
 GUIDE CONTRE-AUDIT

Votre prestataire IT, vérifié en toute indépendance.

Votre infrastructure est gérée par un prestataire ou par une équipe interne. Ce guide explique ce qu'un contre-audit vérifie, ce que les textes vous permettent d'exiger, et comment mener la démarche sans abîmer la relation avec votre prestataire.

PME et ETI dont l'IT est infogérée ou gérée en interne

17 pages



Jérémy Manet

Fondateur, ingénieur et architecte système et réseau
Une question : 0471 87 87 07, tous les jours dès 9 h



Version en ligne

SYNTHÈSE

Un prestataire gère votre infrastructure, mais c'est votre entreprise qui porte le risque.

1 Déléguer l'exploitation ne délègue pas la responsabilité

La direction reste responsable de la sécurité de l'entreprise. Pour les entités concernées, NIS2 lui demande d'approuver et de superviser les mesures de cybersécurité (art. 20), y compris celles qui touchent aux prestataires (art. 21).

2 Les écarts se cachent entre le contrat et la réalité

Supervision prévue mais jamais configurée, sauvegardes qui tournent sans avoir été restaurées, comptes administrateurs connus d'une seule personne : ces écarts ne se voient qu'en vérifiant sur pièces.

3 Vous avez le droit de vérifier

Le RGPD impose au sous-traitant de permettre les audits (art. 28). Dans le secteur financier, DORA prévoit des droits d'accès, d'inspection et d'audit dans les contrats TIC (art. 30). Votre contrat peut aussi le prévoir.

4 Un contre-audit n'est pas une mise en accusation

Le rapport est factuel et rédigé pour être partagé avec votre prestataire. Il sert d'abord à mieux piloter la relation, pas à la rompre.

5 Quatre angles, un rapport priorisé

Infrastructure et configurations, sécurité et sauvegardes, contrat face à la réalité, documentation et réversibilité. Vous recevez des constats prouvés et un plan de remédiation classé par priorité.

Public : PME et ETI dont l'IT est infogérée ou gérée en interne · Édition octobre 2026

SOMMAIRE

Ce que contient **ce guide**.

01	Le contexte, en chiffres	4
02	Ce qu'un contre-audit met souvent au jour	5
03	Six idées reçues, et ce qu'il en est	6
04	Trois situations typiques en Belgique	7
05	Ce qui change quand la démarche est en place	8
06	Faites le point, en cinq minutes	8
07	Ce que nous vérifions pour vous	9
08	Une feuille de route en quatre phases	10
09	Ce que les textes vous permettent d'exiger	11
10	Vos actions, par ordre de priorité	12
11	Les questions qu'on nous pose souvent	13
12	Les termes techniques, expliqués simplement	14
13	Pour aller plus loin	15
14	À propos de FlashModz	15

— 01 · CONTEXTE

Le contexte, en chiffres.

Art. 28

du RGPD : votre sous-traitant doit permettre les audits, y compris les inspections, menés par vous ou par un auditeur mandaté

Art. 21

de NIS2 : la sécurité de la chaîne d'approvisionnement fait partie des mesures obligatoires

Art. 30

de DORA : droits d'accès, d'inspection et d'audit dans les contrats TIC des fonctions critiques

45 min

de Check-up Infra & OPS, offert, pour cadrer le périmètre du contre-audit

Sources : textes officiels et publications citées dans ce guide. Les durées de projet sont des estimations pour un cas type.

Dans beaucoup de PME, l'informatique est confiée à un prestataire ou à une petite équipe interne. Tant que tout fonctionne, personne ne regarde de près. Le jour d'une panne, d'un rançongiciel ou d'un changement de prestataire, on découvre ce qui n'était pas en place.

Un contre-audit est une vérification indépendante de cette infrastructure. Il ne refait pas le travail du prestataire : il contrôle, preuves à l'appui, que ce qui est prévu existe vraiment. Les sauvegardes se restaurent-elles ? Les accès sont-ils maîtrisés ? Le contrat est-il respecté ? Pourriez-vous changer de prestataire sans tout perdre ?

C'est aussi une question de gouvernance. NIS2 attend de la direction qu'elle supervise les risques liés aux prestataires, et le RGPD vous donne le droit d'auditer ceux qui traitent des données pour vous. Un contrôle documenté montre que vous exercez cette responsabilité.

