FLASHMODZ ENTERPRISE

Cabinet d’expertise IT — Charleroi · Belgique & international

FlashModz

COBIT — Gouvernance IT pragmatique pour PME

Guide COBIT / Gouvernance

COBIT 2019 démythifié pour les structures qui ne sont pas des grands comptes. Comment cadrer la gouvernance IT, aligner business et IT, mesurer la performance, sans transformer l'exercice en usine à gaz.

Scannez pour acceder
a la version en ligne

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

https://flashmodz.be

SYNTHÈSE EXÉCUTIVE

L'essentiel en 5 minutes

Sans gouvernance IT, votre PME finance de la technologie sans la maîtriser. COBIT 2019 vous donne le cadre, sans l'usine à gaz.

1

COBIT n'est pas réservé aux grands comptes

Le Design Guide COBIT 2019 recommande explicitement de choisir 3 à 15 objectifs selon 11 facteurs de conception, pas les 40. Pour une PME, 6-8 objectifs bien choisis couvrent l'essentiel de la valeur. La documentation se dimensionne avec la structure : 1 page suffit pour une PME là où un grand compte en demande 15.

2

L'absence de gouvernance coûte cher (mais invisiblement)

Les PME sans gouvernance IT paient un triple prix : des projets qui dépassent budgets et délais, des incidents récurrents sans apprentissage, un shadow IT qui prolifère hors de tout contrôle. S'y ajoute la difficulté à recruter de bons profils IT. Le coût total dépasse souvent l'investissement gouvernance, mais il est diffus, donc invisible.

3

COBIT rend les arbitrages explicites et légitimes

Dans une PME avec COBIT, chacun sait qui décide de quoi, avec quelles informations, selon quels critères. Les décisions deviennent traçables, légitimes, révisables. Fini les frustrations du type "Je ne sais pas pourquoi ce projet est prioritaire". Le climat d'entreprise en bénéficie autant que la performance.

4

COBIT est le chapeau qui fédère NIS2, ISO 27001, ITIL, CIS

Contrairement à ce qu'on pourrait croire, COBIT ne s'ajoute pas aux autres référentiels : il les organise. Implémenter COBIT allégé rend NIS2 plus simple, la certification ISO 27001 plus rapide, l'adoption d'ITIL plus cohérente. Un effort, plusieurs conformités.

5

Un projet COBIT light se boucle en 4-6 mois pour 25-60 K€

Contrairement aux projets lourds des cabinets internationaux (300-800 K€, 18 mois), un COBIT light pour PME se cadre en 6 mois avec un budget 25-60 K€. La clé est la sélectivité : 6-8 objectifs, pas 40. Et un accompagnement opérationnel, pas du consulting slideware.

Et maintenant ?

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

Document conçu pour PME & ETI — Gouvernance IT · Lecture : ~15-20 min · Édition 2026

Table des matières

Naviguez rapidement vers les sections qui vous concernent.

Le marché belge en chiffres

Chapitre 1

40

objectifs de gouvernance et management COBIT 2019 (5 gouvernance + 35 management)

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

11

facteurs de conception du COBIT Design Guide pour tailler le framework à votre contexte

4-6 mois

durée typique d'une mise en place COBIT allégée pour une PME de 100 personnes

6-8

objectifs COBIT bien choisis suffisent à couvrir l'essentiel de la valeur pour une PME

Contexte & enjeux

Soyons directs : dans la plupart des PME belges, il n'y a pas vraiment de gouvernance IT. Le DSI court après les incidents, les projets dérivent, les budgets explosent, les priorités changent chaque semaine. Personne n'est satisfait : ni la direction, ni les métiers, ni l'équipe IT.

COBIT 2019 (Control Objectives for Information and Related Technologies), publié par l'ISACA, répond à ce chaos. Il propose 40 objectifs : 5 objectifs de gouvernance dans le domaine EDM (Evaluate, Direct and Monitor), porté par le conseil et la direction, et 35 objectifs de management répartis en quatre domaines : APO (Align, Plan and Organize : stratégie, budget, risques, RH IT), BAI (Build, Acquire and Implement : projets et changements), DSS (Deliver, Service and Support : exploitation, incidents, continuité) et MEA (Monitor, Evaluate and Assess : performance et conformité). Chaque objectif a des pratiques, des métriques, et des niveaux de maturité de 1 à 5.

