FLASHMODZ ENTERPRISE

Cabinet d’expertise IT — Charleroi · Belgique & international

FlashModz

Mise en conformité NIS2 pour PME en Belgique

Guide NIS2 / PME

La loi belge NIS2 est en vigueur depuis le 18 octobre 2024 et le CCB est passé en phase de contrôle actif en 2026. Des milliers de PME belges sont concernées sans le savoir. Ce guide vous aide à déterminer si vous l'êtes, à comprendre ce qu'on attend de vous, et à construire un plan réaliste sur 6 à 12 mois.

Scannez pour acceder a la version en ligne

contact@flashmodz.be | +32 471 87 87 07

https://flashmodz.be

SYNTHÈSE EXÉCUTIVE

FlashModz

L'essentiel en 5 minutes

NIS2 concerne probablement votre PME. Et le CCB est passé en phase de contrôle actif en 2026.

1

Des milliers de PME belges sont concernées, souvent sans le savoir

NIS2 couvre 18 secteurs (santé, alimentation, logistique, industrie, prestataires numériques…) pour toute entreprise de plus de 50 employés ou 10 M€ de CA. La première étape est une auto-évaluation en 30 minutes, suivie de l'enregistrement obligatoire via Safeonweb@Work. Ne pas être au courant n'est pas une excuse légale.

2

La responsabilité personnelle du dirigeant est engagée

NIS2 art. 20 : les organes de direction doivent approuver et superviser les mesures cyber, et suivre une formation. En cas de manquement grave, sanctions financières personnelles et interdictions temporaires d'exercer. Ce n'est plus une "affaire IT".

3

Les sanctions sont réelles : jusqu'à 10 M€ ou 2% du CA

L'échéance du 18 avril 2026 est passée pour les entités essentielles et le CCB contrôle activement. Les plafonds : 10 M€ ou 2% du CA mondial (entités essentielles), 7 M€ ou 1,4% (entités importantes), avec publication possible des sanctions. Pour une PME qui dépend de contrats grands comptes, l'impact réputationnel pèse autant que l'amende.

4

6 à 12 mois suffisent pour être conforme

Avec une méthode claire, un budget de 25 000 € à 80 000 € selon la taille, et un référentiel adapté (CyFun ou ISO 27001), une PME peut se mettre en conformité en un an. Les 10 domaines NIS2 sont logiques et cumulatifs : pas d'usine à gaz.

5

NIS2 est une opportunité, pas seulement une contrainte

Les PME conformes NIS2 gagnent des contrats grands comptes (qui leur imposent cette conformité), négocient de meilleures conditions d'assurance cyber, et réduisent durablement leurs incidents opérationnels. Le retour sur investissement se mesure dès 18-24 mois.

Et maintenant ?

Les pages qui suivent détaillent chacun de ces points avec exemples, chiffres et actions concrètes.

Document conçu pour PME & ETI (secteurs essentiels / importants) · Lecture : ~15-20 min · Édition 2026

Table des matières

Naviguez rapidement vers les sections qui vous concernent.

Le marché belge en chiffres

Chapitre 1

10 M€

amende maximale NIS2 pour les entités essentielles, ou 2% du CA mondial

Sources : textes officiels (NIS2, RGPD, DORA) et publications des éditeurs cités

18/04/2026

échéance CyFun/ISO 27001 des entités essentielles, dépassée : le CCB contrôle activement

24h

délai maximum de pré-notification d'un incident significatif au CCB

6-12 mois

durée typique d'un projet de mise en conformité NIS2 pour une PME

Contexte & enjeux

Soyons directs : si vous dirigez une PME dans un secteur "essentiel" ou "important" en Belgique, vous êtes probablement soumis à NIS2. Et beaucoup de dirigeants ne l'ont pas encore vérifié.

NIS2 (Network and Information Security 2) a été transposée en Belgique par la loi du 26 avril 2024, en vigueur depuis le 18 octobre 2024. Elle concerne 18 secteurs (contre 7 pour NIS1), dont la santé, l'alimentation, la logistique, l'industrie manufacturière, les prestataires de services numériques, la gestion des déchets, la poste et l'espace. Surtout, elle s'applique dès la taille moyenne : plus de 50 employés ou 10 M€ de chiffre d'affaires. Des milliers de PME belges entrent dans le champ.

Ce qui change concrètement : gestion des risques cyber obligatoire, notification d'incident au CCB dans les 24 heures, responsabilité personnelle des dirigeants (art. 20), sanctions jusqu'à 10 millions d'euros ou 2% du chiffre d'affaires mondial pour les entités essentielles (7 millions ou 1,4% pour les entités importantes), contrôle des prestataires critiques. Et une formalité souvent oubliée : l'enregistrement obligatoire via le portail Safeonweb@Work.

La bonne nouvelle : NIS2 n'est pas une usine à gaz. Pour la plupart des PME, c'est un cadre pragmatique qui oblige à formaliser ce qui devrait déjà exister : politique de sécurité, plan de continuité, inventaire des actifs, gestion des accès, gestion des prestataires. La Belgique offre trois voies pour démontrer sa conformité : la certification CyberFundamentals (CyFun, niveaux Basic, Important ou Essential), la certification ISO/IEC 27001, ou l'inspection directe du CCB.

