Checklist de conformité NIS2 — Article 21(2)

Les dix mesures de gestion des risques avec l'évaluation des écarts SMSI — v1.0 · 2026-07-16

#	Mesure (art. 21(2))	Couverture SMSI	L'écart	Que faire	Priorité
(a)	**Politiques d'analyse des risques et de sécurité des systèmes d'information**	Couvert par le SMSI	—	Vérifiez que l'analyse des risques couvre les aspects opérationnels propres à NIS2 : signalement d'incidents, chaîne d'approvisionnement, preuve d'efficacité.	**Faible**
(b)	**Gestion des incidents**	Fondation — ajout opérationnel requis	Capacité opérationnelle 24 h/72 h sous pression — coordination entre sécurité, juridique, communication et direction.	Construisez une gestion des incidents au-delà du plan : exercices sur table contre le délai de 24 heures ; modèles pour les trois étapes de signalement.	**Élevée**
(c)	**Continuité d'activité et gestion de crise**	Couvert par le SMSI	—	Vérifiez que les plans de continuité couvrent les cyberincidents avec obligations simultanées de signalement (article 23).	**Faible**
(d)	**Sécurité de la chaîne d'approvisionnement**	Fondation — ajout opérationnel requis	Surveillance continue au lieu d'instantanés annuels ; réévaluations déclenchées par événement ; preuves fournisseurs récupérables.	Construisez la capacité de surveillance ; passez d'évaluations cycliques à des évaluations déclenchées ; ajoutez des clauses NIS2 aux contrats ; rendez les preuves récupérables à la demande.	**Élevée**
(e)	**Sécurité dans l'acquisition, le développement et la maintenance**	Couvert par le SMSI	Vérifier la divulgation des vulnérabilités au regard des lignes directrices de l'ENISA.	Vérifiez que les processus de divulgation répondent aux attentes NIS2/ENISA — elles vont au-delà des implémentations SMSI typiques.	**Moyenne**
(f)	**Évaluation de l'efficacité des mesures de gestion des risques**	Fondation — ajout opérationnel requis	Disponibilité continue des preuves, pas une documentation au rythme des audits.	Faites passer la gestion des preuves à la disponibilité continue : versionnage, périodes de validité, responsables ; pouvoir répondre aux demandes des autorités en quelques jours.	**Élevée**
(g)	**Cyber-hygiène et formation en cybersécurité**	Couvert par le SMSI	Participation démontrable de la direction à la formation.	Assurez-vous que l'organe de direction participe de manière démontrable aux formations — cette preuve est directement pertinente pour la responsabilité.	**Faible**
(h)	**Cryptographie et chiffrement**	Couvert par le SMSI	—	Maintenez les politiques de cryptographie à jour et alignées sur l'état de l'art.	**Faible**
(i)	**Sécurité du personnel, contrôle d'accès et gestion des actifs**	Couvert par le SMSI	—	Confirmez la couverture MFA là où NIS2 l'exige (voir mesure (j)).	**Faible**
(j)	**MFA, communications sécurisées et communications d'urgence**	Partiellement couvert	Canaux de communication d'urgence sécurisés fonctionnant indépendamment de l'infrastructure régulière (potentiellement compromise).	Auditez la couverture MFA ; établissez des canaux d'urgence indépendants de l'infrastructure régulière ; garantissez une communication chiffrée pour la coordination des incidents.	**Moyenne**

Obligations art. 23 & art. 20

Obligation	Délai / règle	Base juridique
Alerte précoce au CSIRT ou à l'autorité compétente	Dans les 24 heures après avoir eu connaissance d'un incident important	Art. 23(4)(a)
Notification de l'incident	Dans les 72 heures après en avoir eu connaissance — évaluation incl. gravité, impact, indicateurs de compromission	Art. 23(4)(b)
Rapport final	Dans un délai d'un mois après la notification de l'incident	Art. 23(4)(d)
Approbation et supervision des mesures de gestion des risques par l'organe de direction	En continu — l'organe de direction approuve les mesures, supervise leur mise en œuvre et peut être tenu responsable	Art. 20(1)
Formation en cybersécurité de l'organe de direction	Régulière — les membres de l'organe de direction sont tenus de suivre une formation	Art. 20(2)

Comment utiliser cette checklist

1. Passez en revue chacune des dix mesures de l'article 21(2) et évaluez honnêtement : non pas « avons-nous un processus ? », mais « pouvons-nous l'exécuter opérationnellement sous pression, vis-à-vis de parties externes, avec des preuves vérifiables ? »

2. Utilisez la colonne priorité comme point de départ : les trois écarts « Élevée » (gestion des incidents, chaîne d'approvisionnement, preuve d'efficacité) portent l'urgence réglementaire la plus forte.

3. Pour chaque écart, planifiez la construction opérationnelle : quel système, quel processus ou quelle capacité est concrètement nécessaire ?

4. Conservez le SMSI comme couche de contrôle interne et complétez-le par la couche opérationnelle que NIS2 exige en plus.

5. Suivez le statut, le responsable et les preuves par mesure dans la feuille checklist — les autorités peuvent demander des preuves à tout moment.

Explications complètes par mesure, sources et analyse des écarts SMSI :
https://www.orbiqhq.com/fr/reglementations-ue/nis2-checklist-conformite-article-21