Vytalx

NIS2 :
Livre Blanc

"Comprendre les exigences, prioriser les actions, produire les preuves."

Vytalx

Table des matières

Approche opérationnelle

La mise en conformité NIS2 repose sur des mesures proportionnées, mais surtout sur une capacité démontrable : prévention, détection, continuité, et preuves exportables.
VYTALX permet d'industrialiser ces exigences via une plateforme unifiée et un agent unique, avec des briques activables selon le périmètre et le budget.

Vytalx

Cadre

La directive NIS2 (Directive (UE) 2022/2555) fixe un cadre commun visant à élever le niveau de cybersécurité des organisations opérant des services essentiels et importants au sein de l'Union européenne. Elle répond à une intensification des attaques (rançongiciel, fraude, compromissions de chaînes de dépendances) et à la nécessité d'harmoniser les exigences minimales entre États membres.

Les États membres devaient transposer NIS2 au plus tard le 17 octobre 2024, la france est donc en retard. La directive devait remplacer NIS1 à compter du 18 octobre 2024 : les exigences deviennent donc le nouveau socle de référence, même si leur mise en œuvre opérationnelle dépend des textes nationaux.

Ce que NIS2 change concrètement

- **Périmètre élargi :** davantage de secteurs et d'organisations concernées.
- **Gouvernance renforcée :** responsabilités et pilotage au niveau direction.
- **Mesures "proportionnées" mais démontrables :** gestion des risques, sécurité opérationnelle, continuité, preuves.
- **Notification structurée des incidents :** ≤ 24h (alerte initiale), ≤ 72h (notification), ≤ 1 mois (rapport final).
- **Chaîne d'approvisionnement :** exigence accrue sur les fournisseurs critiques.

Note France :

En France, la mise en conformité s'appuie sur les textes nationaux de transposition. La Commission européenne indiquait avoir adressé une reasoned opinion pour défaut de notification de transposition complète (mai 2025), d'où l'intérêt d'anticiper sur les fondamentaux (gouvernance, preuves, résilience, incident).

Vytalx

Comprendre NIS2 : périmètre et organisations concernées

Ce que vise NIS2

NIS2 établit un cadre européen commun pour élever le niveau de cybersécurité des organisations opérant dans des secteurs critiques. Elle repose sur une logique simple : exiger des mesures proportionnées, mais démontrables (pilotage, preuves, tests, traçabilité).

Le périmètre : secteurs couverts

La directive couvre 18 secteurs
Énergie, transport, santé, eau, infrastructures numériques, services numériques, administrations publiques, etc.

Entités “essentielles” vs “importantes”

NIS2 distingue généralement :

Entités essentielles :

Organisations dont l’impact potentiel sur la société/économie est plus élevé et soumises à une supervision plus stricte.

Entités importantes :

Organisations relevant du périmètre mais avec un niveau de supervision généralement différent.

La qualification dépend du secteur, de la taille et, selon les cas, du rôle critique ; les États membres établissent et maintiennent des listes nationales.

Comment savoir si vous êtes concernés

1. Votre activité relève d’un des secteurs NIS2.
2. Votre organisation emploie plus de 50 personnes ou réalise plus de 10 millions d’euros de chiffre d’affaire
3. Vous pouvez vous connecter sur la page “MonEspaceNIS2” de l’ANSSI afin de vérifier votre statut.

Vytalx

Exigences majeures NIS2 : mesures minimales et obligations de notification

NIS2 ne demande pas uniquement “d’avoir des mesures”, mais de pouvoir démontrer qu’elles sont pilotées, appliquées et maintenues. La directive encadre à la fois la gouvernance, un socle de mesures minimales, et un calendrier de notification des incidents.

Gouvernance et responsabilité de la direction

- Les organes de direction doivent approuver les mesures de gestion des risques cyber, superviser leur mise en œuvre, et peuvent être tenus responsables en cas de manquements.
- Les membres de la direction doivent suivre une formation (et l’organisation est encouragée à former régulièrement les équipes).

Preuves attendues : décision formelle / CR de comité, RACI, suivi d’actions, registre d’exceptions, preuves de formation.