Ce guide présente ce que nous vérifions, les écarts que nous rencontrons le plus souvent et une méthode pour mener la démarche dans un bon climat avec votre prestataire.



« La plupart des prestataires font du bon travail. Le contre-audit sert à le montrer, et à repérer ce qui manque avant qu'une panne ne le révèle. »

Jérémy Manet, FlashModz

02 · RISQUES

Ce qu'un contre-audit met souvent au jour.

Des écarts fréquents, rarement visibles tant qu'aucun incident ne survient.

01 Des sauvegardes jamais restaurées

Les sauvegardes affichent « réussi » chaque nuit, mais personne n'a tenté de restauration complète. Le jour où il faut repartir, on découvre des fichiers manquants, une base de données inutilisable ou un délai de reprise bien plus long que prévu.

02 Des accès administrateurs mal maîtrisés

Comptes à privilèges partagés, anciens techniciens toujours actifs, mot de passe administrateur connu du seul prestataire. L'entreprise ne contrôle plus qui peut tout faire sur son propre système.

03 Une supervision prévue mais absente

Le contrat parle de surveillance et d'alertes, mais aucune sonde n'est configurée sur les serveurs critiques, ou les alertes arrivent dans une boîte que personne ne lit.

04 Des mises à jour en retard

Correctifs de sécurité appliqués avec des mois de retard, systèmes en fin de support toujours en production, pare-feu jamais mis à jour. Ce sont les failles que les attaquants exploitent en premier.

05 Une documentation inexistante

Schéma réseau absent, mots de passe dans un fichier non protégé, procédures dans la tête d'une seule personne. Sans documentation, chaque incident dure plus longtemps et la dépendance au prestataire augmente.

06 Une réversibilité impossible

Licences au nom du prestataire, nom de domaine enregistré par lui, configurations impossibles à exporter. Changer de prestataire devient un projet risqué, ce qui affaiblit votre position dans la relation.

— 03 · IDÉES REÇUES

Six idées reçues, et ce qu'il en est.

CE QU'ON ENTEND	CE QU'IL EN EST
« Notre prestataire est certifié, tout est donc en ordre »	Une certification porte sur des compétences ou sur une organisation, pas sur l'état de votre infrastructure à vous. Le contre-audit regarde vos serveurs, vos sauvegardes et vos accès. Repère : Une certification n'est pas un contrôle de votre parc
« Un audit va abîmer la relation avec notre prestataire »	Le rapport est factuel et pensé pour être partagé. Les prestataires sérieux y trouvent une base de travail claire et des priorités validées par le client. Repère : Rapport partageable avec le prestataire
« S'il y avait un problème, il nous l'aurait dit »	Un prestataire ne voit pas toujours ce qui sort de son contrat, et il lui est difficile de signaler ce qu'il n'a pas fait. Un regard extérieur n'a pas cette difficulté. Repère : Un regard sans conflit d'intérêts
« Nous n'avons pas le droit de regarder, c'est leur système »	C'est votre infrastructure et ce sont vos données. Le RGPD impose au sous-traitant de permettre les audits, et beaucoup de contrats prévoient un droit de contrôle. L'audit se fait avec des accès en lecture, sans rien modifier. Repère : RGPD, article 28
« Un contre-audit, c'est un chantier de plusieurs mois »	Le périmètre est cadré au départ et le forfait est borné en durée et en budget. On peut commencer par les points les plus sensibles, comme les sauvegardes et les accès. Repère : Forfait borné, devis écrit sous 48 h
« Si le rapport est mauvais, il faudra changer de prestataire »	La plupart du temps, le rapport sert à corriger avec le prestataire en place. Le changement reste une option, et le volet réversibilité vous dit s'il est réaliste. Repère : Mieux piloter, pas forcément remplacer

— 04 · CAS CONCRETS

Trois situations typiques en Belgique.

Des scénarios construits à partir de situations courantes. Les noms et les chiffres sont illustratifs.

Distributeur en Hainaut : des sauvegardes qui ne se restaurent pas

CONTEXTE	PME de distribution, informatique confiée au même prestataire depuis plusieurs années. Un rapport mensuel indique « sauvegardes OK ».
CE QUI S'EST PASSÉ	Pendant le contre-audit, le test de restauration de la base de gestion commerciale échoue : la sauvegarde copiait les fichiers, pas la base active. Le prestataire a corrigé la configuration et ajouté un test de restauration trimestriel.
À RETENIR	Une sauvegarde n'existe que si elle a été restaurée. Le test se fait devant vous, sur des données réelles.

