

Préparer l'évaluation NIS2

Guide pour la direction et l'IT • Complète le questionnaire Excel à choix de réponses

Ce document complète la liste de contrôle initiale, « Est-ce que NIS2 s'applique à votre entreprise? » qui reste inchangée. Elle nous aide à comprendre la portée, les responsabilités et la situation connue avant une évaluation ou une vérification. Nous ne vous demandons pas d'effectuer des enquêtes techniques afin de répondre.

Ce que vous obtenez à ce stade

Une vue déclarée de la situation, l'information qui doit être clarifiée et une base pour choisir le service approprié. Il n'en résulte pas une note officielle DNSC, un certificat ou une confirmation de conformité.

Comment remplir le fichier

QUI	OÙ RENSEIGNER	CE QUI EST INDIQUÉ
Coordinateur de la demande	01_Profil et 05_Delais	L'entité, les volumes approximatifs, les rôles de contact et les étapes connues.
Direction / personne désignée	02_Direction — 14 questions	Responsabilités, activités essentielles, risques, décisions et ressources.
IT interne, prestataire ou groupe	03_IT — 24 questions; 04_Cas_particuliers spéciales — 6	Existence de mesures, champ d'application couvert et d'inconnus.

Temps indicatif: 10-15 minutes pour la gestion et 15-25 minutes pour la TI, plus les données du profil. Ce sont des estimations, pas des délais imposés. Une copie est remplie pour chaque entité juridique.

Cinq réponses, sans longs développements techniques

Oui — la situation est connue sur tout le périmètre concerné. Partiellement — seule une partie est couverte. Non — selon les informations connues, la mesure n'existe pas. Nous ne savons pas — l'information ne peut être confirmée. Potentiellement non applicable — expliquez pourquoi ; l'applicabilité sera validée ensuite.

Ne remplir que les cellules jaune pâle. Pour «Oui», la preuve est examinée plus tard. Pour «Possiblement non applicable» l'explication ne constitue pas une exclusion légale. Le résumé compte les réponses; il ne calcule pas un pourcentage de conformité.

Points à clarifier avant l'évaluation

Le questionnaire sépare les décisions de gestion de l'exécution technique. Une entreprise n'est pas considérée comme conforme du seul fait qu'elle détient une licence, et un fournisseur n'est pas supposé avoir assumé toutes les obligations de gestion. [R1–R3]

FONCTION	QUESTION CENTRALE	EXEMPLES INDICATIFS
Gouverner — GV	Qui décide et assure le suivi ?	Responsabilités, politiques, risques, fournisseurs, budget et rapports.
Identifier — ID	Que faut-il protéger ?	Actifs et applications connus, activités critiques, vulnérabilités et dépendances.
Protéger — PR	Qu'est-ce qui réduit le risque ?	Accès, authentification, appareils, données, formation, sauvegardes et segmentation.
Détecter — DE	Qui détecte les problèmes ?	Alertes, journaux, surveillance des événements et horaires réels de surveillance.
Répondre — RS	Que faisons-nous lors d'un incident ?	Remontée des incidents, décisions, limitation des effets, communication et conservation des preuves.
Rétablir — RC	Comment reprendre l'activité ?	Restauration testée, priorités de reprise et canaux alternatifs.

Les six fonctions sont tirées de la structure des mesures DNSC. Les questions sont notre propre synthèse, pas une reproduction du catalogue ou un substitut pour vérifier tous les contrôles applicables. [R3]

Exemples du niveau de détail attendu

Pour l'authentification: «Oui, pour les administrateurs informatiques; inconnu pour tous les autres. » Pour la sauvegarde: « Nous avons des sauvegardes, mais nous ne savons pas quand la restauration a été testée pour la dernière fois. » Pour un groupe: « La sécurité est gérée centralement; la personne responsable locale peut identifier qui confirme la couverture. »

N'envoyez ni données clients ni informations exploitables
Ne saisissez pas les mots de passe, les jetons, les clés, les adresses IP, les configurations, les listes d'utilisateurs, les extraits de système ou les rapports de vulnérabilité.

Les domaines particuliers — développement, nuage, services gérés, OT/IoT/médical, exposition du public et environnement physique — sont clarifiés séparément. Pour les catégories DORA et numérique visées par le règlement 2024/2690, le régime applicable est contrôlé sans que les obligations ne soient pleinement appliquées cumulativement. [R6]

Prestations pouvant suivre

La proposition est préparée une fois que la portée et les besoins identifiés sont compris. L'audit préalable est une étape de préparation commerciale, et non une obligation universelle distincte. Un client peut avoir besoin de procéder directement à une vérification ou peut seulement avoir besoin de compléter certaines preuves.