Le problème : COBIT est souvent présenté comme un monstre réservé aux grands comptes. Un document de 400 pages, des dizaines de matrices, une vingtaine de rôles différents. Pour une PME de 80 personnes, ça semble inapplicable.

La réalité : COBIT se customise. Le "COBIT Design Guide" officiel recommande de choisir 3 à 15 objectifs prioritaires selon 11 facteurs de conception (taille, criticité de l'IT, modèle de sourcing, culture...), pas les 40. Pour une PME belge typique, 6 à 8 objectifs couvrent l'essentiel de la valeur : APO01 (cadre de management IT), APO04 (innovation), APO07 (RH IT), BAI03 (gestion des solutions), DSS02 (incidents et demandes), DSS04 (continuité), MEA01 (performance), MEA03 (conformité externe).

Bien mené, un projet "COBIT light" sur 4-6 mois transforme le pilotage IT d'une PME. Les arbitrages

> *"COBIT, c'est remettre de la discipline dans la gouvernance IT sans y perdre son agilité. Pour une PME, c'est la différence entre subir l'IT et la piloter."*
>
> — Jérémy Manet, FlashModz Enterprise

Les symptômes d'une gouvernance IT absente

Chapitre 2

Pas besoin d'être grand compte pour avoir besoin de gouvernance. Ces symptômes, vous les avez peut-être.

Vos projets IT dépassent les budgets et les délais

Sans cadre de gouvernance, les projets IT glissent : budgets dépassés, délais qui s'étirent, et souvent un périmètre raboté en bout de course. Le COMEX perd confiance, le DSI est perçu comme non fiable, et les métiers commencent à faire du shadow IT. La racine du problème est rarement technique : c'est un déficit de pilotage, celui que les domaines APO et BAI de COBIT viennent structurer.

Les arbitrages IT sont opaques ou arbitraires

Pourquoi ce projet est-il prioritaire ? Qui a décidé du budget cyber ? Pourquoi cet outil et pas un autre ? Sans gouvernance, ces questions restent sans réponse claire. Les décisions paraissent arbitraires, ce qui génère de la frustration et mine la crédibilité du DSI. COBIT rend les décisions traçables et légitimes.

Le board ne comprend pas les enjeux IT

Les PME où le COMEX ou le conseil n'ont aucune visibilité sur l'IT sont nombreuses. Pas de KPI, pas de tableau de bord, pas de reporting structuré. Résultat : l'IT est perçu comme un centre de coût opaque, pas comme un levier stratégique. Une gouvernance COBIT (même allégée) donne au board les outils pour arbitrer et soutenir.

Les incidents se répètent sans apprentissage

Sans processus formalisé de gestion des incidents (DSS02) et de retour d'expérience (MEA01), les mêmes problèmes reviennent. Même crash Exchange qu'il y a 6 mois, même ransomware évité de justesse, mêmes erreurs de déploiement. La gouvernance COBIT force la capitalisation sur les incidents.

La conformité (NIS2, RGPD, ISO) est gérée en panique

Chaque audit est une course : on rassemble les preuves dans l'urgence, on découvre des écarts à corriger en quelques semaines, on stresse les équipes. Un cadre de gouvernance COBIT (MEA03) organise la conformité en continu : les preuves sont produites au fil de l'eau, les écarts sont identifiés en amont, les audits deviennent des exercices formels, pas des crises.

L'équipe IT est surchargée mais peu valorisée

Sans gouvernance, l'équipe IT est la variable d'ajustement de tous les projets métier, mais personne ne mesure sa productivité ni sa valeur. Résultat : burn-out, turnover, difficulté à recruter. Un cadre COBIT (APO07 RH IT) professionnalise la fonction IT et rend visible sa contribution à la performance business.

Le shadow IT explose et personne ne le voit

Quand les métiers perdent confiance en l'IT, ils s'équipent seuls : SaaS non référencés, Dropbox personnels, Excel qui tournent le business. Une part significative du budget IT réel échappe à tout suivi dans les PME sans gouvernance. Risque cyber, perte de données, et désormais shadow AI. COBIT remet de la cohérence sans basculer dans l'autoritarisme.

