NIS2 · ENTITÉ ESSENTIELLE · GRILLE DE LECTURE

Système OT critique : que devez-vous prouver ?

Checklist et pièces à produire pour un responsable d'application industrielle

Repères CyFun / NIST CSF et références réglementaires · échéance du 18 avril 2027

Pourquoi ce document

La plupart des responsables d'applications industrielles reçoivent une demande de conformité NIS2 sans savoir ce qu'ils doivent concrètement produire, ni jusqu'où descendre. Ce document répond à cette seule question. Il ne remplace pas l'analyse de risque de votre organisation et ne contient aucune donnée propre à une entreprise : c'est une grille de lecture générique, applicable à un système de radiocommunication critique, de supervision, de signalisation, de télégestion ou de contrôle d'accès.

Les trois repères de calendrier

18 octobre 2024 : entrée en vigueur de la loi belge du 26 avril 2024 transposant la directive (UE) 2022/2555.
18 avril 2026 : les entités essentielles transmettent au CCB leur auto-évaluation CyFun Basic ou Important, ou leur politique, périmètre et déclaration d'applicabilité ISO/IEC 27001. Échéance passée.
18 avril 2027 : certification CyFun de niveau Essential par un organisme accrédité, pour les entités essentielles ayant retenu cette voie (AR NIS2 du 9 juin 2024, art. 22, § 2). À défaut, un rapport d'avancement est attendu. La certification ISO/IEC 27001 équivalente est attendue pour le 18 avril 2028.

Indépendamment de ces dates, le service d'inspection du CCB peut réclamer tout document à tout moment (loi NIS2, art. 48, § 1er).

Les deux malentendus à lever d'emblée

1. L'OT n'est pas hors périmètre. Le périmètre d'évaluation couvre l'ensemble des réseaux et systèmes d'information de l'entité. Un système industriel n'en sort pas parce qu'il est ancien, fermé, ou opéré par un tiers. S'il n'est pas explicitement exclu et justifié, il est dedans.
2. La responsabilité ne se transfère pas au fournisseur. L'entité répond de la sécurité de son système, y compris pour la part exploitée par un tiers (directive art. 21, § 2, d). Le contrat répartit le travail, pas la responsabilité.

Les repères CyFun cités sont les sous-catégories du NIST CSF reprises par le référentiel du CCB, croisé avec ISO/IEC 27001 et 27002, les CIS Controls et la série IEC 62443. Vérifiez le numéro exact de la mesure dans la version en vigueur du CyFun Essential avant tout usage en audit.

Comment utiliser cette grille

Les sections 1 à 5 suivent les cinq fonctions du référentiel : identifier, protéger, détecter, répondre, rétablir. La section 6 traite du volet fournisseur, la section 7 réduit le tout à douze pièces à cocher, la section 8 propose un ordre de marche.
Lisez d'abord la section 7. Si une pièce vous manque, remontez à la section correspondante pour savoir ce qu'elle doit contenir. La colonne de droite est écrite pour le terrain : elle indique où porter le regard, pas ce qu'il faut répondre à un questionnaire.

