Contents

Pilotage Sécurité — Document de Référence Global

MeilleureSCPI.com — 2025

---

1. Introduction

1.1 Contexte

Dans le cadre de mes objectifs annuels, il a été décidé de structurer la démarche de sécurité du SI et d'externaliser autant que possible cette responsabilité à un prestataire spécialisé.

L'analyse présentée ici repose sur des hypothèses réalistes pour une PME SaaS, dans l'objectif d'identifier ce qui peut être externalisé et ce qui devra rester géré en interne.

Le choix d'un cadre ISO 27001 (version allégée) fournit une structure reconnue, adaptée à notre taille, sans imposer une démarche lourde ou industrielle. Le périmètre préliminaire a été défini avec l'aide de ChatGPT afin d'obtenir une base cohérente avec notre organisation (applications, API, SaaS, données, pratiques internes). Il sera ensuite affiné avec le prestataire.

Certaines actions resteront nécessairement internes (gestion des accès, pratiques dev/ops, décisions organisationnelles).

Ce document présente la méthodologie retenue, les phases du projet et les estimations associées.

Mon rôle : cadrage, sélection prestataire, pilotage interne, validation technique.

1.2 Objectifs

L'objectif est de renforcer la sécurité de nos applications et de notre SI de façon structurée et durable, en limitant au maximum la charge interne.

Un autre enjeu est d'améliorer notre conformité globale : protection des données, gestion des accès, journalisation, et maîtrise des services externes. Ne pas le faire expose l'entreprise à des risques juridiques (RGPD, responsabilité), opérationnels (interruptions, pertes de données) et réputationnels.

---

2. Workflow global

---

3. Phase 0 — Recherche & Qualification des prestataires

3.1 Objectif

Identifier **3 à 5 prestataires pertinents avant de finaliser notre périmètre interne**. Cela permet :

