Glossaire NIS2 : français, néerlandais, anglais

Les termes clés de NIS2 et de la loi NIS2 belge dans les trois langues, avec une explication en langage clair. Utile pour les équipes bilingues, les conseils d'administration et les fournisseurs.

NIS2 Aware · nis2aware.eu · novembre 2026

Les termes suivent le vocabulaire officiel de la directive et de la loi belge lorsqu'il existe.

Français	Néerlandais	Anglais	Signification
Alerte précoce	Vroegtijdige waarschuwing	Early warning	Premier signalement au CCB dans les 24 heures après avoir pris connaissance d'un incident significatif.
Amende administrative	Administratieve geldboete	Administrative fine	Sanction financière infligée par l'autorité : jusqu'à 10 M€ ou 2 % du chiffre d'affaires mondial (essentielle) ou 7 M€ ou 1,4 % (importante).
Authentification multifacteur (MFA)	Multifactorauthenticatie (MFA)	Multi-factor authentication (MFA)	Connexion avec au moins deux facteurs différents, par exemple un mot de passe et un code sur votre téléphone.
Autorité nationale de cybersécurité	Nationale cyberbeveiligingsautoriteit	National cybersecurity authority	En Belgique, le Centre pour la Cybersécurité Belgique (CCB) : supervision, inspection, sanctions et accompagnement.
Autorité sectorielle	Sectorale overheid	Sectoral authority	Autorité compétente pour un secteur donné (par ex. finance, télécoms, énergie) qui travaille aux côtés du CCB.
Continuité des activités	Bedrijfscontinuïteit	Business continuity	Maintien des activités critiques pendant et après un incident : sauvegardes, reprise après sinistre, gestion de crise.

CSIRT	CSIRT	CSIRT	Centre de réponse aux incidents de sécurité informatique. En Belgique, CERT.be (au sein du CCB) reçoit les notifications d'incidents.
CyberFundamentals (CyFun®)	CyberFundamentals (CyFun®)	CyberFundamentals (CyFun®)	Cadre belge de mesures de sécurité développé par le CCB, avec les niveaux d'assurance Basic, Important et Essential.
Cyberhygiène	Cyberhygiëne	Cyber hygiene	Bonnes pratiques de sécurité de base au quotidien : mises à jour, authentification forte, sauvegardes, sensibilisation.
Cybermenace	Cyberdreiging	Cyber threat	Toute circonstance ou tout événement susceptible d'endommager ou de perturber les réseaux et systèmes d'information ou leurs utilisateurs.
DORA	DORA	DORA	Règlement européen sur la résilience opérationnelle numérique du secteur financier. Prime sur NIS2 pour la gestion des risques TIC et la notification des incidents des entités financières.
Enregistrement	Registratie	Registration	Déclaration obligatoire d'une entité NIS2 au CCB sur le portail Safeonweb@Work.
Entité essentielle	Essentiële entiteit	Essential entity	Organisation concernée soumise au régime le plus strict : supervision proactive et évaluation de la conformité obligatoire. En général, les grandes organisations des secteurs hautement critiques.
Entité importante	Belangrijke entiteit	Important entity	Organisation concernée avec les mêmes obligations mais une supervision surtout réactive. En général, les organisations moyennes de l'annexe I et moyennes ou grandes de l'annexe II.

Fournisseur de services de sécurité gérés	Aanbieder van beheerde beveiligingsdiensten	Managed security service provider (MSSP)	Prestataire qui exécute ou soutient des tâches de cybersécurité pour ses clients (par ex. surveillance, réponse aux incidents).
Fournisseur de services gérés	Aanbieder van beheerde diensten	Managed service provider (MSP)	Entreprise qui gère des produits, réseaux ou services TIC pour ses clients (par ex. support informatique, hébergement, maintenance).
Incident significatif	Significant incident	Significant incident	Incident qui a causé ou peut causer une perturbation opérationnelle grave ou des pertes financières, ou des dommages considérables à des tiers. Doit être notifié au CCB.
Incident évité	Bijna-incident	Near miss	Événement qui aurait pu compromettre vos systèmes mais qui a été évité ou ne s'est pas concrétisé. Peut être notifié volontairement.
Mesures de gestion des risques en matière de cybersécurité	Maatregelen voor het beheer van cyberbeveiligingsrisico's	Cybersecurity risk-management measures	Mesures techniques, opérationnelles et organisationnelles pour gérer les risques pesant sur les réseaux et systèmes d'information, proportionnées à ces risques.
Notification d'incident	Incidentmelding	Incident notification	Notification au CCB dans les 72 heures, qui complète l'alerte précoce par une première évaluation de l'incident.
Organe de direction	Bestuursorgaan	Management body	Les personnes qui dirigent et contrôlent l'organisation (par ex. conseil d'administration, direction). Doit approuver et superviser les mesures de cybersécurité et suivre une formation.
Organisme d'évaluation de la conformité (OEC)	Conformiteitsbeoordelingsinstantie (CBI)	Conformity assessment body (CAB)	Organisme indépendant, accrédité par BELAC et agréé par le CCB, qui vérifie ou certifie les mesures d'une organisation.

Présomption de conformité	Vermoeden van conformiteit	Presumption of conformity	Une vérification CyberFundamentals ou une certification ISO/IEC 27001 valable (avec le bon périmètre) est présumée démontrer le respect des mesures.
Rapport final	Eindverslag	Final report	Rapport détaillé au CCB dans le mois suivant la notification : description, cause, mesures prises.
Supervision ex ante	Toezicht ex ante	Ex ante supervision	Supervision proactive : l'autorité peut inspecter à tout moment, sans incident préalable. S'applique aux entités essentielles.
Supervision ex post	Toezicht ex post	Ex post supervision	Supervision réactive, surtout après un incident ou des indices de non-conformité. S'applique aux entités importantes.
Sécurité de la chaîne d'approvisionnement	Beveiliging van de toeleveringsketen	Supply chain security	Gestion des risques de sécurité liés à vos fournisseurs et prestataires de services.
Vulnérabilité	Kwetsbaarheid	Vulnerability	Faiblesse d'un système ou d'un produit qui peut être exploitée par un attaquant.
Évaluation de la conformité	Conformiteitsbeoordeling	Conformity assessment	Vérification, par un organisme accrédité ou par l'autorité, que les mesures répondent aux exigences. Obligatoire et périodique pour les entités essentielles.

Information générale sur le cadre NIS2 belge en date de novembre 2026, pas un avis juridique. Consultez toujours les dernières informations du CCB (ccb.belgium.be et atwork.safeonweb.be).