1. Identifier : de quoi est fait ce système, et de quoi dépend-il

Ce que vous devez produire	Repères	Ce que cela veut dire sur le terrain
Inventaire matériel complet et daté	**ID.AM-1** **art. 21.2 i)**	Automates et PLC, RTU, passerelles, coffrets terrain, relais et antennes, terminaux embarqués, serveurs, baies. Pour chacun : référence, version de firmware, site, propriétaire, date de fin de support constructeur. Un inventaire qui s'arrête au niveau serveur ne passe pas.
Inventaire logiciel et applicatif	**ID.AM-2** **art. 21.2 i)**	Applicatifs, middleware, bases de données, firmwares, projets d'automates et leurs fichiers sources, licences et dongles, certificats avec leurs dates d'expiration.
Cartographie des flux	**ID.AM-3** **IEC 62443-3-2**	Matrice des flux entre l'OT et l'IT dans les deux sens : protocole, port, sens, zone, conduit, justification. C'est la pièce que personne n'a et que tout auditeur demande.
Chaîne de dépendances	**ID.BE-4**	Alimentation, réseau, DNS, annuaire, synchronisation horaire, serveur de licences, liaison opérateur, climatisation. En radio comme en signalisation, l'horloge est une dépendance critique et régulièrement oubliée.
Systèmes et accès externes	**ID.AM-4** **art. 21.2 d)**	Liaisons fournisseur, télémaintenance, liens opérateur, interconnexions avec d'autres entités. Chaque accès a un propriétaire, une finalité, une fenêtre et une trace.
Classification et criticité	**ID.AM-5** **art. 21.2 a)**	Cotation en disponibilité, intégrité et confidentialité validée par le métier et non par l'informatique. Position du système dans le portefeuille critique, et conséquence sur le niveau d'assurance visé.
Rôles et responsabilités nominatifs	**ID.AM-6, ID.GV-2** **art. 20**	RACI nommé : responsable applicatif, référent terrain, exploitation, sécurité, fournisseur, et surtout le décideur habilité en crise. Un rôle vacant est un constat d'audit.
Exigences de résilience pour tous les états	**ID.BE-5, PR.PT-5**	Ce que le système doit encore assurer en mode dégradé et en mode secours : fonctions minimales, capacité réduite acceptée, durée maximale tenable.
Analyse de risque documentée	**ID.RA-1 à ID.RA-6** **art. 21.2 a)** **IEC 62443-3-2**	Des scénarios réellement OT : perte du canal de communication, perte de la supervision, corruption d'une configuration, compromission du poste d'ingénierie, perte d'un site, défaillance du fournisseur. Risque résiduel accepté par un responsable nommé.
Gouvernance et dérogations	**ID.GV-1 à ID.GV-4** **art. 20**	Politique applicable au système, dérogations formalisées avec échéance et mesure compensatoire, reporting au management. La responsabilité de l'organe de direction est personnelle.
Chaîne d'approvisionnement identifiée	**ID.SC-1 à ID.SC-5** **art. 21.2 d)**	Fournisseurs et sous-traitants, criticité, dépendance à un acteur unique, compétences internes résiduelles, plan en cas de défaillance du fournisseur.
Registre tenu à jour	**ID.AM** **art. 48.1**	Fréquence de revue, responsable de la mise à jour, source d'autorité unique. Un inventaire de 2022 est un constat, pas une preuve.