Gouvernance et responsabilité de la direction

Les mesures doivent être “appropriées et proportionnées” et inclure au minimum :

- Politiques d’analyse de risques & sécurité SI
- Gestion des incidents
- Continuité : sauvegarde, PRA, gestion de crise
- Sécurité de la chaîne d’approvisionnement
- Sécurité du cycle de vie : acquisition, développement, maintenance.
- Évaluation de l’efficacité des mesures
- Hygiène cyber + formation
- Cryptographie / chiffrement
- Sécurité RH, contrôle d’accès, gestion des actifs
- MFA / authentification continue et communications sécurisées

Notification des incidents : le calendrier à connaître

Pour un incident significatif, NIS2 impose une approche en plusieurs étapes :

- Alerte initiale : ≤ 24h après prise de connaissance
- Notification d’incident : ≤ 72h après prise de connaissance, mise à jour et première évaluation
- Rapport final : ≤ 1 mois après la notification avec “progress report” si l’incident est encore en cours

Quand l’incident est “significatif” ?

- S’il cause (ou peut causer) une perturbation opérationnelle sévère / une perte financière ; ou
- S’il affecte (ou peut affecter) d’autres personnes/organisations par des dommages matériels ou immatériels importants.

Vytalx

Défis et enjeux : de la conformité “papier” à la capacité démontrable

Dans la plupart des organisations, les briques existent déjà partiellement.
La difficulté n’est pas de “tout réinventer”, mais d’industrialiser : prioriser, tester, prouver, et maintenir dans le temps.

Les défis les plus fréquents

- **Hétérogénéité des outils :** détection, sauvegarde, M365, vulnérabilités… pilotés en silos, donc preuves fragmentées.
- **Trop d’alertes, pas assez de qualification :** le signal utile arrive, mais la décision est lente.
- **Continuité non démontrée :** PRA/PCA existent, mais tests rares ou peu réalistes, preuves insuffisantes.
- **Chaîne d’approvisionnement :** fournisseurs critiques identifiés, mais exigences, contrôles et revues restent inconstants.
- **Gouvernance :** décisions et exceptions existent, mais ne sont pas tracées et donc difficiles à démontrer.

Erreurs courantes

- **Confondre rétention et sauvegarde :** la capacité de restauration indépendante et testée reste un attendu.
- **Mesurer la conformité sans routine :** sans cadence de revue, la posture peut dérive.
- **Avoir un plan d’incident sans exercice :** lorsque la menace se présente, tout est plus long, et la preuve manque.
- **Laisser les exceptions s’accumuler :** elles deviennent la norme.

Ce qu’attend un audit

Un audit ou une revue de conformité cherche surtout :

1. Des décisions (gouvernance)
2. Des mesures (réduction du risque)
3. Des preuves (exports, rapports, tests datés)
4. Un cycle d’amélioration (écarts → actions → suivi)

La trajectoire la plus efficace consiste à structurer une capacité démontrable en 4 chantiers : gouvernance, réduction du risque, détection/réponse, continuité et preuves.

Vytalx

Trajectoire de mise en conformité : prioriser, exécuter, prouver

Dans la plupart des organisations, les briques existent déjà partiellement.
La difficulté n'est pas de "tout réinventer", mais d'industrialiser : prioriser, tester, prouver, et maintenir dans le temps.

Étape 1 : Cadrage

Objectif : clarifier le périmètre, les responsabilités et les priorités.

Livrables :

- Périmètre NIS2 (secteurs, services, tiers critiques)
- Nomination / RACI et gouvernance (comité, cadence)
- Registre initial des risques et des écarts majeurs

Preuves attendues :

- Décision formelle et compte rendu de comité
- Registre versionné
- Liste des actifs/services critiques et dépendances

Étape 2 : Réduction du risque

Objectif : sécuriser ce qui réduit le risque rapidement.