Cabinet comptable à Namur : un seul compte administrateur

CONTEXTE	Une douzaine de collaborateurs, serveur de fichiers et logiciel comptable gérés à distance par un technicien indépendant.
CE QUI S'EST PASSÉ	Tous les accès reposent sur un compte administrateur unique, utilisé aussi pour la maintenance, et l'accès à distance n'a pas de double authentification. Le cabinet ne détenait aucun des mots de passe.
À RETENIR	Les accès à privilèges doivent être nominatifs et protégés par MFA, et l'entreprise garde la maîtrise des comptes de secours.

PME industrielle en Brabant wallon : un contrat plus large que la réalité

CONTEXTE	Contrat d'infogérance avec supervision, mises à jour mensuelles et rapport trimestriel.
CE QUI S'EST PASSÉ	Aucune sonde de supervision n'était active sur deux serveurs de production, et les mises à jour avaient plusieurs mois de retard. Le rapport, partagé avec le prestataire, a servi à redéfinir les engagements et à fixer des indicateurs suivis en comité.
À RETENIR	Un contrat ne protège que s'il est vérifié. Quelques indicateurs simples, revus régulièrement, évitent que l'écart se creuse.

— 05 · AVANT ET APRÈS

Ce qui change quand la démarche est en place.

SITUATION	SANS CONTRE-AUDIT	APRÈS UN CONTRE-AUDIT
Sauvegardes	Rapports « OK » sans test de restauration.	Restauration testée devant vous, délai de reprise connu.
Accès administrateurs	Comptes partagés, anciens accès encore actifs.	Comptes nominatifs, MFA, liste des accès tenue à jour.
Contrat	Engagements jamais vérifiés.	Écarts identifiés, indicateurs suivis avec le prestataire.
Documentation	Savoir concentré chez le prestataire.	Schémas et procédures remis à l'entreprise.
Réversibilité	Changer de prestataire paraît impossible.	Licences, domaine et configurations au nom de l'entreprise.
Direction	Risque lié au prestataire non suivi.	Contrôle documenté, utile face à NIS2 et aux assureurs.

— 06 · AUTO-ÉVALUATION

Faites le point, en cinq minutes.

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

— VOTRE SCORE

Comptez 0 point par « non », 1 par « partiel » et 2 par « oui ». Sous 40 % du total, les bases sont à poser. De 40 à 70 %, la posture est à renforcer. Au-delà de 70 %, elle est bonne.

SITUATION	NON	PARTIEL	OUI
1. Une restauration complète a été testée au cours des douze derniers mois.	☐	☐	☐
2. Vous connaissez le délai réel pour redémarrer vos systèmes critiques.	☐	☐	☐
3. Les comptes administrateurs sont nominatifs et protégés par une double authentification.	☐	☐	☐

SITUATION	NON	PARTIEL	OUI
4. L'entreprise détient les mots de passe des comptes de secours.	☐	☐	☐
5. Les accès des anciens collaborateurs et techniciens sont supprimés dès leur départ.	☐	☐	☐
6. Les correctifs de sécurité sont appliqués dans un délai défini et vérifiable.	☐	☐	☐
7. La supervision alerte une personne qui agit, dans des délais connus.	☐	☐	☐
8. Un schéma réseau et un inventaire à jour vous ont été remis.	☐	☐	☐
9. Les licences, le nom de domaine et les comptes cloud sont au nom de l'entreprise.	☐	☐	☐
10. Le contrat précise les engagements de service et vous les vérifiez.	☐	☐	☐
11. Le contrat prévoit un droit d'audit et une clause de réversibilité.	☐	☐	☐
12. La direction revoit au moins une fois par an les risques liés au prestataire.	☐	☐	☐

— 07 · ACCOMPAGNEMENT

Ce que nous vérifions **pour vous.**

Quatre angles, un rapport factuel et un plan de remédiation priorisé. Forfait selon périmètre, sur devis écrit sous 48 h.

Infrastructure et configurations

Serveurs, réseau, Wi-Fi, virtualisation : nous comparons les configurations réelles aux bonnes pratiques et aux recommandations des éditeurs.

