NIS2 glossary: English, French, Dutch

The key terms of NIS2 and the Belgian NIS2 law in the three languages, with a plain-language explanation. Useful for bilingual teams, boards and suppliers.

NIS2 Aware · nis2aware.eu · November 2026

Terms follow the official vocabulary of the directive and the Belgian law where it exists.

English	French	Dutch	What it means
Administrative fine	Amende administrative	Administratieve geldboete	Financial sanction imposed by the authority: up to €10M or 2% of worldwide turnover (essential) or €7M or 1.4% (important).
Business continuity	Continuité des activités	Bedrijfscontinuïteit	Keeping critical activities running during and after an incident: backups, disaster recovery, crisis management.
Conformity assessment	Évaluation de la conformité	Conformiteitsbeoordeling	Check, by an accredited body or the authority, that the measures meet the requirements. Mandatory and periodic for essential entities.
Conformity assessment body (CAB)	Organisme d'évaluation de la conformité (OEC)	Conformiteitsbeoordelingsinstantie (CBI)	Independent body, accredited by BELAC and authorised by the CCB, that verifies or certifies an organisation's measures.
CSIRT	CSIRT	CSIRT	Computer Security Incident Response Team. In Belgium, CERT.be (part of the CCB) receives incident notifications.
Cyber hygiene	Cyberhygiène	Cyberhygiëne	Basic everyday security practices: updates, strong authentication, backups, awareness.

Cyber threat	Cybermenace	Cyberdreiging	Any potential circumstance or event that could damage or disrupt network and information systems or their users.
CyberFundamentals (CyFun®)	CyberFundamentals (CyFun®)	CyberFundamentals (CyFun®)	Belgian framework of security measures developed by the CCB, with assurance levels Basic, Important and Essential.
Cybersecurity risk-management measures	Mesures de gestion des risques en matière de cybersécurité	Maatregelen voor het beheer van cyberbeveiligingsrisico's	Technical, operational and organisational measures to manage the risks to network and information systems, proportionate to those risks.
DORA	DORA	DORA	EU Digital Operational Resilience Act for the financial sector. Takes precedence over NIS2 for ICT risk management and incident reporting of financial entities.
Early warning	Alerte précoce	Vroegtijdige waarschuwing	First report to the CCB within 24 hours of becoming aware of a significant incident.
Essential entity	Entité essentielle	Essentiële entiteit	Organisation in scope with the strictest regime: proactive supervision and mandatory conformity assessment. Typically large organisations in high-criticality sectors.
Ex ante supervision	Supervision ex ante	Toezicht ex ante	Proactive supervision: the authority can inspect at any time, without a prior incident. Applies to essential entities.
Ex post supervision	Supervision ex post	Toezicht ex post	Reactive supervision, mainly after an incident or indications of non-compliance. Applies to important entities.
Final report	Rapport final	Eindverslag	Detailed report to the CCB within one month of the incident notification: description, root cause, measures taken.

Important entity	Entité importante	Belangrijke entiteit	Organisation in scope with the same obligations but mainly reactive supervision. Typically medium-sized Annex I and medium or large Annex II organisations.
Incident notification	Notification d'incident	Incidentmelding	Report to the CCB within 72 hours, updating the early warning with a first assessment of the incident.
Managed security service provider (MSSP)	Fournisseur de services de sécurité gérés	Aanbieder van beheerde beveiligingsdiensten	Provider that carries out or supports cybersecurity tasks for clients (e.g. monitoring, incident response).
Managed service provider (MSP)	Fournisseur de services gérés	Aanbieder van beheerde diensten	Company that manages ICT products, networks or services for clients (e.g. IT support, hosting, maintenance).
Management body	Organe de direction	Bestuursorgaan	The people who lead and control the organisation (e.g. board of directors, executive management). Must approve and oversee the cybersecurity measures and follow training.
Multi-factor authentication (MFA)	Authentification multifacteur (MFA)	Multifactorauthenticatie (MFA)	Logging in with at least two different factors, e.g. a password plus a code on your phone.
National cybersecurity authority	Autorité nationale de cybersécurité	Nationale cyberbeveiligingsautoriteit	In Belgium, the Centre for Cybersecurity Belgium (CCB): supervision, inspection, sanctions and guidance.
Near miss	Incident évité	Bijna-incident	An event that could have compromised your systems but was prevented or did not materialise. Can be reported voluntarily.
Presumption of conformity	Présomption de conformité	Vermoeden van conformiteit	A valid CyberFundamentals verification or ISO/IEC 27001 certification (with the right scope) is presumed to show compliance with the measures.

Registration	Enregistrement	Registratie	Mandatory declaration of a NIS2 entity to the CCB on the Safeonweb@Work portal.
Sectoral authority	Autorité sectorielle	Sectorale overheid	Authority competent for a specific sector (e.g. finance, telecoms, energy) that works alongside the CCB.
Significant incident	Incident significatif	Significant incident	An incident that has caused or can cause severe operational disruption or financial loss, or considerable damage to others. Must be reported to the CCB.
Supply chain security	Sécurité de la chaîne d'approvisionnement	Beveiliging van de toeleveringsketen	Managing the security risks linked to your suppliers and service providers.
Vulnerability	Vulnérabilité	Kwetsbaarheid	A weakness in a system or product that can be exploited by an attacker.

General information on the Belgian NIS2 framework as of November 2026, not legal advice. Always check the latest guidance from the CCB (ccb.belgium.be and atwork.safeonweb.be).