Le calendrier, lui, ne pardonne plus. L'échéance de mise en conformité CyFun/ISO 27001 des entités essentielles était fixée au 18 avril 2026. Elle est dépassée. Le CCB (Centre pour la Cybersécurité

> *"NIS2 n'est pas un papier à cocher. C'est un levier pour passer d'un IT artisanal à un IT mature, sans reprendre tout de zéro. Les PME qui l'abordent comme une opportunité en sortent transformées."*
>
> — Jérémy Manet, FlashModz Enterprise

Ce que NIS2 change concrètement pour vous

Chapitre 2

Les risques et obligations que beaucoup de PME sous-estiment encore.

Vous êtes probablement concerné sans le savoir

Beaucoup de dirigeants pensent que NIS2 ne concerne que les grands groupes. Faux. Une PME industrielle de 80 personnes à Charleroi, un grossiste alimentaire à Liège, un prestataire logistique à Namur, un cabinet de santé de 60 collaborateurs : tous concernés. Premier réflexe : faire l'auto-évaluation pour savoir où vous vous situez, puis vous enregistrer via Safeonweb@Work si vous êtes dans le champ.

La responsabilité personnelle du dirigeant est engagée

NIS2 art. 20 prévoit que les organes de direction (gérant, CEO, administrateurs) doivent approuver les mesures de gestion des risques ET suivre une formation cyber. En cas de manquement grave, la responsabilité personnelle peut être engagée, avec sanctions pécuniaires et interdictions temporaires d'exercer. Ce n'est plus "un sujet IT".

Les délais de notification sont très courts

24 heures pour la pré-notification au CCB, 72 heures pour le rapport intermédiaire, un mois pour le rapport final. Sans procédure interne claire et testée, vous ne tiendrez jamais ces délais. Et un retard de notification est une infraction sanctionnable en soi, même si l'incident lui-même est bien géré.

Vos prestataires sont votre maillon faible

NIS2 vous rend responsable de la cybersécurité de vos prestataires critiques (art. 21). Votre prestataire IT, votre hébergeur, votre éditeur logiciel, votre cabinet comptable qui a accès à vos données : vous devez pouvoir démontrer que vous avez évalué leurs pratiques et inclus des clauses cyber dans vos contrats. Beaucoup de PME n'ont jamais fait cet exercice.

Le contrôle actif a commencé, les plafonds de sanction sont lourds

L'échéance du 18 avril 2026 est passée pour les entités essentielles et le CCB est entré en phase de contrôle actif. Les plafonds parlent d'eux-mêmes : jusqu'à 10 millions d'euros ou 2% du CA mondial pour les entités essentielles, 7 millions ou 1,4% pour les entités importantes. Les sanctions peuvent être rendues publiques, avec un impact réputationnel durable. "On verra si ça s'applique vraiment" n'est plus une stratégie viable.

Les assurances cyber se durcissent en parallèle

Les assureurs cyber conditionnent désormais leurs polices à un minimum de maturité NIS2 (politique formelle, MFA, sauvegardes testées, plan de réponse). Sans conformité, vous risquez un refus d'assurance, des exclusions multiples ou une prime nettement plus élevée. La conformité NIS2 est devenue un prérequis assurance, pas juste légal.

Vos clients grands comptes vont vous imposer NIS2 par contrat

Si vous êtes fournisseur de grands comptes soumis à NIS2 (banques, énergéticiens, santé publique), ils sont OBLIGÉS d'inclure des clauses NIS2 dans vos contrats. Nous voyons déjà des PME perdre des marchés parce qu'elles ne peuvent pas démontrer leur maturité cyber. Se mettre en conformité, c'est protéger son business.

Mythes vs Réalité

Chapitre 3

Six idées reçues qui empêchent d'agir — et ce qu'en disent les chiffres.

01

ON ENTEND SOUVENT

On est une PME de 80 personnes, NIS2 ne peut pas nous concerner.

EN RÉALITÉ — *Seuils : 50 salariés OU 10 M€ CA*

Faux. NIS2 s'applique à partir de 50 employés ou 10 M€ de CA dans 18 secteurs. Une PME industrielle, un grossiste alimentaire, un cabinet médical multi-sites : toutes concernées. Commencez par une auto-évaluation, c'est gratuit et ça prend 30 minutes.

02

ON ENTEND SOUVENT

Les directives européennes, ça met toujours des années à être vraiment appliqué.

EN RÉALITÉ — *Contrôle actif du CCB depuis 2026*

L'échéance de conformité du 18 avril 2026 est dépassée pour les entités essentielles et le CCB est en phase de contrôle actif. Les assureurs cyber conditionnent leurs polices à NIS2. Vos clients grands comptes l'imposent par contrat. Attendre coûte plus cher que faire.

03

ON ENTEND SOUVENT

NIS2 c'est des politiques à rédiger, rien de concret.

EN RÉALITÉ — *Contrôles opérationnels réels*

NIS2 exige des MESURES techniques vérifiables : MFA, sauvegardes testées, gestion des accès, plans de continuité, tests PRA annuels. Le CCB contrôle la réalité opérationnelle, pas seulement les documents. Les PME qui n'ont "que des politiques" se font épingler.

04

ON ENTEND SOUVENT

On a un prestataire IT, il s'occupe de la cybersécurité.