Sécurité et sauvegardes

Durcissement, accès, segmentation, et un test de restauration réel sur un périmètre choisi avec vous.

Contrat face à la réalité

Nous confrontons votre contrat de services (engagements, périmètre, livrables) à ce qui est réellement en place, point par point.

Documentation et réversibilité

Nous vérifions que votre informatique est documentée et que vous pourriez changer de prestataire sans perdre l'accès à vos systèmes, vos licences ou vos données.

Restitution à la direction

Une synthèse lisible pour la direction et un volet technique détaillé pour le prestataire. Le rapport et sa méthodologie restent votre propriété.

Contre-vérification

Sur demande, nous revérifions les points corrigés une fois la remédiation faite, pour confirmer que les écarts sont bien refermés.

Notre façon de travailler.

1

AUDIT

Voir clair

Nous partons de votre existant : inventaire, entretiens avec les équipes, risques réels. Le diagnostic se fait sur vos systèmes, pas sur des hypothèses.

2

PLAN

Prioriser ensemble

Nous classons les actions par impact, effort et budget, et nous construisons le plan avec vous. Les décisions restent les vôtres.

3

ACTION

Stabiliser

Nous corrigeons et durcissons par étapes courtes. Vous validez chaque étape avant la suivante, dans le budget du devis.

4

AUTONOMIE

Transmettre

Nous documentons ce qui a été fait et formons vos équipes, pour que vous puissiez continuer sans dépendre de nous.

— 08 · FEUILLE DE ROUTE

Une feuille de route en quatre phases.

Chaque phase produit un livrable utilisable seul. Vous pouvez marquer une pause entre deux phases, selon votre budget et votre charge interne.

1

AVANT LA MISSION

Cadrage

Périmètre et objectifs
Accès en lecture
Information du prestataire

2

SUR PIÈCES

Collecte

Contrat et engagements
Documentation existante
Inventaire

3

SUR SITE OU À DISTANCE

Vérifications

Configurations
Test de restauration
Revue des accès

4

FIN DE MISSION

Rapport

Constats et preuves
Plan priorisé
Restitution

09 · CADRE RÉGLEMENTAIRE

Ce que les textes vous permettent d'exiger.

Le droit de vérifier un prestataire existe déjà dans plusieurs textes. Encore faut-il l'exercer.

RGPD art. 28

Le droit d'auditer vos sous-traitants

Quand votre prestataire traite des données personnelles pour vous, il est sous-traitant au sens du RGPD. Il doit mettre à votre disposition les informations nécessaires et permettre les audits, y compris les inspections, menés par vous ou par un auditeur que vous mandatez.

Ce que vous y gagnez : Le contre-audit exerce ce droit de façon cadrée, et vérifie au passage que le contrat de sous-traitance existe et couvre les bons traitements.

NIS2 art. 20 et 21

La supervision des prestataires par la direction

Pour les entités concernées, la sécurité de la chaîne d'approvisionnement fait partie des mesures obligatoires (art. 21), et la direction doit approuver et superviser ces mesures (art. 20).

Ce que vous y gagnez : Un contrôle indépendant et documenté montre que la direction suit réellement le risque lié à ses prestataires.

DORA art. 28 et 30

Les prestataires TIC du secteur financier

Les entités financières doivent gérer le risque lié à leurs prestataires TIC. Pour les fonctions critiques ou importantes, les contrats prévoient des droits d'accès, d'inspection et d'audit, ainsi qu'une stratégie de sortie.

Ce que vous y gagnez : Le contre-audit apporte une vérification indépendante et met à l'épreuve la stratégie de sortie, deux points attendus par le règlement.

Contrat

Les clauses à vérifier dans votre contrat

Engagements de service mesurables, droit d'audit, propriété des licences et des données, remise de la documentation et assistance à la réversibilité en fin de contrat.

Ce que vous y gagnez : Vérifiées puis appliquées, ces clauses renforcent votre position sans créer de conflit avec le prestataire.

— 10 · PLAN D'ACTION

Vos actions, par ordre de priorité.

À imprimer et à cocher au fil de l'eau. Commencez par les actions à fort impact et faible effort.

