Vytalx

Check-list opérationnelle NIS2

Traduire NIS2 en actions vérifiables :
priorités opérationnelles, preuves, préparation à l'audit
(30 minutes)

Vytalx

Comment utiliser cette checklist ?

Cochez chaque point selon votre situation.
L'objectif étant d'identifier rapidement les zones à risque
et de prioriser les actions qui rapproche réellement de la conformité à NIS2

Mode d'emploi

1. **Choisissez un périmètre :**
   Services critiques, SI support, dépendances majeures (prestataires, cloud, opérateurs).

2. **Cochez chaque point :**
   - ✅ Oui = en place et compatible production
   - ⚠️ Partiel = existe, mais incomplet / non standardisé / non prouvé
   - ❌ Non = absent

3. **Notez une preuve (si possible) :**
   politique, procédure, rapport, ticket, compte rendu de test, journal, tableau de bord.

Exemple

"Tests de restauration mensuels"

- ✅ : test daté et documenté
- ⚠️ : test fait "de temps en temps"
- ❌ : aucun test effectué

Scoring simple

- ✅ = 2 points
- ⚠️ = 1 point
- ❌ = 0 point

Les 5 preuves attendues

1. Gouvernance : rôles (DSI/RSSI), RACI, revue périodique / arbitrages
2. Gestion des risques : registre, priorisation, plan de traitement
3. Gestion d'incident : procédure, escalade, modèle de compte rendu
4. Continuité : PRA/PCA, objectifs RTO/RPO, test(s) datés
5. Pilotage : indicateurs, reporting, actions correctives suivies

Ce qui compte : NIS2 attend des mesures proportionnées, mais surtout une capacité à démontrer : "qui fait quoi", "comment", et "avec quelles preuves".

Vytalx

Votre périmètre NIS2

**NIS2 ne se limite pas à des contrôles techniques :
il s'agit d'un dispositif complet (gouvernance, gestion du risque, opérations, continuité, gestion d'incident) qui doit être applicable à votre périmètre critique et démontrable.**

Les 6 thèmes à couvrir

1. **Gouvernance :** responsabilités claires et pilotage régulier
2. **Gestion des risques :** identification, traitement, suivi
3. Mesures techniques : accès, durcissement, sauvegarde, journalisation
4. **Gestion des incidents :** détection, réponse, communication, preuves
5. **Continuité :** PRA/PCA testés, objectifs RTO/RPO, restauration prouvée
6. **Tiers & chaîne d'approvisionnement :** exigences, contrôles, suivi

Contacts & organisation

- Point de contact sécurité : _____
- Point de contact exploitation / infra : _____
- Référent métier (service critique) : _____
- Prestataires clés (NOC/SOC/infogérance/cloud) : _____

Périmètres à couvrir

Service & activité critique	SI support (applications, infra, cloud/SaaS)	Dépendances majeures (prestataires, infogérance, éditeurs, opérateurs)	Propriétaire (métier / IT)	Impact en cas d'arrêt	Preuve disponible ?

Signaux de risque immédiat :

- Périmètre critique non formalisé
- Mesures en place mais sans preuves ni reporting
- Incident/PRA : procédures présentes mais jamais testées
- Dépendances fournisseurs non cartographiées ou non contractuelles
- Pas de propriétaire clair

Vytalx

Checklist : Fondations OT (couverture & compatibilité production)

Point de contrôle	Oui ✅	Partielle ⚠️	Non ❌	N/A	Preuve ? (oui/non) rapport / capture / procédure / ticket / test daté
Un propriétaire de la cybersécurité est identifié (responsabilités explicites, arbitrages possibles)	☐	☐	☐	☐	
La sécurité est pilotée régulièrement (revue périodique, décisions, suivi)	☐	☐	☐	☐	
Une politique de sécurité existe (périmètre, principes, exceptions, mise à jour)	☐	☐	☐	☐	
Le périmètre critique est formalisé (services, SI support, dépendances)	☐	☐	☐	☐	
Un registre de risques cyber existe (menaces, impacts, priorisation)	☐	☐	☐	☐	
Un plan de traitement des risques est suivi (actions, responsables, échéances)	☐	☐	☐	☐	
Des exigences minimales sont définies (mesures attendues, par périmètre)	☐	☐	☐	☐	
La gestion des exceptions est encadrée (justification, durée, validation)	☐	☐	☐	☐	
Inventaire des actifs et des dépendances à jour (IT, cloud, prestataires)	☐	☐	☐	☐	
Gestion des tiers structurée (exigences contractuelles, niveau de service, sécurité)	☐	☐	☐	☐	
Suivi des prestataires critiques (revue périodique, incidents, changements)	☐	☐	☐	☐	
Sensibilisation minimale planifiée (au moins annuel + ciblage profils sensibles)	☐	☐	☐	☐	
Indicateurs sécurité définis et suivis (ex. MFA, patching, sauvegarde, incidents)	☐	☐	☐	☐	
Un dispositif d'amélioration continue existe (actions correctives, revues post-incident)	☐	☐	☐	☐	

Point de vigilance : Sans gouvernance et registre de risques, les mesures techniques restent difficiles à prioriser et encore plus difficiles à démontrer.