ÉTAPE	TRAVAUX RÉALISÉS	RÉSULTAT CONCRET
P1 • Évaluation initiale / pré-audit	Applicabilité, risques, documents et mise en œuvre ; entretiens et contrôles autorisés. Préparation de l'autoévaluation selon la procédure applicable.	État des lieux, écarts, preuves et appui aux documents à approuver ou transmettre.
P2 • Audit indépendant	Vérification réglementée effectuée par un vérificateur indépendant certifié par le DNSC; outils, documents, entrevues et tests dans le cadre approuvé.	Rapport d'audit et constats. Un scan seul ne constitue pas un audit.
P3 • Plan et budget	Priorités selon les risques, options de traitement, responsables, délais, dépendances et coûts initiaux/récurrents.	Plan approuvé et budget transparent ; préparation de la transmission si nécessaire.
P4 • Mise en œuvre	Solutions techniques et organisationnelles, configuration, formation, tests de réception et collecte de preuves.	Mesures mises en œuvre et vérifiées ; limites et risques résiduels documentés.
P5 • Entretien et rapports	Revue et nouveaux tests, mise à jour documentaire, appui aux réévaluations et communications requises.	Preuves et rapports de direction à jour ; appui à la clôture des mesures.

Contenu nécessaire de la proposition

Les entités, les sites et les systèmes comprenaient les services et les méthodes, le nombre d'entrevues et de vérifications, les produits livrables, les limites d'accès, les hypothèses, les responsabilités des clients, les coûts initiaux et récurrents, les exclusions, les critères d'acceptation et les conditions pour modifier la portée.

Nous commençons par les mesures existantes. Selon le risque, une exigence peut être traitée par la configuration, une procédure, une formation ou un produit. Choisir une marque n'est pas, en soi, une condition de conformité.

Des prestations clairement distinctes

Le client n'est pas tenu d'acheter chaque étape auprès d'un même fournisseur. La mise en œuvre et l'audit indépendant ont des rôles distincts.

Déroulement de la vérification technique

Un outil peut aider à l'inventaire et à la vérification de certaines configurations, permissions, vulnérabilités ou journaux, en fonction de ses capacités réelles. En soi, il ne peut démontrer la gouvernance, l'acceptation des risques, l'application de toutes les procédures ou le plein respect des exigences.

Avant toute connexion

ÉLÉMENT	ACCORD ÉCRIT
Périmètre et méthode	Systèmes inclus/exclus, méthode de collecte, scans/tests approuvés, fenêtres de temps et règles d'arrêt.
Accès et modifications	Privilèges minimums; accès en lecture seule lorsque la méthode le permet; comptes contrôlés révoqués après le travail.
Données et confidentialité	Données recueillies, stockage, destinataires, durée de conservation et suppression. Accords de confidentialité et de traitement, si nécessaires.
Tiers et systèmes sensibles	Autorisation des propriétaires/fournisseurs; une méthode sûre et des fenêtres approuvées pour les systèmes OT, médicaux et critiques. Pas de balayage actif par défaut.
Livraison et traçabilité	Registre des activités, constatations, preuves pertinentes, limites des outils et questions nécessitant une vérification manuelle.

Le questionnaire n'autorise aucun scan

Choisir «Je voudrais une proposition» ou renvoyer le cahier Excel ne constitue pas un consentement pour l'accès, l'installation d'un agent, la numérisation du système ou les modifications de configuration.

Qui est responsable et qui vérifie

La direction approuve et surveille les mesures, fournit des ressources et assume les obligations applicables. L'équipe chargée de l'évaluation et de la mise en œuvre s'acquitte du mandat convenu. L'auditeur attesté formule de manière indépendante les conclusions de l'audit réglementé. [R1–R2]

L'indépendance est également vérifiée lorsque l'auditeur et l'exécuteur appartiennent à différentes sociétés du même groupe: les services actuels et antérieurs, les relations professionnelles/financières et les incompatibilités prévues à l'article 58 sont examinés. La simple existence de deux sociétés n'est pas suffisante. [R2]

Nous ne promettons pas l'autorisation d'un auditeur de l'auto-évaluation et ne présentons pas l'outil comme l'émission de la certification NIS2. Les rôles, attestations et toute reconnaissance sont vérifiés dans la pratique avant la passation des marchés.

Des constats à la mise en œuvre et au suivi

Un plan utile n'est pas une liste de produits. Chaque constat est relié à une exigence, une preuve, un risque pour l'entreprise et un critère démontrant sa correction.

