FLASHMODZ ENTERPRISE

Cabinet d’expertise IT — Charleroi · Belgique & international

FlashModz

DORA — Résilience opérationnelle numérique en Belgique

Guide DORA / Finance

DORA (règlement (UE) 2022/2554) est applicable depuis le 17 janvier 2025 et les contrôles BNB/FSMA s'intensifient en 2026. Si vous êtes banque, assurance, gestionnaire d'actifs, PSF ou fintech, ce guide vous accompagne dans la conformité : registre prestataires, tests de résilience, gouvernance TIC.

Scannez pour acceder a la version en ligne

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

https://flashmodz.be

L'essentiel en 5 minutes

DORA est applicable depuis janvier 2025 et les contrôles BNB/FSMA s'intensifient en 2026. Les écarts sont nombreux, même dans les

1

DORA s'applique en droit direct (pas de transposition nationale)

Contrairement à NIS2, DORA est un règlement UE : applicable directement depuis le 17 janvier 2025, sans besoin de loi belge. Les autorités belges (BNB, FSMA) ont commencé à contrôler dès le premier semestre 2025. Le temps de grâce est terminé.

2

Le registre des prestataires TIC est votre premier chantier

La plupart des institutions découvrent, en faisant l'exercice du registre (art. 28), qu'elles n'ont pas la visibilité attendue sur leurs prestataires, surtout les sous-traitants de 2e niveau. C'est le point de départ pragmatique, et il conditionne toute la conformité DORA.

3

Les TLPT révèlent des angles morts que les pentests classiques ne voient pas

Pour les grandes institutions, le TLPT (art. 26-27, coordonné via TIBER-BE) est un exercice de 4 à 12 semaines, nettement plus avancé qu'un pentest. Il mesure votre capacité réelle à détecter et contenir un attaquant qui prend son temps. DORA vous force à regarder cette réalité en face, au moins tous les 3 ans.

4

La responsabilité monte au board

Le board (conseil d'administration) approuve la stratégie TIC, suit les indicateurs, se forme (art. 5). Dans beaucoup d'institutions, cette remontée est un vrai changement culturel, pas juste documentaire. La BNB et la FSMA lisent les procès-verbaux de board pour vérifier.

5

Proportionnalité pour les petits acteurs, mais socle minimum exigeant

PSF, fintechs, petits gestionnaires : vous êtes soumis à DORA avec des allègements, mais le socle minimum (politique TIC, registre prestataires, procédures incidents, tests de résilience) est incontournable. Anticiper est toujours moins coûteux que corriger sous contrainte régulateur.

Et maintenant ?

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

Document conçu pour Secteur financier (banques, assurances, PSF, fintechs) · Lecture : ~15-20 min · Édition 2026

© 2026 FlashModz Enterprise — https://flashmodz.be

Table des matières

Naviguez rapidement vers les sections qui vous concernent.

© 2026 FlashModz Enterprise — https://flashmodz.be

Le marché belge en chiffres

Chapitre 1

17/01/2025

date d'entrée en application de DORA en droit direct (sans transposition)

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

2%

du chiffre d'affaires : plafond des sanctions encourues en cas de manquement à DORA

20 000+

entités financières européennes concernées par DORA (+ leurs prestataires TIC critiques)

3 ans

fréquence minimale des tests TLPT (Threat-Led Penetration Testing) pour les grandes institutions

Contexte & enjeux

Parlons franchement. DORA (Digital Operational Resilience Act, règlement (UE) 2022/2554) est probablement la réglementation la plus structurante imposée au secteur financier européen depuis MiFID II. Applicable en droit direct depuis le 17 janvier 2025, elle concerne l'ensemble des entités financières belges : banques, assurances, entreprises d'investissement, gestionnaires d'OPC, établissements de paiement, prestataires de services sur cryptoactifs, et leurs prestataires TIC critiques.

Ce qui change fondamentalement : DORA impose un cadre harmonisé (fini les différences BNB / FSMA / régulateurs étrangers) et exigeant de résilience opérationnelle numérique. Cinq piliers : gestion des risques TIC (art. 5 à 16), gestion et notification des incidents (art. 17 à 23), tests de résilience dont les TLPT (art. 24 à 27), gestion des risques liés aux tiers avec le registre des prestataires (art. 28 à 30), partage d'information (art. 45).