Vytalx

Mesures techniques & opérations

Point de contrôle	Oui ✅	Partielle ⚠️	Non ❌	N/A	Preuve ? (oui/non) rapport / capture / procédure / ticket / test daté
MFA déployé (priorité : comptes à privilèges, accès distants)	☐	☐	☐	☐	
Contrôle des accès à privilèges (moindre privilège, revue des admins)	☐	☐	☐	☐	
Durcissement des systèmes (baseline, services inutiles, configurations sensibles)	☐	☐	☐	☐	
Gestion des correctifs (périmètre, cadence, exceptions, suivi)	☐	☐	☐	☐	
Gestion des vulnérabilités (scan, priorisation, remédiation)	☐	☐	☐	☐	
Segmentation réseau (au minimum : zones critiques séparées, flux maîtrisés)	☐	☐	☐	☐	
Sauvegarde des services critiques (périmètre défini, rétention alignée)	☐	☐	☐	☐	
Protection contre suppression/chiffrement pour au moins une copie (immutabilité / équivalent)	☐	☐	☐	☐	
Tests de restauration réalisés (au moins périodiques sur services critiques)	☐	☐	☐	☐	
Journalisation activée sur composants critiques (identités, endpoints, réseau, SaaS)	☐	☐	☐	☐	
Alerting & détection (routage, priorités, responsables)	☐	☐	☐	☐	
Inventaire & contrôle des applications tierces (SaaS/OAuth/connexions).	☐	☐	☐	☐	
Chiffrement / protection des données sensibles (au repos/en transit si applicable)	☐	☐	☐	☐	
Gestion des configurations (traçabilité des changements, sauvegarde des configs)	☐	☐	☐	☐	

Priorité : Concentrez-vous sur l'identités, la sauvegarde/restauration prouvée, la segmentation et journalisation exploitable
Ce sont les fondations qui réduisent le risque rapidement.

Vytalx

Checklist : Incident, continuité & preuves

Point de contrôle	Oui ✅	Partielle ⚠️	Non ❌	N/A	Preuve ? (oui/non) rapport / capture / procédure / ticket / test daté
Procédure de gestion d'incident (détection → triage → réponse → rétablissement)	☐	☐	☐	☐	
Chaîne d'escalade claire (qui décide, qui exécute, qui valide, qui communique)	☐	☐	☐	☐	
Runbooks opérationnels pour scénarios fréquents (compte compromis, ransomware, exfiltration)	☐	☐	☐	☐	
Journal des incidents tenu (chronologie, impact, actions, leçons)	☐	☐	☐	☐	
Exercice de crise / simulation réalisé régulièrement (au moins annuel)	☐	☐	☐	☐	
Capacité de notification cadrée (qui collecte les faits, qui notifie, quels éléments)	☐	☐	☐	☐	
PRA/PCA existants sur le périmètre critique (pas uniquement "sur le papier")	☐	☐	☐	☐	
Objectifs RTO/RPO définis pour les services critiques	☐	☐	☐	☐	
Tests PRA datés (mesure des délais réels, validation applicative)	☐	☐	☐	☐	
Sauvegarde "prouvée" (restauration granulaire, preuves exportables)	☐	☐	☐	☐	
Conservation des preuves (logs/audit) suffisante pour investiguer	☐	☐	☐	☐	
Capacité d'investigation (répondre à "qui a fait quoi, quand")	☐	☐	☐	☐	
Revue post-incident systématique (RCA + plan d'amélioration)	☐	☐	☐	☐	
Tableau de bord de pilotage (incidents, temps de réaction, tests, écarts)	☐	☐	☐	☐	

À retenir : NIS2 ne se limite pas à "avoir un plan" : il faut pouvoir démontrer qu'il est applicable (tests), et qu'il produit des preuves (traçabilité).

Vytalx

Synthèse & plan d'action

Votre résultat

Score total : ____ / ____

Niveau : ☐ Risque élevé (0%-49%) ☐ À consolider (50%-74%) ☐ Structuré (75%-100%)

Barème :	Calcul :
✅ Oui = 2 pts ⚠️ Partiel = 1 pt ❌ Non = 0 pt	Score obtenu = somme des points Score Max = 2 × (nb de lignes évaluées)

Zones rouges

Vos 5 écarts prioritaires :

_____

_____

_____

_____

_____

Points bloquants

- ☐ Périmètre critique non formalisé (services, SI, dépendances)
- ☐ Gouvernance et registre de risques absents (ou non suivis)
- ☐ Gestion d'incident non opérationnelle (pas de runbook / pas d'exercice)
- ☐ Continuité non prouvée (pas de tests PRA / restauration non démontrée)
- ☐ Journalisation / preuves insuffisantes (investigation difficile)

Plan d'action

Phase 1 : Cadrage & gouvernance

- Formaliser le périmètre critique et leurs propriétaires
- Mettre à jour la gouvernance (RACI, revues, exceptions)
- Créer / actualiser le registre de risques et plan de traitement

Phase 2 : Mesures techniques à fort impact

- Verrouiller les identités (MFA + revue privilèges)
- Valider la sauvegarde (périmètre, immutabilité/équivalent, supervision)
- Renforcer la journalisation (identités, endpoints, SaaS, périmètre)

Phase 3 : Incident & continuité opérationnels

- Rédiger 2-3 runbooks (compte compromis, ransomware, exfiltration)
- Définir l'escalade et un modèle de fiche d'incident
- Réaliser un test PRA ciblé (mesure RTO/RPO réel, compte rendu)

Phase 4 : Preuves & pilotage

- Mettre en place un tableau de bord (MFA, patching, incidents, tests)
- Structurer la conservation des preuves (rétention, exports)
- Planifier une revue mensuelle et suivi des actions correctives

contact/vytalx.fr contact@vytalx.fr