EN RÉALITÉ

Gouvernance = dirigeant, pas IT

NIS2 impose une gouvernance formelle avec responsabilité du dirigeant. Votre prestataire IT ne peut pas porter cette responsabilité à votre place. Et vous êtes responsable de sa cybersécurité à lui (supply chain art. 21). Il faut documenter, piloter, contrôler. Pas déléguer à l'aveugle.

05

ON ENTEND SOUVENT

Un projet NIS2 c'est 200 000 €, on ne peut pas.

EN RÉALITÉ

Fourchette réaliste PME : 25-80 k€

Pour une PME de 80-150 personnes, un projet NIS2 bien cadré coûte entre 25 000 € et 80 000 € selon la maturité de départ. C'est un investissement amorti en 2-3 ans par la réduction d'incidents, l'amélioration des conditions d'assurance et les contrats gagnés.

06

ON ENTEND SOUVENT

Les directives européennes, c'est toujours complexe et bureaucratique.

EN RÉALITÉ

10 domaines, ~50 mesures pratiques

NIS2 est structurée en 10 domaines logiques. Chaque domaine correspond à 5-10 mesures concrètes. Une PME peut couvrir l'essentiel du sujet avec une vingtaine de mesures bien choisies, et le référentiel CyFun du CCB les liste noir sur blanc. L'usine à gaz vient des cabinets qui veulent facturer, pas du texte lui-même.

Cas concrets en Belgique

Chapitre 4

Trois scénarios types, inspirés de situations réelles et anonymisés.

Grossiste alimentaire en Hainaut (120 employés)

Contexte: Distribution B2B, secteur "alimentaire" donc entité importante NIS2. Pas de RSSI, IT externalisé chez un prestataire local.

Impact: Contrôle CCB en 2026, dans le cadre de la phase de contrôle actif : aucune politique de sécurité formelle, pas d'inventaire des actifs, pas de plan de continuité. Mise en demeure avec 6 mois pour régulariser. Dirigeant personnellement convoqué pour formation cyber obligatoire.

Leçon: Les secteurs qu'on ne croit pas "IT" sont pleinement concernés. L'alimentaire, la logistique, la distribution sont des secteurs essentiels/importants au sens NIS2. Ne pas attendre un contrôle pour s'y mettre.

PME industrielle wallonne (90 employés, équipementier automobile)

Contexte: Entité importante NIS2. Sous-traitant de constructeurs soumis eux-mêmes à NIS2. Pas de CISO, responsabilité cyber floue entre IT et direction générale.

Impact: Client principal (constructeur allemand) exige dans un avenant contractuel 2025 : ISO 27001 OU preuve de conformité NIS2 sous 9 mois. Sans cela, rupture du contrat qui représente 45% du CA de la PME. Projet de conformité lancé en urgence.

Leçon: La pression NIS2 arrive autant par la chaîne de valeur que par le régulateur. Être proactif, c'est préserver ses contrats stratégiques et gagner des marchés face à la concurrence moins mature.

Cabinet médical multisite à Bruxelles (55 collaborateurs)

Contexte: Entité importante NIS2 (secteur santé + taille > 50 employés). Ransomware double-extorsion fin 2024. Chiffrement des dossiers patients et exfiltration de données.

Impact: Notification CCB effectuée à H+96 au lieu de H+24 (procédure inexistante). Or le défaut de notification est une infraction en soi, passible pour une entité importante d'une amende pouvant atteindre 7 M€ ou 1,4% du CA. En ajoutant remédiation, perte d'exploitation et honoraires de crise, la facture dépasse de très loin le coût d'une préparation sérieuse.

Leçon: Ce n'est pas l'incident qui coûte le plus cher : c'est le défaut de préparation et de procédures. Quelques dizaines de milliers d'euros investis en amont pèsent peu face à une amende et une crise mal gérée.

Avant / Après — la différence concrète

Chapitre 5

Ce qui change quand on passe d'une posture artisanale à une posture maîtrisée.

Avant mise en conformité	Après mise en conformité NIS2
01 POSTURE FACE À UN CONTRÔLE CCB	
Panique, recherche de documents dans tous les sens, réponses approximatives. Sanction probable.	Dossier conformité prêt, politiques signées, preuves de mise en œuvre. Le contrôleur repart rassuré.
02 GESTION D'UN INCIDENT	
Cellule de crise improvisée, notification CCB à H+96 au lieu de H+24, sanction pour retard.	Procédure claire, cellule mobilisée en 30 min, notification sous 24h avec toutes les informations requises.
03 NÉGOCIATION ASSURANCE CYBER	
Prime × 3 ou exclusions multiples. Certains assureurs refusent de couvrir.	Prime négociée à la baisse, meilleures franchises, couverture étendue. L'assureur devient un partenaire.
04 MARCHÉS B2B GRANDS COMPTES	
Perte de contrats car incapacité à démontrer la maturité cyber demandée par le client.	Argument commercial différenciant. Les clients grands comptes privilégient les fournisseurs conformes.
05 RESPONSABILITÉ DU DIRIGEANT	
Exposition personnelle non maîtrisée. Sanctions possibles, interdictions temporaires d'exercer.	Formation effectuée, gouvernance formalisée, décisions documentées. La responsabilité est mesurée.
06 INCIDENTS OPÉRATIONNELS	
Plusieurs incidents par an avec impact business significatif. Pas d'amélioration continue.	Nette réduction des incidents, année après année. Les procédures s'améliorent après chaque événement.