2. Protéger : ce qui doit être en place et démontrable

Ce que vous devez produire	Repères	Ce que cela veut dire sur le terrain
Comptes et identités	**PR.AC-1** **art. 21.2 i)**	Liste nominative, comptes techniques et de service documentés avec leur usage, comptes fournisseur individualisés, procédure de retrait à la sortie, revue périodique signée.
Accès distant et télémaintenance	**PR.AC-3, PR.MA-2** **art. 21.2 j)**	Passage par un bastion, authentification forte, ouverture à la demande dans une fenêtre limitée, session enregistrée, accompagnement interne pour les actes sur le terrain. Le VPN permanent du fournisseur est le constat le plus fréquent.
Moindre privilège et séparation des rôles	**PR.AC-4**	Qui peut téléverser une configuration dans un automate, avec quelle validation, et qui ne peut que lire. Exploitation, ingénierie et administration séparées.
Segmentation	**PR.AC-5, PR.PT-4** **IEC 62443-3-2 et 3-3**	Zones et conduits documentés, zone démilitarisée industrielle, aucun flux direct de la bureautique vers le niveau terrain, filtrage justifié flux par flux.
Authentification forte	**PR.AC-7** **art. 21.2 j)**	Sur tous les accès d'administration et fournisseur. Les impossibilités techniques propres à l'OT sont listées, compensées et datées, pas passées sous silence.
Chiffrement et gestion des clés	**PR.DS-1, PR.DS-2** **art. 21.2 h)**	Chiffrement des liaisons et des sauvegardes, inventaire des clés et des certificats, procédure de renouvellement et de révocation. Et surtout : qui détient les clés un dimanche à 3 heures du matin.
Configuration de référence	**PR.IP-1**	Base durcie, export versionné des configurations d'équipements terrain, gestion des écarts. Une configuration qui n'existe que dans l'automate n'existe pas.
Sauvegardes	**PR.IP-4** **art. 21.2 c)**	Pas seulement les serveurs : firmwares, projets d'automates, configurations réseau, clés, licences. Copie hors ligne ou immuable, et preuve de restauration réussie datée.
Plan de continuité et de reprise	**PR.IP-9** **art. 21.2 c)** **ISO 22301, ISO/IEC 27031**	Plan nommé, RTO et RPO validés par le métier, séquence de reprise, prérequis, acteurs, durées. L'écart entre le RTO annoncé et le temps constaté en test doit être assumé par écrit.
Tests de plan	**PR.IP-10** **ISO 22398**	Scénario, date, participants, écarts constatés, procès-verbal signé. Un plan non testé vaut zéro en audit, et souvent moins que zéro en crise.
Maintenance et correctifs	**PR.MA-1** **art. 21.2 e)**	Politique de correctifs adaptée à l'OT, fenêtres d'arrêt négociées avec l'exploitation, traitement des systèmes non corrigeables par mesures compensatoires, suivi des fins de support.
Journalisation	**PR.PT-1** **art. 21.2 f)**	Ce qui est journalisé, la durée de rétention, l'horodatage, l'export vers la supervision de sécurité. Et ce qui n'est pas journalisable côté terrain : à déclarer explicitement plutôt qu'à laisser découvrir.
Résilience technique	**PR.PT-5**	Redondance, répartition des sites, alimentation de secours avec autonomie réellement mesurée, liaison de repli, capacité à fonctionner isolé du réseau central.
Formation des intervenants et du management	**PR.AT-1 à PR.AT-5** **art. 20.2 et 21.2 g)**	Intervenants terrain, astreintes, et direction. La formation des organes de direction est une obligation légale, pas une bonne pratique.

3. Détecter : le maillon le plus faible en environnement industriel

Ce que vous devez produire	Repères	Ce que cela veut dire sur le terrain
Comportement normal de référence	**DE.AE-1**	Profil de trafic et d'activité du système. Sans référence, aucune anomalie n'est détectable et toute alerte est discutable.
Surveillance du réseau industriel	**DE.CM-1, DE.CM-7 art. 21.2 f)**	Détection passive, alerte sur nouvel équipement, nouvelle connexion, poste d'ingénierie inconnu, support amovible branché sur un automate.
Surveillance des accès	**DE.CM-3**	Alerte sur l'usage d'un compte fournisseur hors fenêtre autorisée, élévation de privilège, connexion hors heures ouvrables.
Gestion des vulnérabilités	**DE.CM-8, ID.RA-1 art. 21.2 e)**	Abonnement aux bulletins du constructeur et aux avis sur systèmes industriels, délai de qualification, décision documentée quand on choisit de ne pas corriger.
Seuils, corrélation et escalade	**DE.AE-2, DE.AE-3, DE.AE-5**	Qui reçoit l'alerte, en 24/7 ou non, quel critère déclenche un incident, et comment cela se relie au poste de commandement de l'exploitation.
Rôles de détection	**DE.DP-1 à DE.DP-5**	Qui surveille, avec quel mandat, testé et amélioré. Le trou classique : un système critique que personne ne surveille la nuit et le week-end.