Livrables :

- Contrôles identités (comptes à privilèges, MFA, revues)
- Segmentation / durcissement sur actifs critiques
- Gestion vulnérabilités/correctifs (cadence + exceptions)

Preuves attendues :

- Rapports de couverture MFA / privilèges
- Registre d'exceptions
- Compte rendu de revue vulnérabilités et actions

Étape 3 : Détection et réponse

Objectif : réduire le délai de qualification et rendre l'incident gérable.

Livrables :

- Collecte et exploitation des journaux critiques
- Plan de réponse à incident (rôles, escalade, communication, preuves)
- Runbooks "top 3" (compte compromis, ransomware, fuite)

Preuves attendues :

- Règles d'escalade et chronologie type
- Compte rendu d'exercice annuel
- Exports / rapports d'événements critiques

Étape 4 : Continuité et preuves

Objectif : rendre la reprise exécutable et démontrable.

Livrables :

- Sauvegarde protégée contre l'altération
- PRA/PCA avec RTO/RPO par application critique
- Tests réalistes et actions correctives

Preuves attendues :

- Compte rendu de test daté + résultat
- Mesures observées RTO/RPO + écarts
- Historique des corrections et re-tests

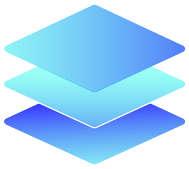
Vytalx

Industrialiser avec VYTALX : capacités, preuves, maîtrise budgétaire

La mise en conformité NIS2 devient fragile lorsqu'elle repose sur une juxtaposition d'outils et de preuves dispersées. L'approche VYTALX vise au contraire une exploitation standardisée, des preuves exportables, et une activation progressive des capacités, en fonction du périmètre et du budget.

Plateforme unifiée et agent unique : industrialiser l'exploitation

Une console unifiée, appuyée sur un agent unique déployé sur postes et serveurs



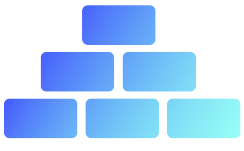
permet d'homogénéiser la mise en œuvre et l'exploitation au quotidien. Cette approche réduit la fragmentation des contrôles, limite les ruptures de responsabilité et facilite la production de preuves exportables. À l'échelle, elle rend les routines plus reproductibles : mêmes méthodes de pilotage, mêmes livrables, mêmes indicateurs, dans la durée.

Intégration dans l'existant : capitaliser sans empilement

L'objectif n'est pas de "remplacer" l'existant, mais de s'y intégrer pour capitaliser sur les pratiques, les outils et les contraintes déjà en place. L'intégration vise à consolider les signaux et à réduire les points de friction opérationnels (collecte, alertes, reporting, preuves), tout en évitant l'empilement de solutions et les intégrations coûteuses. La trajectoire peut ainsi rester progressive, sans dépendre d'un chantier de refonte complet.

Capacités activables selon le besoin

Plutôt qu'un projet monolithique, l'approche consiste à activer des capacités par périmètre fonctionnel, afin d'aligner l'effort sur le risque et les priorités métier. Cela permet d'avancer par étapes, avec une trajectoire progressive et mesurable, sans dépendre d'un déploiement "tout ou rien".



- **Périmètre résilience** : sauvegarde, protection contre l'altération, restauration, tests et preuves.
- **Périmètre Microsoft 365** : protection et restauration granulaire des environnements collaboratifs, avec preuves.
- **Périmètre détection et qualification** : collecte des signaux prioritaires, corrélation, qualification, escalade et reporting.
- **Périmètre sensibilisation** : programme continu, mesure de progression, preuves exploitables.

Vytalx

Passer à une conformité démontrable

NIS2 impose un cadre commun, mais la conformité ne se résume pas à une liste d'exigences.
L'enjeu est de construire une capacité démontrable :
gouvernance, mesures proportionnées, continuité testée, réponse à incident organisée,
et preuves exploitables.

Une trajectoire pragmatique consiste à concentrer l'effort sur ce qui réduit le risque rapidement, puis à industrialiser l'exploitation : routines, rapports, tests, décisions et actions correctives. C'est cette capacité qui fait la différence lors d'un audit, d'une exigence client ou d'un incident.

Réserver un rendez-vous

www.vytalx.fr/contact contact@vytalx.fr