07 COÛT ANNUEL CYBER

- Dépenses éparses non coordonnées. ROI difficile à démontrer au COMEX.

- Budget cyber piloté, rattaché à des indicateurs mesurables. Le COMEX voit le retour sur investissement.

Auto-évaluation de maturité

Chapitre 6

Faites le point en 5 minutes : où en êtes-vous vraiment ?

Pour chaque question, cochez la case qui correspond le mieux à votre situation actuelle.

SITUATION	NON	PARTIEL	OUI
1. J'ai déterminé formellement si mon organisation est soumise à NIS2 (essentielle, importante, hors champ).	☐	☐	☐
2. Si concerné, mon organisation est enregistrée auprès du CCB via Safeonweb@Work.	☐	☐	☐
3. Une voie de démonstration de conformité est choisie : CyFun (Basic/Important/Essential), ISO/IEC 27001 ou inspection du CCB.	☐	☐	☐
4. Un responsable NIS2 est désigné au sein de l'organisation (peut être cumulé DPO/DSI).	☐	☐	☐
5. Le COMEX/CA a approuvé formellement une politique de sécurité de l'information.	☐	☐	☐
6. Une analyse de risques documentée existe et est révisée au moins annuellement.	☐	☐	☐
7. J'ai un plan de continuité d'activité (BCP) et un plan de reprise technique (PRA) testés.	☐	☐	☐
8. Mes prestataires critiques sont inventoriés, évalués et soumis à clauses cyber contractuelles.	☐	☐	☐
9. Une procédure de notification d'incident avec délais 24h/72h/1 mois est documentée et testée.	☐	☐	☐
10. Les dirigeants (COMEX/CA) ont suivi une formation cyber avec attestation.	☐	☐	☐
11. L'ensemble du personnel est sensibilisé annuellement (1-2h), avec traçabilité de la participation.	☐	☐	☐
12. La MFA est généralisée sur tous les accès sensibles (email, VPN, admin, applications critiques).	☐	☐	☐
13. Les sauvegardes sont testées au moins 2× par an avec exercice de restauration complet.	☐	☐	☐
14. Un tableau de bord NIS2 permet au COMEX de suivre la conformité et les incidents.	☐	☐	☐

SCORING : Non = 0 pt • Partiel = 1 pt • Oui = 2 pts

< 40% : Critique • 40-70% : À renforcer • > 70% : Bonne posture

Ce qu'on met en place avec vous

Chapitre 7

De l'audit de conformité à la mise en œuvre concrète, sans usine à gaz.

Diagnostic NIS2 express (demi-journée)

Nous déterminons si vous êtes concerné (essentielle / importante / non concernée), nous vérifions votre enregistrement Safeonweb@Work, nous identifions les 10 écarts les plus critiques et nous vous remettons un rapport actionnable. Forfait fixe, sans engagement de suite. Idéal pour le COMEX qui hésite à se lancer.

Audit de conformité NIS2 complet

Analyse exhaustive des 10 domaines NIS2 (gouvernance, risques, continuité, supply chain, incidents, sensibilisation, cryptographie, RH, actifs, accès). Livrable : matrice de conformité, plan de remédiation priorisé, estimation budgétaire. 5 à 10 jours selon la taille.

Sprint de mise en conformité (3 à 6 mois)

Accompagnement opérationnel pour combler les écarts critiques : rédaction des politiques, mise en place de la gouvernance, tests de PCA/PRA, formation des équipes, procédures d'incident. Forfait jalonné, livrables testables à chaque étape.

RSSI fractionnel (vCISO) pour PME

Vous n'avez pas les moyens d'un RSSI à temps plein. On met à votre disposition un RSSI externe 2 à 5 jours par mois : pilotage du plan NIS2, reporting COMEX, gestion de crise, interface CCB et assureur. Coût d'un profil junior pour l'expertise d'un senior.

Formation dirigeants NIS2 (art. 20)

NIS2 exige que les dirigeants soient formés à la cybersécurité. Nous proposons un format 2h dédié au COMEX/board : enjeux NIS2, responsabilités personnelles, questions à poser à votre DSI, mise en situation d'incident. Attestation formelle fournie.

Gestion de crise cyber & notification CCB

En cas d'incident, vous disposez de 24h pour notifier. Nous intervenons : coordination de la cellule de crise, rédaction de la notification, interface avec CCB et CERT.be, communication aux parties prenantes. Les clients vCISO bénéficient d'un circuit d'escalade convenu à l'avance.

Audit supply chain (prestataires critiques)

Évaluation de vos prestataires IT/cloud/données sous l'angle NIS2 : collecte questionnaires, analyse contractuelle, classement des risques, plan de remédiation. Inclut la rédaction d'un addendum cyber à intégrer à vos contrats-cadres.

Notre façon de travailler

Une méthode en 4 étapes, progressive, pensée pour votre réalité. Pas de slides : des livrables concrets à chaque étape.

1

VOIR CLAIR

AUDIT

On commence par comprendre votre contexte : cartographie de l'existant, entretiens avec les équipes, identification des vrais risques. Pas de diagnostic à distance, pas d'hypothèses. On part de ce qui existe chez vous.

2

PRIORISER ENSEMBLE

PLAN

Qu'est-ce qui est urgent, qu'est-ce qui peut attendre ? On construit le plan avec vous, pas à votre place. Chaque action est pondérée par son impact, son effort et votre budget. Vous gardez la main sur les décisions.

