

ISO 27001 pour une PME : pour qui, pour quoi, à quel prix

La certification sécurité de référence démystifiée : ce qu'elle exige vraiment, quand elle vaut l'investissement, et les alternatives.

8 min de lecture · Niveau Avancé · cyberionis.fr/ressources/iso-27001-pme

ISO 27001 est LA certification de sécurité de l'information : un système de management (SMSI) audité par un tiers, reconnu mondialement. Longtemps réservée aux grands comptes, elle descend vers les PME — poussée par les appels d'offres, NIS2 et les questionnaires clients. Faut-il y aller ? Réponse honnête : parfois oui, souvent pas encore — et il existe des marches intermédiaires qui capturent l'essentiel de la valeur.

1. Ce que c'est vraiment

- Un système de management, pas une liste technique : analyse de risques, politiques, responsabilités, amélioration continue — la norme exige que vous SACHIEZ et PILOTIEZ, plus qu'elle n'impose des outils précis
- L'annexe A : le catalogue de 93 mesures de référence (dans la version 2022) parmi lesquelles vous justifiez vos choix — accès, chiffrement, sauvegardes, fournisseurs, incidents... le contenu de nos guides, structuré
- La certification : un audit initial par un organisme accrédité, puis des audits de surveillance annuels et un renouvellement à trois ans
- Le périmètre se choisit : certifier l'activité d'hébergement ou le service concerné, pas forcément toute l'entreprise — levier majeur de coût

2. Quand elle vaut l'investissement

- Vos clients l'exigent ou la scorent : éditeurs et prestataires IT servant des grands comptes, sous-traitants de secteurs régulés — le certificat débloque des marchés fermés autrement
- Elle répond d'un coup aux questionnaires : le certificat remplace des dizaines d'audits clients par an — un vrai calcul de temps commercial
- Elle structure une croissance rapide : le SMSI discipline ce que la croissance désorganise
- Signaux que c'est prématuré : aucun client ne la demande, le socle de base n'est pas en place (la norme formalise, elle ne crée pas la sécurité), ou la motivation est « le logo sur le site »

BON À SAVOIR

Les ordres de grandeur pour une PME (périmètre raisonnable) : 6 à 18 mois de démarche, un accompagnement conseil de 15 à 40 jours, l'audit de certification en milliers d'euros par an, et — le vrai coût — le temps interne d'un pilote. Total première année : typiquement quelques dizaines de milliers d'euros. À mettre en face des marchés accessibles : pour un éditeur B2B, un seul contrat gagné rembourse souvent tout.

3. Les marches intermédiaires (souvent le bon choix)

- Le guide d'hygiène ANSSI mis en œuvre et documenté : le socle reconnu, gratuit, qui répond déjà à beaucoup de questionnaires
- Une « conformité ISO sans certification » : s'aligner sur la norme, le déclarer, et laisser l'audit client vérifier — la moitié de la valeur pour une fraction du coût
- Les labels accessibles : ExpertCyber pour les prestataires, les référentiels sectoriels — plus légers, parfois suffisants pour vos marchés
- La trajectoire honnête : socle !' documentation !' analyse de risques !' (si le marché le justifie) certification — chaque marche a sa valeur propre, aucune n'est du travail perdu pour la suivante

4. Réussir la démarche si vous y allez

- Un sponsor direction réel : le SMSI meurt sans portage — c'est un projet d'entreprise, pas un projet informatique
- Un périmètre initial resserré : l'activité qui fait face aux clients exigeants, extensible ensuite
- Un accompagnement expérimenté PME : la norme s'adapte à votre taille — méfiez-vous des consultants qui livrent le classeur de 300 pages d'un groupe
- S'appuyer sur l'existant : documentation, gestion des accès, incidents — la démarche capitalise tout ce que vous avez déjà
- Viser l'utile : un SMSI vivant qu'on consulte, pas un monument documentaire qu'on ressort à l'audit

L'essentiel à retenir

- 01 Vérifier la demande réelle du marché (clients, appels d'offres)
- 02 Consolider d'abord le socle d'hygiène et sa documentation
- 03 Choisir un périmètre de certification resserré
- 04 Chiffrer accompagnement, audit ET temps interne
- 05 Nommer un pilote et un sponsor direction
- 06 Considérer les marches intermédiaires avant de trancher

Questions fréquentes

Quelle différence entre ISO 27001 et un audit de sécurité ?

L'audit photographie votre sécurité à un instant T ; ISO 27001 certifie que vous avez un SYSTÈME pour la gérer en continu — analyse de risques, pilotage, amélioration. L'audit dit « où vous en êtes », la certification dit « comment vous vous y prenez, durablement ». Les deux se complètent : le SMSI intègre d'ailleurs des audits réguliers.

HDS, SecNumCloud, SOC 2 : comment s'y retrouver ?

Par le marché visé : HDS est obligatoire pour héberger des données de santé françaises ; SecNumCloud est la qualification ANSSI des clouds de confiance (secteur public et sensible) ; SOC 2 est l'équivalent d'usage nord-américain — pertinent si vos clients sont américains. ISO 27001 reste le socle générique international, souvent prérequis ou accélérateur des autres. On choisit selon les clients qu'on veut servir, pas par collection.

Une certification garantit-elle qu'on ne sera pas piraté ?

Non — elle garantit un niveau de maîtrise et de réaction, pas l'invulnérabilité : des entreprises certifiées subissent des incidents, et les gèrent généralement mieux. Méfiez-vous du raisonnement inverse chez vos fournisseurs : le certificat est un excellent signal (voir notre guide), pas un blanc-seing qui dispense des questions de base.

Pour aller plus loin

AFNOR — la certification ISO/IEC 27001 — www.afnor.org

ANSSI — le guide d'hygiène, socle avant certification — cyber.gouv.fr/publications/guide-dhygiene-informatique

Structurer sans vous noyer dans la paperasse ?

Audit, mise en conformité, chartes et sensibilisation des équipes : un accompagnement à la taille de votre entreprise.

contact@cyberionis.fr · 06 64 90 07 74 · cyberionis.fr