Pour une banque ou une assurance de taille moyenne en Belgique, DORA représente typiquement 18 à 24 mois de projet, 400 à 800 K€ d'investissement, et une refonte en profondeur de la gouvernance IT, du registre des prestataires, des procédures d'incident et des pratiques de test.

La BNB (Banque Nationale de Belgique) et la FSMA sont les régulateurs compétents. Leur message est clair : ils attendent des preuves opérationnelles, pas seulement documentaires. Les premières inspections DORA ont eu lieu courant 2025, et 2026 marque une nette intensification des contrôles. Les écarts constatés sont nombreux, même dans les institutions matures. Les sanctions peuvent atteindre 2% du chiffre d'affaires.

© 2026 FlashModz Enterprise — https://flashmodz.be

La bonne nouvelle : DORA est structuré de façon pragmatique. Le règlement s'appuie sur des référentiels

> *"DORA oblige le secteur financier à passer de la politique à la preuve. C'est exigeant, c'est structurant, et c'est une vraie opportunité de redescendre la cybersécurité du niveau technique au niveau stratégique."*
>
> — Jérémy Manet, FlashModz Enterprise

Les vrais enjeux DORA pour le secteur financier belge

Chapitre 2

Les risques opérationnels, réglementaires et business que DORA vous oblige à regarder en face.

Le registre des prestataires TIC est plus complexe qu'il n'y paraît

DORA art. 28 impose un registre complet de TOUS les prestataires TIC, avec classification des risques, des prestations critiques, et transmission annuelle aux autorités. Chez la plupart des acteurs, ce registre n'existe pas au niveau de granularité attendu. Reconstituer l'historique des contrats, identifier les sous-traitants critiques, évaluer les risques de concentration : 3 à 6 mois de travail à temps partagé.

Les TLPT vont révéler des faiblesses que vous ne soupçonnez pas

Pour les grandes institutions (seuils fixés par les ESA), DORA art. 26 exige un TLPT tous les 3 ans. Un TLPT n'est pas un pentest classique : c'est une simulation d'attaquant avancé sur 4 à 12 semaines, coordonnée en Belgique via le cadre TIBER-BE, avec des scénarios réalistes (APT, insider, supply chain). L'exercice mesure votre capacité réelle de détection et de réaction. Le verdict est rarement flatteur au premier passage.

La gouvernance du risque TIC doit remonter au board

DORA art. 5 place la responsabilité au sommet : le board approuve la stratégie de gestion des risques TIC, assure la formation adéquate de ses membres, et revoit régulièrement les indicateurs clés. Dans beaucoup d'institutions, le sujet reste piloté au niveau comité exécutif ou CRO. La remontée au board complet implique des changements structurels dans la gouvernance.

La classification des incidents est plus stricte qu'avant

DORA (art. 17 à 19) et les RTS des ESA (EBA/EIOPA/ESMA) définissent très précisément les seuils d'incident "majeur" à notifier. Critères : clients affectés, durée, perte financière, portée géographique, impact sur les services critiques. Les équipes cyber sont habituées aux incidents internes, mais doivent apprendre à qualifier au sens DORA le jour même, pas à H+72.

Les prestataires TIC critiques sont désignés par le régulateur

Les "Critical Third-Party Providers" (CTPP) sont désignés par les ESA à partir de critères objectifs (part de marché, nombre de clients financiers, substituabilité). Une fois désigné, votre prestataire tombe sous supervision directe des ESA. Impact : clauses contractuelles renforcées, possibilité d'audits régulateur, obligations d'exit plans.

© 2026 FlashModz Enterprise — https://flashmodz.be

La concentration sur le cloud est un angle mort majeur

La plupart des institutions belges ont concentré leur IT sur AWS, Azure ou Google Cloud. DORA vous oblige à cartographier cette concentration, évaluer les scénarios de défaillance, et avoir un plan de sortie (exit plan) crédible. Constater en 2026 qu'on ne peut pas sortir de son cloud provider en moins de 18 mois est devenu un problème de conformité, pas juste stratégique.