4. Répondre : ce qui doit exister avant l'incident

Ce que vous devez produire	Repères	Ce que cela veut dire sur le terrain
Fiche réflexe d'une page	**RS.RP-1 art. 21.2 b)**	Symptômes, premiers gestes, qui appeler, numéro d'astreinte fournisseur, périmètre d'impact. Critère de qualité : utilisable à 3 heures du matin par quelqu'un qui ne connaît pas le système.
Critères de qualification de l'incident	**RS.AN-4 art. 23**	À partir de quand l'incident devient significatif, qui le décide, et sur quel seuil : durée d'indisponibilité, nombre d'usagers, impact sur la sécurité des personnes.
Chaîne de notification réglementaire	**RS.CO-2 art. 23**	Alerte précoce sous 24 heures, notification sous 72 heures, rapport final sous un mois, vers le CSIRT national. Qui rédige, qui valide, qui envoie. Le canevas doit exister avant, pas pendant.
Communication de crise	**RS.CO-1, RS.CO-3 à RS.CO-5**	Chaîne interne, exploitation, autorité de tutelle, information des usagers, porte-parole. Et le canal de secours prévu si le système touché est lui-même le canal de communication.
Capacité d'analyse et de preuve	**RS.AN-1 à RS.AN-3**	Comment figer une preuve sur un équipement terrain sans interrompre l'exploitation, et qui a l'autorité pour l'ordonner.
Confinement	**RS.MI-1, RS.MI-2**	Comment isoler une zone sans arrêter le service, avec les effets de bord connus à l'avance et la décision tracée.
Coordination fournisseur en crise	**RS.CO-5, ID.SC-5**	Le fournisseur intervient selon un engagement contractuel, pas selon sa disponibilité. Astreinte, délai d'intervention, escalade nominative.

5. Rétablir : la partie que les audits creusent le plus

Ce que vous devez produire	Repères	Ce que cela veut dire sur le terrain
Procédure de restauration testée	**RC.RP-1 art. 21.2 c) ISO/IEC 27031**	Pas à pas, avec des durées mesurées lors d'un test réel et non estimées. Un RTO déclaré sans preuve chronométrée est une intention, pas une capacité.
Ordre de redémarrage et dépendances	**RC.RP-1, ID.BE-4**	Séquence du socle vers l'applicatif, prérequis externes, points de synchronisation, et qui prononce le GO ou le NO-GO.
Jeu de données de référence	**PR.IP-4, RC.RP-1**	Dernière configuration saine identifiée, moyen de vérifier l'intégrité après restauration, données à ressaisir et par qui.
Mode dégradé et retour au nominal	**ID.BE-5**	Procédure d'exploitation sans le système : phonie de secours, procédure papier, conduite manuelle. Durée maximale tenable, et procédure de retour au nominal, souvent plus risquée que la bascule.
Critères de sortie de crise	**RC.RP-1**	Qui déclare le service rétabli, sur quelle preuve, et avec quelle surveillance renforcée après reprise.
Retour d'expérience effectif	**RC.IM-1, RC.IM-2 art. 21.2 f)**	Actions correctives avec responsable et échéance, et mise à jour réelle du plan. C'est ce point qui sépare une organisation conforme d'une organisation résiliente.
Communication de rétablissement	**RC.CO-1 à RC.CO-3**	Information interne, usagers, autorités, et clôture du dossier vers l'autorité nationale avec le rapport final.

6. Volet fournisseur : ce qui doit être écrit au contrat

Cas typique : un système de radiocommunication critique fourni et maintenu par un grand industriel européen, avec une base installée sur le terrain et une télémaintenance. Voici ce que le responsable applicatif doit pouvoir sortir du contrat, et non de la relation commerciale.

Ce que vous devez produire	Repères	Ce que cela veut dire sur le terrain
Exigences de sécurité contractuelles	**ID.SC-3 art. 21.2 d) IEC 62443-2-4**	Niveau de sécurité attendu, durcissement, gestion des comptes, obligations de journalisation et de fourniture de preuves.
Engagement de reprise aligné sur le métier	**ID.SC-5 art. 21.2 c)**	Le délai contractuel doit découler du RTO métier, et non l'inverse. Astreinte 24/7, délai d'intervention sur site, pénalités, moyens de secours.
Participation aux exercices	**ID.SC-5, PR.IP-10**	Le fournisseur participe aux tests de reprise par contrat, fournit ses propres procédures, et le procès-verbal est contradictoire.
Support et fin de vie	**PR.MA-1**	Date de fin de support par version, feuille de route de mise à niveau, engagement de correctifs de sécurité et délai de publication.
Notification d'incident vers l'entité	**ID.SC-4 art. 23 CRA art. 14**	Délai contractuel compatible avec vos 24 heures. Depuis le 11 septembre 2026, le fabricant a lui-même l'obligation de notifier les vulnérabilités activement exploitées sous 24 heures (règlement (UE) 2024/2847). Vérifiez qui vous prévient, vous, et dans quel délai.
Droit d'audit et de vérification	**ID.SC-4 art. 48.1**	Audit, questionnaire, preuve de certification. Une déclaration commerciale n'est pas une preuve d'évaluation de conformité.
Accès aux journaux et aux données	**PR.PT-1**	Accès aux journaux de l'équipement et de la plateforme, dans un format exploitable, sans passer par une demande commerciale à chaque incident.
Réversibilité	**ID.SC-2**	Documentation, configurations, séquestre des sources ou des clés. Objectif : ne pas dépendre d'un acteur unique le jour où il ne répond pas.
Sécurité du produit lui-même	**IEC 62443-4-1 et 4-2 règlement 2024/2847**	Processus de développement sécurisé, nomenclature logicielle, gestion des vulnérabilités sur toute la durée de vie du produit.