Mythes vs Réalité

Chapitre 3

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

01

ON ENTEND SOUVENT

COBIT c'est un monstre de 400 pages, ça ne peut pas s'appliquer à une PME.

EN RÉALITÉ — *COBIT Design Guide ISACA*

Le Design Guide COBIT 2019 recommande une sélection customisée de 3 à 15 objectifs selon 11 facteurs de conception. Pour une PME de 100 personnes, 6-8 objectifs bien choisis couvrent l'essentiel de la valeur. COBIT est un buffet, pas un menu imposé. On choisit ce qui nous nourrit.

02

ON ENTEND SOUVENT

On est une PME de 80 personnes, la gouvernance IT c'est du luxe corporate.

EN RÉALITÉ — *Coûts diffus = coûts invisibles*

Une PME de 80 personnes fait tourner l'essentiel de son chiffre d'affaires sur son IT. Projets qui dérapent, incidents récurrents, shadow IT hors de contrôle : ces coûts sont massifs mais diffus, donc invisibles au COMEX. La gouvernance n'est pas du luxe, c'est du pilotage.

03

ON ENTEND SOUVENT

On utilise déjà ITIL, ajouter COBIT c'est doublonner.

EN RÉALITÉ — *COBIT ≠ ITIL (complémentaires)*

COBIT et ITIL sont complémentaires, pas concurrents. COBIT couvre la gouvernance IT globale (pourquoi, qui décide, quels KPI). ITIL couvre l'exécution opérationnelle (gestion des incidents, changements, services). Pour une PME, on utilise COBIT comme chapeau et ITIL pour les processus opérationnels IT.

04

ON ENTEND SOUVENT

On est une scale-up agile, COBIT va nous bureaucratiser.

EN RÉALITÉ

~15-20 pages utiles, pas 400

COBIT bien implémenté DANS une PME = moins de documentation qu'une startup mal organisée (fichiers Excel partout, knowledge dans les têtes, décisions orales). La documentation COBIT utile pour une PME tient sur 15-20 pages : politique IT, RACI, méthodologie projet, processus incidents, tableau de bord. Pas plus.

05

ON ENTEND SOUVENT

On a un prestataire IT, la gouvernance c'est son problème.

EN RÉALITÉ

Gouvernance "` exécution

Même avec un prestataire IT, VOUS décidez : budget, priorités, projets, risques, conformité. Le prestataire exécute. La gouvernance est la responsabilité du donneur d'ordre, pas du fournisseur. COBIT clarifie exactement cette frontière, et protège votre prestataire autant que vous.

06

ON ENTEND SOUVENT

Un projet COBIT c'est au minimum 200 000 €, on ne peut pas.

EN RÉALITÉ

COBIT light PME : 25-60 k€

Pour une PME de 80-150 personnes, un COBIT light bien cadré coûte 25-60 K€ sur 4-6 mois. Le ROI se mesure en 12-18 mois : réduction des dépassements projets, moins d'incidents, meilleur recrutement IT, facilitation conformité. Les gros budgets sont pour les grands cabinets, pas pour COBIT lui-même.

Cas concrets en Belgique

Chapitre 4

Trois scénarios types, inspirés de situations réelles et anonymisés.

PME industrielle wallonne (130 employés)

Contexte: Équipementier mécanique, IT externalisé chez un prestataire local + une équipe IT interne de 3 personnes. Pas de DSI formel. Direction générale frustrée par les dépassements budgétaires IT récurrents.

Impact: Projet COBIT light sur 5 mois. Sélection de 7 objectifs prioritaires (dont APO01, DSS02, MEA01). Mise en place d'un comité de pilotage IT mensuel, d'un tableau de bord à 8 KPI, d'une RACI claire avec le prestataire. Résultat 12 mois plus tard : nettement moins de dépassements projets, des métiers réconciliés avec l'IT, un budget maîtrisé.

Leçon: Une PME de 130 personnes peut implémenter COBIT sans usine à gaz. L'essentiel n'est pas la documentation mais la discipline de pilotage. 7 objectifs bien gérés valent mieux que 40 survolés.