ACTION	EFFORT	IMPACT	DÉLAI
☐ Demander à votre prestataire un test de restauration complet, réalisé devant vous.	● ● ● ● ●	● ● ● ● ●	Ce mois-ci
☐ Récupérer les mots de passe des comptes de secours et les conserver hors du système.	● ● ● ● ●	● ● ● ● ●	Cette semaine
☐ Faire la liste des comptes administrateurs et supprimer ceux qui ne servent plus.	● ● ● ● ●	● ● ● ● ●	1 mois
☐ Activer la double authentification sur les accès à distance et les comptes administrateurs.	● ● ● ● ●	● ● ● ● ●	1 mois
☐ Vérifier que les licences, le nom de domaine et les comptes cloud sont au nom de l'entreprise.	● ● ● ● ●	● ● ● ● ●	1 mois
☐ Relire le contrat : engagements de service, droit d'audit, réversibilité, remise de la documentation.	● ● ● ● ●	● ● ● ● ●	1 mois
☐ Obtenir un schéma réseau et un inventaire à jour.	● ● ● ● ●	● ● ● ● ●	2 mois
☐ Demander un rapport régulier sur l'application des correctifs de sécurité.	● ● ● ● ●	● ● ● ● ●	2 mois
☐ Fixer trois ou quatre indicateurs suivis en comité avec le prestataire.	● ● ● ● ●	● ● ● ● ●	3 mois
☐ Planifier un contre-audit sur le périmètre le plus sensible.	● ● ● ● ●	● ● ● ● ●	3 mois

11 · QUESTIONS

Les questions qu'on nous pose souvent.

Dois-je changer de prestataire après un contre-audit ?

Non, et ce n'est pas l'objectif. Le contre-audit est un livrable autonome : un état des lieux factuel et un plan de remédiation priorisé. La plupart du temps, il sert à mieux piloter la relation avec votre prestataire actuel, pas à le remplacer.

Mon prestataire doit-il être informé ?

C'est votre choix, mais nous le conseillons : il peut fournir les accès en lecture nécessaires, et le rapport est rédigé pour être partagé avec lui comme base de travail.

De quels accès avez-vous besoin ?

D'accès en lecture aux consoles et aux équipements concernés, du contrat et de la documentation existante. Nous ne modifions rien pendant la mission. Le test de restauration se fait sur un périmètre convenu à l'avance.

Combien de temps dure un contre-audit ?

Cela dépend du périmètre : nombre de sites, de serveurs et de services concernés. Le Check-up Infra & OPS de 45 minutes, offert, sert à le cadrer. Vous recevez ensuite un devis écrit sous 48 h, avec un forfait borné en durée et en budget.

Qu'est-ce qui garantit votre indépendance ?

Nous ne vendons ni licences, ni matériel, et nous ne touchons aucune commission d'éditeur. Le rapport ne débouche jamais sur un devis de produits. Vous recevez des recommandations argumentées et vous les faites appliquer par l'équipe de votre choix, votre prestataire actuel compris.

Est-ce utile pour NIS2 ou DORA ?

Oui. Ces cadres attendent des dirigeants qu'ils supervisent leurs risques informatiques, y compris ceux liés aux prestataires. Pour DORA, la gestion du risque lié aux prestataires TIC est une exigence explicite. Un contrôle indépendant documenté en fait partie.

Que contient le rapport ?

Une synthèse pour la direction, les constats avec leurs preuves, un niveau de priorité pour chacun et un plan de remédiation. Un volet technique détaillé s'adresse au prestataire. Le rapport et sa méthodologie restent votre propriété.

Les termes techniques, expliqués simplement.

Infogérance

Gestion de tout ou partie de l'informatique d'une entreprise par un prestataire externe, dans le cadre d'un contrat de services.

Contre-audit

Vérification indépendante d'une infrastructure gérée par un prestataire ou une équipe interne : configurations, sauvegardes, sécurité, respect du contrat, documentation et réversibilité.

Réversibilité

Capacité à reprendre son informatique ou à la confier à un autre prestataire sans perdre l'accès aux systèmes, aux données, aux licences ni à la documentation.

Compte à privilèges

Compte qui peut modifier la configuration d'un système ou accéder à toutes ses données, comme un compte administrateur. Il doit être nominatif et protégé par MFA.

MFA

Multi-Factor Authentication : authentification à plusieurs facteurs, par exemple un mot de passe et une application mobile ou une clé physique.

Restauration

Remise en service de données ou d'un système à partir d'une sauvegarde. Seul un test de restauration prouve qu'une sauvegarde est utilisable.