7. Les douze pièces à produire

À cocher tel quel. Si une ligne reste vide, c'est votre priorité, pas celle du voisin.

☐	**01.** Inventaire matériel et logiciel daté, descendant jusqu'au niveau terrain
☐	**02.** Cartographie des flux et chaîne de dépendances du système
☐	**03.** Analyse de risque du système, avec risque résiduel accepté et signé
☐	**04.** RACI nominatif, incluant le décideur habilité en crise
☐	**05.** Analyse d'impact métier : RTO, RPO, impacts, validée par le métier
☐	**06.** Plan de reprise détaillé : séquence, prérequis, acteurs, durées
☐	**07.** Preuve de restauration datée, issue d'un test réel avec procès-verbal
☐	**08.** Procédure de mode dégradé et de retour au nominal
☐	**09.** Fiche réflexe incident d'une page, à jour et accessible hors ligne
☐	**10.** Registre des accès fournisseur et des sessions de télémaintenance
☐	**11.** Clauses contractuelles : sécurité, reprise, notification, audit, réversibilité
☐	**12.** Plan d'actions sur les écarts connus, avec responsable et échéance

8. Plan d'action pour le temps restant

Les 30 premiers jours	Inventaire et cartographie des flux, RACI nominatif, et identification des trois écarts qui bloqueraient une reprise réelle. Objectif : savoir où vous en êtes, pas être conforme.
De 30 à 60 jours	Analyse d'impact validée par le métier, plan de reprise rédigé, clauses fournisseur relues avec les achats et le juridique, vérification d'une sauvegarde par restauration réelle d'un composant.
De 60 à 90 jours	Exercice de reprise partiel avec procès-verbal, fiche réflexe testée en conditions réalistes, et constitution du dossier de preuves au même endroit, accessible en une seule demande.
Ensuite, jusqu'à l'échéance	Revue trimestrielle du dossier, exercice complet au moins une fois, suivi du plan d'actions. Un dossier de preuves se constitue en continu, il ne se rattrape pas le mois précédant l'évaluation.

Sources

Directive (UE) 2022/2555 (NIS2), notamment art. 20, 21 et 23. · Loi belge du 26 avril 2024 établissant un cadre pour la cybersécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique, en vigueur le 18 octobre 2024, art. 48. · Arrêté royal du 9 juin 2024 portant exécution de la loi NIS2, art. 22. · CyberFundamentals Framework (CCB), niveau Essential, structuré sur les cinq fonctions du NIST CSF et croisé avec ISO/IEC 27001 et 27002, les CIS Controls et IEC 62443. · Règlement (UE) 2024/2847 (Cyber Resilience Act), art. 14, applicable depuis le 11 septembre 2026. · ISO 22301, ISO/IEC 27031, ISO 22317, ISO 22398, IEC 62443 (parties 2-1, 2-4, 3-2, 3-3, 4-1, 4-2), NIST SP 800-82 rév. 3.

Document générique à usage pédagogique. Il ne contient aucune information propre à une organisation et ne constitue ni un avis juridique ni un livrable d'audit. Vérifiez les numéros de mesure dans la version en vigueur du référentiel avant tout usage formel.