3

STABILISER

ACTION

On corrige, on durcit, on protège. Des actions concrètes et mesurables, livrées par jalons. À chaque étape, vous validez avant qu'on avance. Pas de surprise, pas de dérive budgétaire.

4

TRANSMETTRE

AUTONOMIE

On documente tout ce qu'on fait, on forme vos équipes, on vous laisse les clés. Notre succès se mesure à votre capacité à continuer sans nous. Pas de dépendance, du transfert de compétences.

Feuille de route en phases

Chapitre 8

Un chemin balisé, du diagnostic à la maturité — étape par étape.

1	2	3	4	5
SEMAINE 1-2	MOIS 1-2	MOIS 2-4	MOIS 4-9	MOIS 9-12
Auto-évaluation	**Diagnostic**	**Fondations**	**Opérationnel**	**Preuves & audit**
• Périmètre NIS2 • Safeonweb@Work • Sponsor COMEX	• Audit 10 domaines • Écart critique • Plan priorisé • Budget validé	• Politiques • Gouvernance • Analyse risques • Formation COMEX	• PCA/PRA testés • Procédures incidents • Supply chain • Sensibilisation	• Dossier conformité • Audit blanc • Tableau de bord • Amélioration continue

Conseil méthodo

Chaque phase est un livrable autonome. Vous pouvez vous arrêter à n'importe quelle étape ou ralentir le rythme selon votre budget et votre charge interne. L'important n'est pas la vitesse — c'est de ne pas reculer.

Cadre réglementaire & articulations

Chapitre 9

Comment NIS2 s'articule avec RGPD, ISO 27001, DORA et les autres textes.

Mesures de gestion des risques

NIS2 art. 21

10 domaines obligatoires : politique d'analyse des risques, gestion des incidents, continuité d'activité, supply chain, sécurité acquisition, efficacité mesurée, hygiène cyber, cryptographie, sécurité RH, accès et actifs.

BÉNÉFICE CACHÉ :

Bien menée, cette structuration réduit sensiblement vos incidents opérationnels et simplifie tout audit futur (ISO, assureur, client grand compte).

Responsabilité du dirigeant

NIS2 art. 20

Les organes de direction doivent approuver les mesures de gestion des risques cyber et suivre une formation. En cas de manquement, responsabilité personnelle engagée, avec sanctions et interdictions possibles.

BÉNÉFICE CACHÉ :

La formation des dirigeants transforme le sujet cyber de "contrainte IT" en "sujet stratégique". Les COMEX formés prennent de meilleures décisions d'investissement cyber.

Notification d'incident

NIS2 art. 23

Pré-notification au CCB sous 24h, rapport intermédiaire sous 72h, rapport final sous 1 mois. Applicable aux incidents "significatifs" : impact opérationnel, données, services rendus.

BÉNÉFICE CACHÉ :

Avoir une procédure claire et testée réduit le temps de décision en cellule de crise de plusieurs heures. C'est le premier test de maturité en cas de vrai incident.

Articulation RGPD / NIS2

RGPD + NIS2

Un incident peut déclencher simultanément une notification RGPD (72h à l'APD) et NIS2 (24h au CCB). Les deux régimes se complètent : RGPD pour les données personnelles, NIS2 pour la continuité des services.

BÉNÉFICE CACHÉ :

Une procédure unifiée RGPD+NIS2 économise plusieurs heures en cas de crise. Et permet d'aligner DPO et RSSI sur une communication cohérente.

Trois voies pour démontrer la conformité

CyFun / ISO 27001

En Belgique, une entité NIS2 démontre sa conformité de trois façons : certification CyberFundamentals (CyFun, niveaux Basic, Important, Essential), certification ISO/IEC 27001, ou inspection directe du CCB.

BÉNÉFICE CACHÉ :

Choisir sa voie tôt structure tout le projet. CyFun est calibré pour les PME belges. ISO 27001 valorise aussi à l'international. L'inspection directe laisse le tempo au régulateur, rarement à votre avantage.

Checklist détachable — vos actions prioritaires

Imprimez cette page, cochez au fur et à mesure. Les colonnes EFFORT et IMPACT vous aident à séquencer.

		EFFORT	IMPACT	DÉLAI
☐	Réaliser l'auto-évaluation NIS2 (grille CCB) pour déterminer votre périmètre.	1/5	4/5	Cette semaine
☐	Enregistrer l'organisation via Safeonweb@Work (obligatoire si concernée).	1/5	3/5	15 jours
☐	Choisir la voie de conformité : CyFun (Basic/Important/Essential) ou ISO 27001.	1/5	3/5	1 mois
☐	Désigner un responsable NIS2 interne (avec lettre de mission).	1/5	4/5	1 mois
☐	Organiser la formation cyber obligatoire du COMEX/CA (2h minimum).	2/5	4/5	2 mois
☐	Faire approuver une politique de sécurité de l'information par la direction.	2/5	4/5	2 mois
☐	Réaliser une analyse de risques documentée (méthode EBIOS RM ou équivalent).	3/5	4/5	3 mois
☐	Inventorier les prestataires critiques et évaluer leur maturité cyber.	3/5	3/5	3 mois
☐	Mettre en place (ou vérifier) la MFA généralisée sur les accès sensibles.	2/5	4/5	2 mois
☐	Tester le PCA/PRA avec un exercice complet (table-top + technique).	3/5	4/5	4 mois
☐	Rédiger et tester la procédure de notification d'incident (24h/72h/1 mois).	2/5	4/5	3 mois