Les petits acteurs (PSF, fintechs) sont aussi concernés

Beaucoup de PSF et fintechs belges pensent que DORA ne concerne que les grandes banques. Faux. DORA propose un principe de proportionnalité (exigences allégées pour les petites entités), mais le socle minimum reste exigeant. Une fintech de 20 personnes doit avoir un registre prestataires, une politique TIC, des procédures d'incident et des tests de résilience.

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 petite fintech, DORA ne peut pas vraiment s'appliquer à nous.

EN RÉALITÉ — *Proportionnalité ≠ exemption*

Faux. DORA s'applique à tout le secteur financier réglementé : établissements de paiement, PSF, gestionnaires d'OPC, prestataires de cryptoactifs. Principe de proportionnalité existe (exigences allégées) mais le socle minimum est obligatoire. Et la FSMA contrôle aussi les petits acteurs.

02

ON ENTEND SOUVENT

Notre ISO 27001 couvre toutes les exigences de DORA.

EN RÉALITÉ — *ISO 27001 = base, pas suffisant*

Non. ISO 27001 couvre une bonne partie du socle, mais pas les exigences propres à DORA : registre structuré des prestataires (art. 28), clauses contractuelles de l'art. 30, TLPT, exit plans cloud, gouvernance portée par le board (art. 5). Le gap est réel, et le régulateur le vérifie.

03

ON ENTEND SOUVENT

AWS est conforme à tous les standards, on est couverts.

EN RÉALITÉ — *Responsabilité finale = chez vous*

La responsabilité DORA reste chez VOUS, pas chez le cloud provider. Vous devez : (1) avoir des clauses contractuelles conformes, (2) avoir un plan de sortie crédible, (3) tester les scénarios de défaillance, (4) documenter la concentration. Aucun cloud provider ne peut faire ça à votre place.

© 2026 FlashModz Enterprise — https://flashmodz.be

04

ON ENTEND SOUVENT

Les régulateurs vont nous laisser le temps, on a encore 2-3 ans.

EN RÉALITÉ — *Contrôles intensifiés en 2026*

Les premières inspections DORA ont eu lieu courant 2025 et les contrôles BNB/FSMA s'intensifient en 2026. Les sanctions peuvent atteindre 2% du CA. Attendre, c'est prendre le risque d'un contrôle en pleine crise (incident, rotation d'équipe, migration cloud) où on ne peut pas répondre.

05

ON ENTEND SOUVENT

On fait déjà un pentest annuel, le TLPT c'est la même chose en plus long.

EN RÉALITÉ — *TLPT ≠ pentest standard*

Non. Un TLPT implique : (1) threat intelligence contextuelle à votre institution, (2) scénarios réalistes d'attaquant motivé, (3) test sur systèmes de production avec règles d'engagement strictes, (4) durée 4-12 semaines vs 2-3 semaines pour un pentest, (5) coordination TIBER-BE/BNB, (6) testeurs accrédités. C'est nettement plus coûteux, et incomparablement plus formateur.

06

ON ENTEND SOUVENT

Les RTS et ITS ne sont pas tous publiés, on va attendre.

EN RÉALITÉ — *RTS/ITS essentiels publiés*

L'essentiel des RTS/ITS a été publié en 2024 et 2025. Les quelques textes restants ne bloquent pas le démarrage de la mise en conformité. Au contraire : les institutions qui ont commencé en 2024 sont largement en avance sur celles qui attendent encore en 2026. Le temps joue contre vous.

Cas concrets en Belgique

Chapitre 4

Trois scénarios types, inspirés de situations réelles et anonymisés.

Banque universelle belge de taille moyenne

Contexte: Banque universelle, ~2500 employés, présente en Belgique et au Luxembourg. Entité essentielle NIS2 + soumise à DORA. Gouvernance cyber mature, ISO 27001 certifiée.

Impact: Inspection BNB ciblée DORA en mai 2025. Écarts identifiés : registre prestataires incomplet (sous-traitants de 2e niveau non couverts), TLPT jamais réalisé, exit plan cloud inexistant. Mise en demeure sur 12 mois. Budget projet correctif : 1,2 M€.