DANS LE PLAN	POINTS À CLARIFIER
Constat et risque	Ce qui a été vérifié, ce qu'est l'écart, quelle activité peut être affectée et pourquoi elle a une priorité particulière.
Options et coûts	Ce que les solutions existantes peuvent résoudre ; alternatives ; coûts initiaux et récurrents ; hypothèses de calcul.
Responsable et délai	Responsable interne, exécutant, dépendances, indisponibilité nécessaire et délai convenu.
Réception et preuves	Test à réaliser, preuve conservée, personne chargée de la réception et risque résiduel à traiter.
Communication	Document transmis, fondement et délai applicables, approbation de la direction et preuve de communication à l'autorité.

Un calendrier propre à chaque entité

La liste de contrôle initiale et les lignes 05_Delais enregistrent les étapes : enregistrement, décision, évaluation des risques, auto-évaluation, plan et vérification. La date limite pour soumettre le plan après l'auto-évaluation est distincte de la date limite de mise en œuvre et de la voie à suivre pour le plan de vérification. Les articles 12, 18 et 57 de l'ordonnance sont contrôlés séparément. [R2]

La conformité ne découle pas seulement du dépôt d'un document. L'aide à la présentation du plan ou à la communication de l'achèvement des mesures est fondée sur un mandat, l'obligation qui s'applique réellement et la preuve. Les mesures incomplètes ne sont pas déclarées complètes; les bloqueurs et les échéances révisées sont traités dans le cadre applicable.

Les incidents n'attendent pas la fin du projet

La procédure d'exploitation doit tenir compte de la déclaration d'incidents importants : avertissement dans les 24 heures et notification dans les 72 heures suivant la prise de conscience, suivi d'un rapport final et de toute mise à jour dans les délais applicables, sous réserve des exceptions prévues par la loi. [R1–R2]

Ce que vous nous renvoyez maintenant

Seulement le cahier Excel rempli, avec l'information connue et les personnes/rôles qui peuvent le confirmer. Nous établissons ensuite les clarifications, la portée et la proposition. Les documents à l'appui et l'accès technique sont demandés plus tard, par un canal sécurisé et dans les limites convenues.

Fondements et limites de ce document

Le questionnaire technique CSAT/CISv8 reçu comporte 63 questions réparties en 20 thèmes. Elles ont été regroupées en 44 questions en roumain, puis complétées par des domaines du cadre NIS2/DNSC. Le registre interne conserve les questions d'origine, leur emplacement dans Excel et les correspondances établies.

Les niveaux de base, standardisé, rationalisé et dynamique, les valeurs de risque et les recommandations commerciales de la source n'ont pas été convertis en scores DNSC, en budgets ou en obligations d'achat. Un « Oui » est une déclaration à vérifier, pas une preuve. Une réponse « Peut-être non applicable » ne suffit pas à établir ou à approuver une exclusion juridique.

Références réglementaires

REF.	SOURCE ET UTILISATION
R1	Directive (UE) 2022/2555: articles 20 (gestion), 21 (mesures de gestion des risques liés à la cybersécurité), 23 (incidents). EUR-Lex: CELEX 32022L2555.
R2	Ordonnance d'urgence du gouvernement n° 155/2024, approuvée avec modifications par la loi n° 124/2025, version consolidée : art. 11-15, 18, 57-58 et annexes. Portail législatif roumain : document 293121.
R3	DNSC Ordonnance n° 1/2026, publiée le 27 août 2026, annexes concernant les mesures et l'auto-évaluation. Portail législatif roumain: documents 314681 / 314360 / 314683.
R4	Arrêté DNSC n° 2/2026 : modifications du cadre de non-applicabilité et des contrôles de groupe. Portail législatif roumain : document 314676.
R5	DNSC Décision n° 3/2026 et règles pour les groupes: application et preuves locales, responsabilités. Portail législatif roumain: documents 314698 / 314699.
R6	Règlement (UE) 2022/2554 — DORA et règlement d'exécution (UE) 2024/2690, dans leurs champs respectifs. EUR-Lex : CELEX 32022R2554 / 32024R2690.

Les adresses complètes et le rôle de chaque source se trouvent dans la feuille 08_References d'Excel. Date de référence du paquet : 6 octobre 2026. La législation et les procédures applicables à la date de l'évaluation de l'entité doivent être utilisées.

Termes essentiels

MFA : authentification à l'aide de plusieurs facteurs. OT : systèmes contrôlant des processus physiques ou des équipements. Sauvegarde : copie de sécurité ; son existence ne prouve pas qu'une restauration a été testée. Preuve : document, enregistrement ou résultat de test étayant un constat. Risque résiduel : risque restant après les mesures.

Coordination de la demande

Cristian Apostol • office@clarified.ro • +40 774 456 127
it.clarified.ro/nis2