		EFFORT	IMPACT	DÉLAI
☐	Lancer une campagne de sensibilisation cyber (tous les salariés, 1-2h).	🟢🟢⚪⚪⚪	🟢🟢🟠🔴⚪	4 mois
☐	Mettre en place un tableau de bord NIS2 pour le COMEX (trimestriel).	🟢🟢⚪⚪⚪	🟢🟢🟠⚪⚪	6 mois
☐	Préparer le dossier conformité (audit blanc avant contrôle réel).	🟢🟢🟠⚪⚪	🟢🟢🟠🔴🔴	9 mois

CONSEIL : Commencez par les actions à fort impact ET faible effort (les "quick wins").

Si vous bloquez sur une action, contactez-nous : on vous oriente gratuitement.

Questions fréquentes

Chapitre 10

Les questions que nos clients posent le plus souvent — et nos réponses sans détour.

Q1. Comment savoir si mon entreprise est soumise à NIS2 ?

Deux critères cumulatifs. Le secteur : 18 secteurs concernés (énergie, transport, banque, santé, eau, espace, alimentation, logistique, industrie manufacturière, prestataires numériques, gestion des déchets, poste, recherche, administration publique, etc.). La taille : plus de 50 employés ou 10 M€ de CA. Si les deux sont remplis, vous êtes concerné et l'enregistrement via Safeonweb@Work est obligatoire. Le CCB publie un test d'auto-évaluation en ligne.

Q2. Quelle est la différence entre entité essentielle et entité importante ?

Entité essentielle : organisation de grande taille (>250 employés ou CA >50 M€) dans un secteur très critique (énergie, banque, santé, transport, eau, prestataires TIC). Obligations renforcées, sanctions jusqu'à 10 M€. Entité importante : organisation de taille moyenne (50-250 employés ou CA 10-50 M€) dans un secteur listé. Obligations proportionnées, sanctions jusqu'à 7 M€. La plupart des PME sont "importantes".

Q3. Combien coûte une mise en conformité NIS2 pour une PME ?

Ordre de grandeur pour une PME de 80-150 personnes : 25 000 € à 80 000 € sur 6-12 mois, selon la maturité de départ. Ce budget couvre l'audit, la rédaction des politiques, la formation COMEX, l'accompagnement opérationnel, et les premiers tests. Les investissements techniques (MFA, sauvegardes, EDR) viennent en complément et dépendent de l'existant.

Q4. Que se passe-t-il en cas de contrôle CCB ?

Le CCB contrôle à distance (questionnaire + documents) ou sur site. Depuis 2026, il est en phase de contrôle actif : l'échéance de conformité du 18 avril 2026 est passée pour les entités essentielles. L'approche reste proportionnée : si un écart est constaté, une mise en demeure avec délai de remédiation est généralement prononcée (typiquement 3 à 6 mois) avant sanction. Les amendes sont réservées aux manquements graves ou répétés, et aux défauts de notification d'incident.

Q5. NIS2 et RGPD, c'est la même chose ?

Non, mais les deux se complètent. RGPD protège les données personnelles (notification à l'APD sous 72h). NIS2 protège la continuité des services numériques (notification au CCB sous 24h). Un même incident peut déclencher les deux. Une PME mature unifie sa gouvernance : DPO et RSSI travaillent ensemble, les procédures sont communes, les tableaux de bord sont croisés.

Q6. Peut-on utiliser ISO 27001 pour démontrer la conformité NIS2 ?

Oui. En Belgique, ISO/IEC 27001 est même l'une des trois voies officielles de démonstration de conformité, avec la certification CyFun et l'inspection directe du CCB. Si vous êtes déjà certifié ISO 27001, vous avez l'essentiel. Il reste quelques briques spécifiques (notification 24h, formation des dirigeants, enregistrement Safeonweb@Work) pour boucler le dossier. Inversement, NIS2 est une bonne porte d'entrée pour viser ISO 27001 ensuite.

Q7. Qu'est-ce que CyFun et quel niveau viser ?

CyberFundamentals (CyFun) est le référentiel du CCB, décliné en trois niveaux : Basic, Important et Essential. Le niveau attendu dépend de votre classification : une entité importante vise généralement le niveau Important, une entité essentielle le niveau Essential. La certification CyFun est l'une des trois voies officielles de conformité NIS2 en Belgique, pensée pour être plus accessible qu'ISO 27001 pour une PME. L'échéance de certification des entités essentielles était fixée au 18 avril 2026.

Q8. Le dirigeant risque-t-il vraiment sa responsabilité personnelle ?

Oui. NIS2 art. 20 est explicite : les organes de direction sont personnellement redevables des mesures de gestion des risques. En cas de manquement grave, les sanctions peuvent inclure des amendes personnelles ET des interdictions temporaires d'exercer des fonctions dirigeantes. C'est l'un des changements majeurs par rapport à NIS1. La formation est obligatoire ET protectrice.

Q9. Combien de temps pour se mettre en conformité ?