Groupe familial retail à Namur (250 employés, 12 magasins)

Contexte: Secteur distribution, IT centralisé au siège avec 5 personnes. Héritage de 20 ans, dette technique importante. Le fils du fondateur, nouveau DG, veut professionnaliser le pilotage.

Impact: Refonte de la gouvernance IT autour de 6 objectifs COBIT clés. Mise en place d'un PMO IT allégé, d'un board IT trimestriel avec le COMEX, d'une méthodologie projet claire. Après 18 mois : le projet de renouvellement de la caisse s'est passé en 4 mois sans dépassement, contre 12 mois pour le projet équivalent 3 ans avant.

Leçon: La gouvernance IT est un puissant levier d'amélioration de la performance globale. Ce n'est pas qu'un sujet IT : c'est un sujet de direction générale qui impacte toute l'organisation.

PME tech bruxelloise (75 employés, SaaS B2B)

Contexte: Scale-up en forte croissance, culture "move fast". Pas de gouvernance IT formelle, équipe produit/tech fusionnée. Investisseurs qui commencent à poser des questions sur la maturité opérationnelle.

Impact: Due diligence d'un fonds prospect révèle des écarts importants : pas de gestion des risques, pas de PCA, pas de procédures incidents, pas de traçabilité des décisions IT. Opportunité de levée ralentie de 6 mois. Projet de "gouvernance minimale" lancé pour combler en 3 mois.

Leçon: La gouvernance IT devient un critère d'investissement. Les fonds regardent désormais la maturité opérationnelle, pas seulement la tech et le produit. Anticiper, c'est préserver la valorisation.

Avant / Après — la différence concrète

Chapitre 5

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

PME sans gouvernance IT	PME avec COBIT light
01 ARBITRAGES IT AU COMEX	
Discussions répétitives, décisions reportées, priorités qui changent chaque réunion.	Comité IT mensuel structuré, décisions traçables, priorités stables et connues de tous.
02 DÉPASSEMENTS PROJETS	
Budgets et délais régulièrement dépassés, périmètre raboté. Frustration généralisée.	Dépassements rares et maîtrisés, visibilité claire dès le cadrage, ajustements documentés.
03 REPORTING IT AU BOARD	
Quand le DG pose la question, pas de réponse factuelle. Perçu comme opaque.	Tableau de bord mensuel à 8 KPI, rapport trimestriel au COMEX, visibilité complète.
04 GESTION DES INCIDENTS	
Incidents récurrents sans apprentissage. Même problème revient 3× par an.	Base de connaissance capitalisée, processus RCA systématique, courbe d'apprentissage visible.
05 RÔLES ET DÉCISIONS	
Flou entre DSI, métiers, COMEX, prestataires. Conflits récurrents.	RACI claire, rôles définis, conflits résolus par le processus, pas par l'ego.
06 CONFORMITÉ (NIS2, ISO, RGPD)	
Chaque audit est une crise. Mobilisation 3-4 semaines dans l'urgence.	Preuves produites au fil de l'eau. Audits = vérifications, pas recherche frénétique.

07 ATTRACTIVITÉ DES TALENTS IT

- Difficulté à recruter, turnover élevé. "On n'a pas de structure".
- Fonction IT professionnalisée, perspectives claires. Rétention améliorée, recrutement facilité.

08 SHADOW IT

- Une part significative du budget IT réel est invisible (SaaS non référencés, solutions métiers).
- Shadow IT résiduel et connu. Les métiers ont confiance dans l'IT et utilisent les canaux officiels.

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. Nous avons un comité de pilotage IT régulier avec COMEX/DG, DSI, et représentants métiers.	☐	☐	☐
2. Les rôles de décision IT (RACI) sont documentés pour les 10 sujets les plus critiques.	☐	☐	☐
3. Un tableau de bord IT à 6-8 KPI est remonté au COMEX au moins trimestriellement.	☐	☐	☐
4. Nous avons une méthodologie projet IT simple et appliquée (phases, jalons, sponsor, chef de projet).	☐	☐	☐
5. Un registre des risques IT est maintenu et révisé au moins trimestriellement par le comité IT.	☐	☐	☐
6. Les incidents IT majeurs donnent lieu à un retour d'expérience formalisé et capitalisé.	☐	☐	☐
7. Les projets IT > 50 K€ font l'objet d'un cadrage formel approuvé par le comité de pilotage.	☐	☐	☐
8. La politique IT est formalisée (5-15 pages) et validée par la direction générale.	☐	☐	☐
9. Les prestataires IT critiques sont identifiés et soumis à évaluation annuelle de performance.	☐	☐	☐
10. Un rapport mensuel d'activité IT est produit par le DSI pour la direction générale.	☐	☐	☐
11. Les conformités (NIS2, RGPD, ISO) sont intégrées dans les processus courants, pas gérées en mode crise.	☐	☐	☐
12. La fonction IT dispose de fiches de poste, d'objectifs et d'un plan de formation annuel.	☐	☐	☐