Leçon: Être ISO 27001 certifiée n'équivaut pas à être DORA-compliant. Le diable se cache dans la supply chain (sous-traitants de sous-traitants) et la résilience opérationnelle prouvée, pas seulement documentée.

Gestionnaire d'actifs bruxellois (95 collaborateurs)

Contexte: Société de gestion d'OPC, FSMA-régulée. Sous-traite 80% de son IT à deux prestataires (hébergement + logiciel de gestion portefeuille). Gouvernance IT légère.

Impact: Premier exercice registre prestataires révèle : 3 sous-traitants TIC critiques, aucun classé comme tel dans les contrats, clauses cyber absentes ou obsolètes. Renégociation en urgence. Coût : 180 000 € sur 9 mois (externe + interne).

Leçon: L'externalisation ne dispense pas des obligations DORA : elle les renforce (art. 28 à 30). La responsabilité finale reste chez vous, et prouver que vos prestataires sont conformes demande un travail contractuel et technique important.

Fintech wallonne spécialisée paiements (35 personnes)

Contexte: Établissement de paiement sous contrôle BNB, ~3 ans d'existence. Culture "move fast", pas de CISO à temps plein, IT principalement sur AWS.

Impact: Audit BNB en 2025 : aucune politique TIC formelle, pas de registre prestataires structuré, pas d'exit plan AWS, pas de test de résilience depuis 12 mois. Mise en demeure sous 6 mois avec risque de retrait d'agrément. Projet de mise en conformité en urgence : 280 000 €.

Leçon: La proportionnalité DORA ne dispense pas du socle minimum. Pour une fintech en forte croissance, anticiper DORA dès la levée de fonds est un choix stratégique qui évite la crise ultérieure avec le régulateur.

Avant / Après — la différence concrète

Chapitre 5

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

	Institution "DORA-unprepared"	Institution "DORA-mature"
01	**REGISTRE DES PRESTATAIRES TIC**	
	• Liste Excel partielle, pas de classification des risques, sous-traitants de 2e niveau invisibles.	• Outil structuré avec classification, analyse de concentration, revue annuelle par le board, transmission régulateur automatisée.
02	**GOUVERNANCE DU RISQUE TIC**	
	• Sujet porté au comité exécutif ou CRO, peu visible au board. Formation cyber du board inexistante.	• Board approuve la stratégie TIC, revoit les KPI trimestriellement, formation annuelle documentée.
03	**TESTS DE RÉSILIENCE**	
	• Pentest annuel externe, pas de programme structuré. PRA théorique, jamais testé en condition réelle.	• Programme multi-niveau annuel (scans, pentests, exercices, TLPT), tests PRA bisannuels documentés.
04	**GESTION D'INCIDENT**	
	• Procédure générique, classification subjective, notification tardive au régulateur. Pas d'entraînement.	• Procédure alignée sur les seuils DORA, entraînement trimestriel (table-top + technique), notification sous 24h testée.
05	**PLANS DE SORTIE CLOUD**	
	• Inexistants ou théoriques. "On ne sortirait jamais d'AWS". Concentration non analysée.	• Exit plans documentés et testés sur un workload critique. Concentration cloud analysée et validée board.
06	**PRÉPARATION INSPECTION RÉGULATEUR**	
	• Panique, mobilisation 3 semaines d'équipes pour rassembler les preuves. Écarts découverts en direct.	• Dossier toujours à jour, preuves tracées dans l'outillage GRC, réponses rapides et factuelles aux questions.

© 2026 FlashModz Enterprise — https://flashmodz.be

07 RELATIONS AVEC PRESTATAIRES CRITIQUES

- Contrats anciens, clauses cyber absentes ou génériques. Dépendance non maîtrisée.

- Contrats refondus DORA, clauses cyber détaillées, revues de performance annuelles, partenariat équilibré.