Pour une PME partant de zéro (pas de politique, pas de procédures) : 9 à 12 mois avec un accompagnement structuré. Pour une PME déjà mature (MFA, sauvegardes, politiques de base) : 4 à 6 mois. L'essentiel n'est pas la vitesse mais la solidité. Cela dit, l'échéance d'avril 2026 étant passée pour les entités essentielles, chaque mois d'attente augmente l'exposition en cas de contrôle.

Glossaire

Chapitre 11

Tous les termes techniques de ce guide, expliqués en français clair.

APO

Align, Plan and Organize. Domaine COBIT qui couvre la stratégie IT, l'architecture, le portefeuille, les RH, le budget, les risques.

BAI

Build, Acquire and Implement. Domaine COBIT qui couvre la conduite des projets, les développements, les acquisitions et la gestion des changements.

BNB

Banque Nationale de Belgique. Régulateur principal DORA pour banques, assurances et institutions financières systémiques.

Bus factor

Nombre de personnes dont l'absence bloquerait une fonction critique. Un "bus factor de 1" est un risque organisationnel majeur.

CCB

Centre pour la Cybersécurité Belgique. Autorité nationale de cybersécurité. Gère le CERT.be, publie des recommandations, et est l'interlocuteur privilégié pour NIS2.

CERT

Computer Emergency Response Team. Équipe qui reçoit, analyse et répond aux incidents cyber. CERT.be est opéré par le CCB.

COBIT

Framework de gouvernance IT publié par l'ISACA. Version 2019 propose 40 objectifs de gouvernance et management alignables avec ISO 27001, NIS2, CIS Controls.

CyFun

CyberFundamentals. Référentiel de certification du CCB à trois niveaux (Basic, Important, Essential). Une des trois voies officielles pour démontrer sa conformité NIS2 en Belgique, avec ISO/IEC 27001 et l'inspection directe du CCB.

DORA

Digital Operational Resilience Act. Règlement (UE) 2022/2554, applicable depuis le 17 janvier 2025 à tout le secteur financier. Impose un cadre harmonisé de résilience opérationnelle numérique.

DPIA / AIPD

Analyse d'impact relative à la protection des données. Obligatoire sous RGPD pour les traitements à risque élevé. Souvent couplée aux analyses de risques NIS2.

DSS

Deliver, Service and Support. Domaine COBIT dédié à l'exploitation : incidents, demandes, continuité, sécurité opérationnelle.

EDM

Evaluate, Direct and Monitor. Premier des 5 domaines COBIT 2019, le seul de pure gouvernance. Porté par le conseil et la direction : évaluer, orienter, surveiller.

ENISA

Agence européenne pour la cybersécurité. Publie des référentiels techniques, guides et orientations pour NIS2, DORA, EUCS, etc.

Entité essentielle

Sous NIS2 : organisation de grande taille (>250 employés ou CA >50M€) dans un secteur critique (énergie, santé, transport, finance, eau, espace). Obligations renforcées.

Entité importante

Sous NIS2 : organisation de taille moyenne (50-250 employés ou CA 10-50M€) dans un secteur listé. Obligations proportionnées mais réelles.

FSMA

Autorité belge des services et marchés financiers. Régulateur DORA pour certains PSF et gestionnaires d'actifs en Belgique.

Gouvernance IT

Ensemble de règles, processus et structures qui assurent que l'IT supporte et améliore la stratégie business. Pilier de COBIT.

Incident majeur

Sous NIS2/DORA : incident cyber qui cause une perturbation opérationnelle significative ou affecte un grand nombre d'utilisateurs. Déclenche des obligations de notification.

ISMS

Information Security Management System. Système de management de la sécurité de l'information, formalisé dans ISO 27001 et attendu sous NIS2.

Maturité (CMMI)

Niveau de maturité d'un processus (1 à 5). Cadre utilisé par COBIT pour évaluer la maturité IT d'une organisation.

MEA

Monitor, Evaluate and Assess. Domaine COBIT qui mesure la performance, le contrôle interne et la conformité aux exigences externes.

NIS2

Directive européenne de 2022 qui impose des obligations cybersécurité à ~160 000 entités dans l'UE. Transposée en Belgique par la loi du 26 avril 2024, en vigueur depuis le 18 octobre 2024. Remplace NIS1 avec un périmètre beaucoup plus large.

Notification 24h

NIS2 exige une pré-notification au CCB dans les 24h suivant la prise de conscience d'un incident significatif. Puis rapport complet sous 72h.

Notification 72h

DORA/NIS2 : notification officielle complète de l'incident avec analyse d'impact et mesures prises. Peut être étendue à 1 mois pour le rapport final.

Plan de continuité (BCP)

Business Continuity Plan. Document qui décrit comment maintenir les activités critiques en cas de sinistre. Obligatoire sous NIS2 et DORA.

PRA / DRP

Plan de Reprise d'Activité / Disaster Recovery Plan. Volet technique du BCP : comment remonter les systèmes IT après incident.

RACI

Matrice de responsabilités : Responsible, Accountable, Consulted, Informed. Outil central en gouvernance COBIT et en conformité NIS2.

Registre des prestataires

DORA art. 28 : tout acteur financier doit maintenir un registre complet de ses prestataires TIC critiques, avec classement des risques.

Safeonweb@Work

Portail du CCB où toute entité soumise à NIS2 doit s'enregistrer. Sert aussi de point d'entrée pour l'auto-évaluation et les échanges avec l'autorité.

