sont fixées contractuellement et contrôlées.

Évaluation : où en êtes-vous ?

0–4 coches	Besoin d'action élevé. Les obligations de base ne sont pas couvertes — en cas d'assujettissement, vous risquez des sanctions et de longues interruptions. Commencez par les points 1–3 et 8.
5–9 coches	Base solide mais incomplète. Les lacunes typiques : processus de notification, enregistrement et détection des attaques — précisément ce que les contrôleurs regardent en premier.
10–12 coches	Bien positionné. Place à la traçabilité : documentation, procès-verbaux de restauration et revues régulières pour rester prêt pour un audit.

Prochaine étape : audit IT gratuit (90 minutes)

Vous recevez une évaluation écrite de vos points ouverts de cette checklist — sur site ou à distance, sans engagement, en français, allemand ou anglais.

Téléphone : +352 20 60 12 44 · E-mail : mail@local-it-partner.lu · Web : local-it-partner.lu

Situation : août 2026. Cette checklist est une aide d'orientation de Local-IT-Partner S.à r.l.-S et ne remplace pas un conseil juridique. Font foi la directive NIS2 (UE) 2022/2555, la loi luxembourgeoise de transposition et les exigences de l'ILR et de la CSSF.