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. Le board approuve formellement la stratégie de gestion des risques TIC et suit les indicateurs clés.	☐	☐	☐
2. Nous avons un registre complet des prestataires TIC avec classification critique/important/standard.	☐	☐	☐
3. Les sous-traitants de 2e niveau des prestataires critiques sont identifiés et évalués.	☐	☐	☐
4. Les contrats avec les prestataires TIC critiques incluent toutes les clauses DORA obligatoires.	☐	☐	☐
5. Nous avons des exit plans documentés et testés pour les prestataires cloud critiques.	☐	☐	☐
6. Notre méthodologie d'analyse de risques TIC est formalisée et revue annuellement.	☐	☐	☐
7. Un programme de tests annuel couvre : scans, pentests, exercices cyber, tests PCA/PRA.	☐	☐	☐
8. Si éligible au TLPT : nous avons un cycle en cours ou planifié avec TIBER-BE.	☐	☐	☐
9. La procédure de notification d'incident est alignée sur les seuils et calendriers DORA (art. 17 à 19).	☐	☐	☐
10. Les membres du board ont suivi une formation cyber formelle dans les 12 derniers mois.	☐	☐	☐
11. Nous testons nos procédures de crise (table-top + technique) au moins 2× par an.	☐	☐	☐
12. La classification des incidents est faite en moins de 24h, de manière cohérente et traçable.	☐	☐	☐
13. Un outillage GRC permet de suivre en temps réel notre conformité DORA.	☐	☐	☐
14. Les indicateurs clés DORA sont remontés au board au moins trimestriellement.	☐	☐	☐

© 2026 FlashModz Enterprise — https://flashmodz.be

15. Un audit blanc DORA a été conduit par une partie externe indépendante dans les 18 derniers mois.	☐	☐	☐

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 aux tests TLPT, une expertise secteur financier.

Diagnostic DORA en 5 jours

Analyse des 5 piliers DORA appliquée à votre contexte spécifique (banque/assurance/PSF/fintech). Livrable : matrice de conformité, top 10 écarts, roadmap priorisée avec budget. Inclut un entretien COMEX de restitution. Forfait fixe.

Audit registre prestataires TIC (art. 28)

Cartographie complète de vos prestataires TIC, classification (critique/important/standard), analyse de concentration, évaluation des clauses contractuelles au regard de l'art. 30, identification des sous-traitants de 2e niveau critiques. Livrable exploitable par la direction juridique et les achats.

Préparation TLPT (Threat-Led Penetration Testing)

Accompagnement pour les grandes institutions soumises au TLPT : cadrage réglementaire avec TIBER-BE, sélection des testeurs qualifiés, coordination avec la BNB, préparation des équipes bleue/rouge/pourpre, conduite de l'exercice, plan d'action post-TLPT. Mission 3 à 6 mois.

Élaboration de la politique TIC DORA

Rédaction sur-mesure de la politique de gestion des risques TIC conforme DORA art. 5 et 6 : gouvernance, rôles, méthodologie risques, relations tiers, continuité, indicateurs. Politique validée par le COMEX/board, intégrée à votre ISMS existant.

Tests de résilience & exercices cyber

Conception et animation d'exercices cyber réalistes : table-top COMEX, simulation d'incident technique, test PCA/PRA complet, scénarios de défaillance prestataire critique. Avec rapport formel et plan d'action. Idéal pour faire progresser toute la ligne de défense.

© 2026 FlashModz Enterprise — https://flashmodz.be

Gestion d'incident TIC avec notification DORA

En cas d'incident TIC majeur, nous intervenons : coordination de la cellule de crise, qualification réglementaire (seuils des art. 17 à 19 et RTS), rédaction des notifications aux autorités (BNB/FSMA), communication clients, coordination avec les partenaires critiques. Circuit d'escalade convenu à l'avance pour les clients sous contrat.

RSSI financier fractionnel

Pour les PSF, fintechs et petits gestionnaires qui ne peuvent pas financer un CISO à temps plein : mise à disposition 3 à 8 jours/mois d'un RSSI spécialisé secteur financier. Pilotage DORA, interface régulateur, gouvernance risque TIC. Coût 40-60% d'un recrutement interne.

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
MOIS 1-2	MOIS 2-5	MOIS 4-9	MOIS 6-15	MOIS 12-24
Diagnostic	**Gouvernance**	**Supply chain**	**Résilience**	**Inspection-ready**
• Audit 5 piliers • Cartographie écarts • Budget board • Sponsor C-level	• Politique TIC • Rôles & RACI • Formation board • KPI pilotage	• Registre complet • Clauses contractuelles • Exit plans cloud • Monitoring	• Programme de tests • TLPT (si éligible) • PCA/PRA prouvés • Exercices cyber	• Audit blanc • Outillage GRC • Dashboard board • 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 DORA & articulations

Chapitre 9

Comment DORA s'articule avec NIS2, les exigences BNB/FSMA et les référentiels ISO/NIST.