TLPT

Threat-Led Penetration Testing. Test d'intrusion avancé basé sur les menaces réelles, obligatoire tous les 3 ans pour les grandes institutions financières (DORA).

Ressources externes

Chapitre 12

Sites officiels, outils gratuits et lectures recommandées pour aller plus loin.

CCB — Centre pour la Cybersécurité Belgique

ccb.belgium.be

Autorité NIS2 en Belgique. Publie guides sectoriels, recommandations techniques et seuils d'application. Interlocuteur principal pour toute PME concernée.

Safeonweb@Work

atwork.safeonweb.be

Portail du CCB pour l'enregistrement obligatoire des entités NIS2, l'auto-évaluation et l'accès aux outils CyberFundamentals (CyFun).

CERT.be

cert.be

Équipe nationale de réponse aux incidents cyber. Portail officiel de notification d'incidents NIS2. Veille hebdomadaire sur menaces.

ENISA

enisa.europa.eu

Agence européenne cybersécurité. Référentiels techniques NIS2, DORA, modèles de politiques, guides sectoriels gratuits.

BNB — Banque Nationale de Belgique

nbb.be

Régulateur DORA pour banques et assurances. Publie les circulaires, attentes prudentielles et le processus de désignation des prestataires TIC critiques.

FSMA

fsma.be

Autorité des services financiers. Régulateur DORA pour entreprises d'investissement, gestionnaires d'OPC et certains PSF belges.

EBA, EIOPA, ESMA

eba.europa.eu

Trois autorités européennes de supervision financière. Publient les RTS/ITS DORA qui précisent les exigences techniques.

ISACA — COBIT 2019

isaca.org/resources/cobit

Éditeur officiel de COBIT. Publications, certifications CGEIT/CISA, documentation framework, design toolkit.

ANSSI — Guides pratiques

cyber.gouv.fr

Agence française de cybersécurité. Nombreux guides gratuits applicables en Belgique : hygiène cyber, ISO 27001, gestion de crise.

NIST Cybersecurity Framework

nist.gov/cyberframework

Référentiel américain largement adopté. Compatible NIS2 et COBIT. Versions 1.1 (2018) et 2.0 (2024) en libre accès.

CIS Controls v8

cisecurity.org/controls

18 contrôles prioritaires de cybersécurité maintenus par le Center for Internet Security. Base pratique pour implémenter NIS2 ou DORA.

À propos de FlashModz Enterprise

FlashModz Enterprise est un cabinet d'expertise IT opérationnelle, fondé par Jérémy Manet et basé à Farciennes, dans la région de Charleroi. Conseil et mise en œuvre concrète : sécurité, audit et pentest, automatisation Linux/DevOps et formations — pour les particuliers comme pour les entreprises, en Belgique et à l'international. Notre conviction : les ressources, les connaissances pointues et les outils des grandes entreprises doivent être accessibles aux PME et aux indépendants. À leur échelle. À leur budget. Avec la même rigueur.

CE QUE NOUS FAISONS

- Audit sécurité
- Pentest & rapport
- Sprint de stabilisation
- Team Lead fractionnel
- Formations Linux / DevOps

CERTIFICATIONS & RÉFÉRENTIELS

- CWNA · Ruckus
- Cisco Meraki
- Fortinet NSE
- Veeam
- Jamf · Apple
- OWASP / PTES
- NIS2
- ISO 27001
- RGPD

Jérémy Manet

Fondateur · Ingénieur & architecte système/réseau

Plus de 15 ans en architecture et ingénierie système/réseau : infrastructure, Wi-Fi d'entreprise, sécurité et virtualisation. Également management (people & technique) et gouvernance IT en tant que Process Owner COBIT, DORA et NIS2. Certifié CWNA, Cisco Meraki, Fortinet, Veeam, Jamf, Apple. Technologies : Aruba, HPE, Cisco, FortiGate, Nutanix.

Spécialités : Architecture · Réseau · Wi-Fi · Sécurité · Virtualisation · Gouvernance · NIS2 · DORA

De l’expertise IT pour ce qui compte vraiment.

contact@flashmodz.be · +32 471 87 87 07 · flashmodz.be

LinkedIn Facebook TikTok Avis Google

IDENTITÉ LÉGALE

FlashModz Enterprise

DÉNOMINATION	FlashModz Enterprise
FONDATEUR	Jérémy Manet
SIÈGE SOCIAL	Rue du Wainage 18, 6240 Farciennes (Belgique)
BCE / TVA	1035.510.038 · BE 1035.510.038
EU VAT	2.386.268.987
ZONES DESSERVIES	Charleroi et alentours (B2C) · Belgique & international (B2B)
CONTACT	contact@flashmodz.be · +32 471 87 87 07 · flashmodz.be

FlashModz

Faites le point sur votre exposition NIS2

Chaque entreprise est unique. Chaque idée a ses contraintes,
son contexte et ses priorités.

C'est pourquoi nous ne proposons pas de grille tarifaire figée.
Nous préférons échanger avec vous, comprendre votre situation
et construire une réponse adaptée à vos vrais besoins.

Parlons de votre situation

EMAIL

contact@flashmodz.be

TELEPHONE

+32 471 87 87 07

WEB

flashmodz.be

RETROUVEZ-NOUS

LinkedIn Facebook TikTok Avis Google

Scannez pour accéder
à ce document

BCE 1035.510.038 | Charleroi · Belgique & international