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

COBIT allégé, priorisé, rendu pratique. Pas de slides, que des livrables utiles.

Diagnostic COBIT express (5 jours)

Évaluation de la maturité de votre gouvernance IT sur les 40 objectifs COBIT 2019. Livrable : radar de maturité, top 8 objectifs prioritaires pour votre contexte, feuille de route 6 mois. Inclut un atelier de restitution avec COMEX et équipe IT. Forfait fixe, sans engagement.

Cadrage gouvernance IT sur-mesure

À partir de votre contexte (secteur, taille, maturité, priorités business), nous sélectionnons 5-10 objectifs COBIT réellement utiles pour vous. Pour chacun : définition, acteurs, indicateurs, niveau de maturité cible. Livrable exploitable immédiatement. Durée : 3-6 semaines.

Mise en œuvre COBIT light (4-6 mois)

Accompagnement opérationnel pour structurer votre gouvernance : comité de pilotage IT, tableau de bord COMEX, RACI des décisions, méthodologie projets, processus incidents, gestion des risques. Livrables jalonnés, testables à chaque étape.

Architecture des rôles et responsabilités

Dans beaucoup de PME, "qui décide quoi en IT ?" est flou. Nous clarifions : rôles du DG, du DSI, du comité IT, des métiers, des prestataires. Matrices RACI formelles pour les 10-15 décisions clés (budget, projets, incidents majeurs, sécurité, conformité).

Comité de pilotage IT (mise en place & animation)

Conception du comité IT adapté à votre taille : périodicité, participants, ordre du jour type, tableau de bord, décisions attendues. Option : animation par notre équipe pendant les 3-6 premiers mois, avec transfert progressif à un pilote interne.

Alignement COBIT / NIS2 / ISO 27001

Si vous êtes soumis à NIS2 ou visez ISO 27001, COBIT peut servir de chapeau intégrateur. Nous construisons une matrice d'équivalence qui évite de doublonner politiques, procédures et audits : les mêmes preuves servent plusieurs conformités, et vous ne rédigez qu'une fois.

Gouvernance IT fractionnée (DSI externe)

Pour les PME qui ne peuvent pas financer un DSI à temps plein : un DSI externe 3 à 8 jours par mois pour piloter la gouvernance, animer le comité IT, arbitrer avec le COMEX. Coût d'un profil junior pour l'expertise d'un senior multi-sectoriel.

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	MOIS 1-2	MOIS 2-4	MOIS 4-6	CONTINU
Diagnostic	**Cadrage**	**Processus**	**Ancrage**	**Maturité**
• Auto-évaluation • Radar maturité • Sélection objectifs • Sponsor DG	• Comité IT • RACI • Tableau de bord • Politique IT	• Méthodo projet • Gestion incidents • Registre risques • Gestion RH IT	• Animation comité • Formation acteurs • Indicateurs • Reporting board	• Audit annuel • Amélioration continue • Extension progressive

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.

Articulation COBIT avec NIS2, ISO, RGPD

Chapitre 9

COBIT est compatible avec tous les référentiels majeurs. Voici comment l'utiliser sans doublonner.

Distinction gouvernance / management

COBIT 2019

COBIT distingue clairement la gouvernance (5 objectifs EDM, portés par le board : Evaluer, Diriger, Monitorer) et le management (35 objectifs APO, BAI, DSS, MEA). Les deux niveaux sont essentiels.