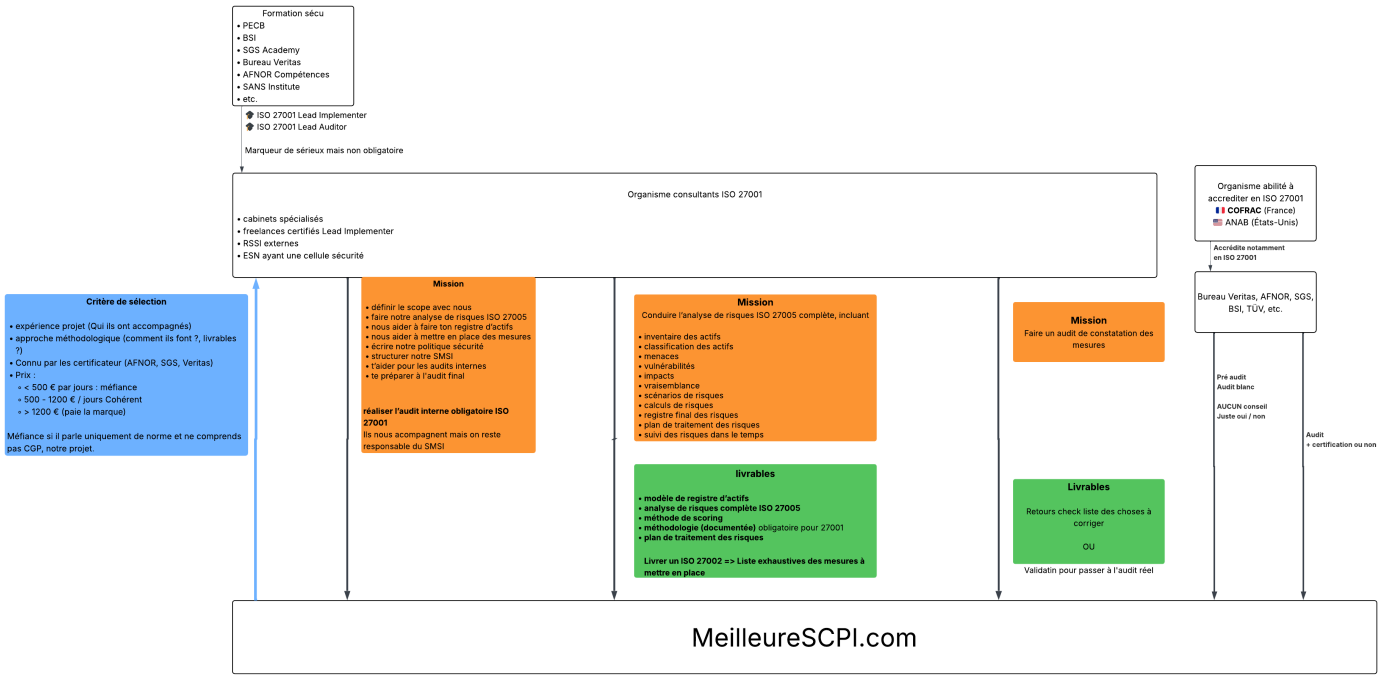

Figure 1: Schema du projet global

- de valider la faisabilité et les méthodologies proposées,
- d'éviter de sur-spécifier le périmètre sans expertise,
- de filtrer rapidement les prestataires non adaptés,
- d'ajuster ensuite notre périmètre théorique.

Plan Global : * Campagne de mail à tous les prestataires * Demander à un LLM de remplire d'extraire les informations selon les critères qu'on a défini dans le sheet de suivi * Éliminer un max à cette étape => Rester sur 3 à 5 presta * Faire une visio avec ceux-ci pour n'en sélectionner finalement qu'un

---

3.2 Mail type à envoyer

Un template à été préparé en **Annexe D**

3.3 Réponse attendue des prestataires

1. Compréhension du besoin
2. Méthodologie détaillée
3. Livrables proposés
4. Capacités d'accompagnement
5. Planning indicatif
6. Certifications
7. Références
8. Contraintes éventuelles

3.4 Grille de comparaison

Version simplifiée (Grandes catégories)

Critère	Prestataire A	Prestataire B	Prestataire C
Compréhension du besoin			
Méthodologie proposée			
Certifications			
Livrables			
Accompagnement			
Références			
Disponibilité			
Budget indicatif			

Version plus exhaustive

C’est une première version qu’on pourras adapter.

Durée totale estimée : 1 semaine (cohérent avec planning T1).

---

4. Périmètre préliminaire (à affiner avec le presta)

1. Code & Données
2. Applications Web & API
3. Infrastructure & SaaS
4. Process internes
5. Gouvernance & Pérennité

 Le périmètre final sera défini avec le prestataire.

---

5. Phase 1 — Préparation interne

Objectif : préparer un dossier complet permettant d’interroger les prestataires et de lancer la mission en Phase 2.

5.1 Finalisation du document de projet

Durée : 0,5 à 1 jour
• Consolidation du contexte, objectifs et planning
• Validation interne (direction + technique)

Livrable : Document “Pilotage Sécurité — v1”

5.2 Définition du besoin détaillé & périmètre préliminaire

Durée : 0,5 à 1 jour
• Définir les blocs analysés (applis, API, SaaS, données, organisation)
• Lister les zones hors scope potentiels
• Récolter les premiers éléments internes nécessaires au prestataire

Livrable : Périmètre préliminaire (version non figée)

5.3 Rédaction du cahier des charges

Durée : 1 jour
• Compilation du besoin
• Formulation des livrables attendus
• Critères de sélection
• Contraintes, méthodologies acceptées, planning prévisionnel
• Exigences minimales (certifications, accompagnement, etc.)

Livrable : Cahier des Charges (CDC) envoyé aux prestataires

5.4 Sélection finale & contractualisation

Durée : 1 à 3 jours

5.4.1 Analyse des réponses et short-list

• Analyse des retours écrits
• Évaluation (grille de critères)
• Sélection de 2–3 prestataires pour visio

5.4.2 Échanges de cadrage

• Visio 30–45 min
• Ajustement du périmètre
• Validation de la méthodologie

5.4.3 Devis & contractualisation

• Réception des devis
• Comparaison technique + budget
• Sélection finale
• Signature du devis / contrat

Livrables :
• Short-list
• Devis validé
• Prestataire retenu

---

6. Phase 2 — Mission du prestataire (ISO 27005)

Durée estimée : **6 à 13 jours** □ Cohérent avec planning T2 (3 à 6 semaines) (Dépend principalement du prestataire).