Gouvernance et gestion des risques TIC

DORA art. 5-6

Le board approuve la stratégie TIC, revoit régulièrement les risques, assure sa formation. Une politique TIC formelle, une méthodologie d'analyse de risques, des indicateurs clés sont exigés.

BÉNÉFICE CACHÉ :

La montée du sujet au board crée un alignement stratégique fort entre business et IT. Les arbitrages budgétaires deviennent plus informés et plus rapides.

Tests de résilience opérationnelle

DORA art. 24-26

Programme de tests formalisé (revues de vulnérabilités, open source, pentests, scénarios de continuité). TLPT obligatoire tous les 3 ans pour les institutions dépassant les seuils ESA.

BÉNÉFICE CACHÉ :

Le programme de tests structuré fait monter en maturité toute la fonction sécurité. Les incidents réels sont mieux gérés car les équipes s'entraînent régulièrement.

Gestion des risques liés aux tiers

DORA art. 28-30

Registre des prestataires TIC (art. 28), clauses contractuelles obligatoires (art. 30), classification critique/important, évaluation ex-ante, monitoring continu, plans d'exit crédibles.

BÉNÉFICE CACHÉ :

Le registre prestataires bien construit est un outil de pilotage business précieux : négociation tarifaire, réduction des risques de concentration, identification des dépendances cachées.

Gestion et notification des incidents

DORA art. 17-19

Classification des incidents selon les seuils des RTS (clients affectés, durée, perte, portée, services critiques). Notification aux autorités compétentes (BNB/FSMA) selon un calendrier strict.

BÉNÉFICE CACHÉ :

La procédure de gestion d'incident est aussi un outil d'apprentissage organisationnel. Bien menée, elle réduit sensiblement la durée des incidents suivants.

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
☐	Nommer un responsable DORA formel avec lettre de mission (CISO, CRO ou COO).			2 semaines
☐	Faire approuver par le board la politique de gestion des risques TIC.			3 mois
☐	Démarrer le chantier registre des prestataires TIC (art. 28) en priorité.			6 mois
☐	Organiser la formation cyber du board (obligatoire, formalisée).			2 mois
☐	Lancer l'audit des contrats prestataires critiques pour identifier les écarts DORA.			4 mois
☐	Documenter un exit plan crédible pour votre principal prestataire cloud.			9 mois
☐	Formaliser un programme annuel de tests de résilience (scans, pentests, exercices).			6 mois
☐	Aligner votre procédure incidents sur les seuils et calendriers DORA.			4 mois
☐	Si éligible TLPT : engager le cadrage avec TIBER-BE (cycle 12-18 mois).			3 mois
☐	Conduire un table-top de crise impliquant le COMEX et le board.			6 mois
☐	Mettre en place un tableau de bord DORA trimestriel pour le board.			6 mois

© 2026 FlashModz Enterprise — https://flashmodz.be

- [ ] Engager un audit blanc DORA par un tiers indépendant avant inspection régulateur.

EFFORT  IMPACT  DÉLAI **12 mois**

- [ ] Évaluer l'opportunité d'un outillage GRC unifié NIS2/DORA/ISO 27001.

EFFORT  IMPACT  DÉLAI **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.

© 2026 FlashModz Enterprise — https://flashmodz.be

Questions fréquentes

Chapitre 10

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

Q1. Mon entreprise est-elle soumise à DORA ?

Oui si vous êtes : banque, assurance, réassurance, entreprise d'investissement, PSF, gestionnaire d'OPC, établissement de paiement, établissement de monnaie électronique, fonds de pension, prestataire de services sur cryptoactifs, administrateur d'indices de référence, agence de notation de crédit, ou prestataire TIC critique désigné par les ESA. Les seuils de taille activent la proportionnalité mais pas l'exemption.

Q2. Quelle est la différence entre DORA et NIS2 ?