BÉNÉFICE CACHÉ :

Cette distinction clarifie immédiatement les responsabilités : le board ne fait pas de la gestion, le management ne fait pas de la gouvernance. Élimine les conflits de rôles fréquents en PME.

Articulation avec NIS2

NIS2 + COBIT

COBIT fournit un cadre qui couvre l'essentiel des exigences de gouvernance NIS2, notamment l'art. 20 : approbation des mesures par la direction, supervision, formation des dirigeants. Implémenter COBIT rend NIS2 plus simple à atteindre.

BÉNÉFICE CACHÉ :

Une seule structure (comité IT, tableau de bord, RACI) sert à la fois COBIT et NIS2. Le ROI est démultiplié : un effort, deux conformités.

Articulation avec ISO 27001

ISO 27001 + COBIT

ISO 27001 est orienté sécurité de l'information. COBIT est plus large (gouvernance IT complète). Les deux sont parfaitement compatibles : COBIT donne le cadre, ISO 27001 précise les contrôles sécurité.

BÉNÉFICE CACHÉ :

Pour une PME qui vise ISO 27001, commencer par un cadre COBIT allégé accélère et sécurise la démarche ISO. La cartographie est plus claire, les audits sont mieux préparés.

Sélection des objectifs prioritaires

COBIT Design Guide

Le Design Guide COBIT recommande de choisir 3 à 15 objectifs selon 11 facteurs de conception (taille, criticité IT, dépendance, culture, etc.). Pas besoin d'implémenter les 40.

BÉNÉFICE CACHÉ :

Cette approche "customisable" rend COBIT utilisable par une PME de 50 personnes comme par une multinationale. Vous n'implémentez que ce qui vous apporte de la valeur.

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 une auto-évaluation COBIT (radar de maturité sur 40 objectifs).	🟢🟢⚪⚪⚪	🟢🟢🟠🔴⚪	1 mois
☐	Sélectionner les 6-8 objectifs COBIT prioritaires avec la DG.	🟢🟢⚪⚪⚪	🟢🟢🟠🔴🔴	2 mois
☐	Mettre en place un comité de pilotage IT mensuel.	🟢🟢⚪⚪⚪	🟢🟢🟠🔴🔴	2 mois
☐	Définir et faire valider la RACI IT (10 décisions clés).	🟢🟢🟠⚪⚪	🟢🟢🟠🔴🔴	3 mois
☐	Créer un tableau de bord IT à 6-8 KPI pour le COMEX.	🟢🟢⚪⚪⚪	🟢🟢🟠🔴🔴	3 mois
☐	Rédiger et faire valider une politique IT formelle (5-15 pages).	🟢🟢🟠⚪⚪	🟢🟢🟠🔴⚪	3 mois
☐	Formaliser une méthodologie projet simple (5 phases, 3 jalons).	🟢🟢⚪⚪⚪	🟢🟢🟠🔴⚪	4 mois
☐	Documenter les 3-5 processus IT critiques (incidents, changements, accès).	🟢🟢🟠🔴⚪	🟢🟢🟠🔴⚪	5 mois
☐	Mettre en place un registre des risques IT trimestriel.	🟢🟢🟠⚪⚪	🟢🟢🟠🔴⚪	4 mois
☐	Professionnaliser la fonction IT (fiches de poste, objectifs, plan de formation).	🟢🟢🟠⚪⚪	🟢🟢🟠🔴⚪	6 mois
☐	Articuler COBIT avec NIS2/ISO 27001/RGPD (matrice d'équivalence).	🟢🟢🟠⚪⚪	🟢🟢🟠🔴⚪	6 mois

		EFFORT	IMPACT	DÉLAI
☐	Engager un audit blanc COBIT à 12-18 mois pour mesurer les progrès.	●●●○○	●●●○○	12 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. Combien d'objectifs COBIT faut-il implémenter dans une PME ?

Le Design Guide COBIT 2019 recommande 3 à 15 objectifs selon 11 facteurs de conception (taille, criticité de l'IT, sourcing, culture...). Pour une PME de 50-150 personnes, 6-8 objectifs couvrent l'essentiel de la valeur. Sélection typique : APO01 (cadre de management IT), APO07 (RH IT), BAI03 (gestion des solutions), DSS02 (incidents), DSS04 (continuité), MEA01 (performance), MEA03 (conformité externe). Plus un objectif EDM de gouvernance pure (EDM01, cadre de gouvernance, ou EDM02, délivrance de valeur).