Supervision

Surveillance continue des serveurs, du réseau et des services, avec des alertes envoyées à une personne chargée d'agir.

Correctif de sécurité

Mise à jour publiée par un éditeur pour corriger une faille. Plus il est appliqué tard, plus la faille reste exploitable.

Sous-traitant (RGPD)

Prestataire qui traite des données personnelles pour le compte de votre entreprise. Le RGPD encadre ce rôle par un contrat et lui impose de permettre les audits (art. 28).

NIS2

Directive européenne sur la cybersécurité, transposée en Belgique par la loi du 26 avril 2024, en vigueur depuis le 18 octobre 2024. Elle couvre aussi la sécurité de la chaîne d'approvisionnement.

DORA

Digital Operational Resilience Act. Règlement (UE) 2022/2554, applicable depuis le 17 janvier 2025 au secteur financier, qui encadre notamment le recours aux prestataires TIC.

RGPD

Règlement général sur la protection des données : règlement européen qui encadre tout traitement de données personnelles. Contrôlé en Belgique par l'APD.

Plan de remédiation

Liste des corrections à apporter après un audit, classées par priorité, avec un responsable et un délai pour chacune.

13 · RESSOURCES

Pour aller plus loin.

Sites officiels et ressources gratuites.

CCB (Centre pour la Cybersécurité Belgique)

Autorité belge de cybersécurité. Recommandations publiques, référentiel CyberFundamentals et informations sur NIS2.

ccb.belgium.be

APD (Autorité de Protection des Données)

Le régulateur belge du RGPD. Informations sur les contrats de sous-traitance et les obligations des sous-traitants.

autoriteprotectiondonnees.be

ENISA (European Union Agency for Cybersecurity)

Agence européenne de la cybersécurité. Publications gratuites sur NIS2 et la sécurité de la chaîne d'approvisionnement.

enisa.europa.eu

Safeonweb@Work

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

atwork.safeonweb.be

14 · À PROPOS

À propos de FlashModz.

FlashModz est un cabinet d'expertise IT indépendant, fondé par Jérémy Manet et basé à Farciennes. Nous auditions, sécurisons et supervisons l'infrastructure des entreprises, en Belgique et à l'international, et nous accompagnons les particuliers dans toute la Wallonie.

Nous ne revendons ni licences ni matériel : nos recommandations restent neutres. Chaque mission démarre sur un devis écrit sous 48 h.



Jérémy Manet

Fondateur, ingénieur et architecte système et réseau

Plus de quinze ans en architecture et ingénierie d'infrastructures : réseau et Wi-Fi d'entreprise, sécurité, virtualisation. Il pilote aussi la gouvernance IT en tant que Process Owner COBIT, DORA et NIS2, notamment dans le secteur bancaire.

— CERTIFICATIONS

CWNA-107 (CommScope, 2021) · RWF 100 (CommScope, 2021) · RAA 200 (CommScope, 2021) · RSP 100 (CommScope, 2021) · CLD 200 (CommScope, 2021) · CMNA (Cisco Meraki, 2019) · Small Business Technical Overview (Cisco, 2022) · NSE 2 (Fortinet, 2021) · NSE 1 (Fortinet, 2021) · PKI Security (ING, 2018) · Veeam VMSP (Veeam Software, 2021) · Veeam VMTSP (Veeam Software, 2021) · Jamf Certified Tech (Jamf, 2019) · Jamf Certified Associate (Jamf, 2019) · Apple Certified Support Essentials 10.13 (Apple, 2019)

— PARLONS-EN

Qui vérifie votre IT ? Un appel suffit pour y voir clair.

Nous commençons par le Check-up Infra & OPS, offert : 45 minutes pour cadrer le périmètre du contre-audit. Vous recevez ensuite un devis écrit sous 48 h, avec un forfait borné en durée et en budget.



Jérémy Manet répond directement

● Tous les jours dès 9 h

0471 87 87 07

Appeler maintenant

Check-up Infra & OPS offert : 45 minutes, à distance ou sur place, sans engagement.

[Être rappelé ou écrire un message](#) · contact@flashmodz.be

ENTREPRISES

Toute la Belgique, sur site ou à distance

DEVIS

Écrit sous 48 h, sans engagement

ADRESSE

Rue du Wainage 18, 6240 Farciennes