NIS2 est une directive (transposée en droit belge), secteur-agnostique, applicable à 18 secteurs dont la finance. DORA est un règlement (applicable directement), spécifique au secteur financier, plus détaillé et plus contraignant sur la résilience opérationnelle. Pour une banque soumise aux deux, DORA prévaut (lex specialis). En pratique, on implémente les deux dans un cadre unifié.

Q3. Combien coûte une mise en conformité DORA ?

Ordre de grandeur sur 18-24 mois : Petit PSF / fintech (< 50 personnes) : 150-350 K€. PME financière (50-250 personnes) : 400-800 K€. Grand acteur (banque, assurance, > 250 personnes) : 1-3 M€. Ces budgets couvrent l'audit, la gouvernance, la supply chain, les tests, l'outillage GRC, et la formation. Les TLPT viennent en sus : 150 à 600 K€ par campagne.

Q4. Qu'est-ce qu'un TLPT et qui doit en faire ?

TLPT = Threat-Led Penetration Testing (DORA art. 26-27). Test d'intrusion avancé de 4 à 12 semaines basé sur une threat intelligence spécifique à votre institution. Les seuils ESA désignent les institutions éligibles (grandes banques, grandes assurances, certains prestataires critiques). Le cadre TIBER-BE pilote ces tests en Belgique, en coordination avec la BNB. Fréquence minimale : tous les 3 ans.

Q5. Peut-on sous-traiter sa conformité DORA ?

Non, la responsabilité finale reste chez l'entité financière. Vous pouvez sous-traiter certaines fonctions opérationnelles (MSSP, vCISO, audit) mais la gouvernance DORA doit être portée en interne au niveau board et COMEX. Le régulateur veut voir des dirigeants qui maîtrisent le sujet, pas des prestataires qui répondent pour eux.

Q6. Comment DORA traite-t-il les prestataires cloud ?

Les hyperscalers (AWS, Azure, Google Cloud) peuvent être désignés par les ESA comme "Critical Third-Party Providers" et tomber sous supervision directe européenne. Côté client : vous devez (1) avoir un registre précis des services utilisés, (2) évaluer la concentration (part de l'IT sur un seul provider), (3) avoir un exit plan crédible et testé, (4) des clauses contractuelles DORA-compliant.

Q7. Quelle est l'articulation avec la réglementation prudentielle existante ?

DORA s'ajoute aux exigences prudentielles existantes (Bâle III, Solvabilité II, CRR/CRD, MiFID II, etc.). La BNB et la FSMA intègrent DORA dans leur programme de contrôle global. L'approche recommandée : bâtir un framework GRC unifié qui couvre DORA + prudentiel + NIS2 + RGPD, plutôt que d'empiler des systèmes en silos.

© 2026 FlashModz Enterprise — https://flashmodz.be

Q8. Quels sont les premiers indices d'un contrôle DORA ?

La BNB et la FSMA envoient généralement (1) un questionnaire détaillé sur les 5 piliers, (2) une demande de documents ciblés (registre prestataires, politique TIC, rapports tests), (3) si nécessaire, une inspection sur site avec interviews. Délai de réponse typique : 2 à 4 semaines. Anticiper = préparer un dossier type qu'on peut livrer rapidement.

Q9. Que regardent concrètement la BNB et la FSMA en 2026 ?

Les contrôles s'intensifient en 2026 sur des points précis : qualité et exhaustivité du registre des prestataires TIC (art. 28) et de sa transmission, clauses contractuelles de l'art. 30, preuve de l'implication du board (procès-verbaux, formation, art. 5), alignement des procédures d'incident sur les seuils des RTS (art. 17 à 19), réalité des tests de résilience (art. 24 à 26), et crédibilité des exit plans cloud. Le fil conducteur : des preuves opérationnelles, pas des politiques sur papier.

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.

© 2026 FlashModz Enterprise — https://flashmodz.be

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.

© 2026 FlashModz Enterprise — https://flashmodz.be

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.

© 2026 FlashModz Enterprise — https://flashmodz.be

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

© 2026 FlashModz Enterprise — https://flashmodz.be

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

© 2026 FlashModz Enterprise — https://flashmodz.be

FlashModz

Cadrez votre conformité DORA

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