Q2. Que recouvrent exactement les domaines EDM, APO, BAI, DSS et MEA ?

EDM (Evaluate, Direct and Monitor) : la gouvernance au sens strict, portée par le conseil et la direction (valeur, risques, ressources, transparence). APO (Align, Plan and Organize) : stratégie IT, architecture, budget, risques, RH. BAI (Build, Acquire and Implement) : projets, développements, acquisitions, changements. DSS (Deliver, Service and Support) : exploitation quotidienne, incidents, continuité, sécurité opérationnelle. MEA (Monitor, Evaluate and Assess) : mesure de la performance, contrôle interne, conformité externe. Une PME n'active que quelques objectifs dans chaque domaine.

Q3. Quelle est la différence entre COBIT et ITIL ?

COBIT est un framework de gouvernance IT : pourquoi, qui décide, quels KPI, comment mesurer la maturité. ITIL est un framework de gestion des services IT : comment gérer incidents, changements, services. Pour une PME, on utilise COBIT comme chapeau stratégique et ITIL pour les processus opérationnels (si pertinents). Les deux sont complémentaires.

Q4. COBIT est-il compatible avec NIS2 ?

Oui, très largement. COBIT couvre l'essentiel des exigences de gouvernance de NIS2 (art. 20 notamment : approbation par la direction, supervision, formation). Implémenter COBIT allégé rend la conformité NIS2 plus simple : la gouvernance est en place, la RACI existe, le tableau de bord remonte au COMEX. Les briques spécifiques NIS2 (notification 24h, enregistrement Safeonweb@Work, registre des prestataires) s'ajoutent naturellement au dispositif COBIT, et le tout prépare une certification CyFun ou ISO 27001.

Q5. Quel est le budget pour un projet COBIT PME ?

Pour une PME de 80-150 personnes, un "COBIT light" bien cadré coûte 25-60 K€ sur 4-6 mois. Ce budget couvre : diagnostic, cadrage des 6-8 objectifs, mise en place du comité IT, rédaction de la politique IT, accompagnement opérationnel. Les gros budgets (300-800 K€) sont l'apanage des cabinets internationaux qui vendent du slideware, pas le coût réel de COBIT.

Q6. Faut-il un DSI à temps plein pour faire du COBIT ?

Non. Une PME peut faire du COBIT avec un DSI temps plein, un DSI fractionnel (externe, 2-5 jours/mois), ou même sans DSI formalisé mais avec un "responsable IT" clairement identifié. L'important est qu'il y ait UN pilote, qu'il ait un mandat clair, et que le comité de pilotage IT fonctionne. COBIT ne crée pas de besoins RH : il clarifie ceux qui existent déjà.

Q7. COBIT vs ISO 27001, lequel commencer ?

Pour une PME qui vise à terme ISO 27001 : commencer par COBIT light (4-6 mois) pour poser la gouvernance, puis enchaîner ISO 27001 (9-15 mois) pour formaliser le SMSI. COBIT facilite énormément l'ISO 27001 car il donne le cadre et les rôles. L'inverse (ISO puis COBIT) fonctionne aussi mais est moins efficient.

Q8. Faut-il une certification COBIT (CGEIT, CISA) pour piloter le projet ?

Utile mais pas indispensable. Les certifications ISACA (CGEIT pour la gouvernance, CISA pour l'audit) attestent d'une connaissance approfondie du framework. Pour une PME, l'expérience pratique compte davantage : un consultant qui a déjà implémenté COBIT dans 3-5 PME de taille similaire apporte plus qu'un consultant junior certifié.

Q9. Comment articuler COBIT avec une méthode agile (Scrum, SAFe) ?

COBIT et agile sont parfaitement compatibles. COBIT définit le cadre de gouvernance (décisions, budgets, priorités), agile gère l'exécution produit/IT au sein de ce cadre. Il existe même un "COBIT 2019 for Agile" qui propose des adaptations spécifiques. Les PME tech en Belgique (SaaS, fintechs) combinent de plus en plus les deux avec succès.

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

Cadrez votre gouvernance IT

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