Workflow résumé

1. Cadrage (Réunion avec eux pour dire ce qu'on veut et voir ce qui est faisable avec le budget)
2. Inventaire actifs (Ils devrons répertorier tous les "actifs" (laptop, locaux, services externes : google, universign...))
3. Menaces (Pour chaque actif identifier les menace potentielles)
4. Vulnérabilités (Pour chaque menace voir si on y est vulnérable)
5. Scénarios
6. Matrice
7. Plan d'action

8. ISO 27002 (une liste des mesures qu'on doit mettre en place)
9. Rapport final

Workflow détaillé

(intégral, non modifié)

---

7. Phase 3 — Mise en œuvre

Durée estimée : **1 à 6 mois** (Dépendra principalement du retour du prestataire et des ressources allouées à la mise en oeuvre)

Actions possibles :

- MFA
- CI/CD sécurisé
- Chiffrement terminaux
- Politique LLM
- Gestion des accès
- Monitoring
- Sensibilisation

Audits récurrents : pentest, infra, RGPD, phishing.

---

8. Phase 4 — Organisme certificateur & Audit officiel

La Phase 1 de l'audit ISO 27001 est un audit documentaire. Elle se fait généralement en visio et consiste à vérifier que le SMSI existe bien : politiques, procédures, registre des risques, périmètre, preuves minimales.

La Phase 2 est l'audit opérationnel. L'auditeur vérifie que les pratiques décrites sont réellement appliquées : accès, sauvegardes, CI/CD, contrôle des documents, gestion des incidents, etc. Cette phase se déroule souvent sur site ou en visio selon le périmètre.

- Phase 1 audit : **1–2 jours**
- Phase 2 audit : **2–5 jours**

Information plus exhaustives en Annexe E

8.1 Objectifs

- choisir organisme
- comprendre méthode
- planifier audit ISO

8.2 Organismes certifiants

(AFNR, BSI, Bureau Veritas, SGS, PECB)

8.3 Étapes de l'audit ISO 27001

1. **Phase 1 documentaire** — 1 à 2 jours
2. **Phase 2 opérationnelle** — 2 à 5 jours

3. **Certification** (optionnelle)

8.4 Coûts

---

9. Phase 5 — Maintien en Conditions de Sécurité (MCS)

Actions annuelles + cycle PDCA.

---

10. Budget global

10.1 Cohérence du budget

Les montants présentés ci-dessous sont **cohérents uniquement dans le cadre d'un périmètre typique de PME SaaS / fintech**, comprenant :

- 1 application web (VueJS),
- 1 backend/API (Symfony),
- 10–20 services SaaS critiques (Google Workspace, GitHub, Dashlane, Datakeen…),
- une dizaine d'utilisateurs internes,
- un fonctionnement hybride (télétravail + coworking),
- aucune infrastructure on-premise complexe,
- un volume d'actifs raisonnable (50–150 actifs ISO 27005).

Ces chiffres supposent également :

- un SI **déjà fonctionnel**, mais **pas encore structuré** au niveau sécurité,
- quelques bonnes pratiques déjà en place (MFA partiel, GitHub, CI/CD existant),
- une volonté d'appliquer **une ISO 27001 light**, pas une industrialisation complète,
- des mesures techniques **simples à moyennes** à mettre en place en Phase 3.

 Pourquoi les coûts peuvent varier (et parfois doubler)

Les budgets dépendent **directement** :

1. Du périmètre retenu Plus il y a d'actifs, de SaaS, d'applications, d'équipes ou de flux métiers, plus l'analyse ISO 27005 est longue plus le plan d'action ISO 27002 est dense plus la mise en œuvre (Phase 3) coûte cher.

2. Du nombre d'actifs à analyser (ISO 27005)

- Une petite structure : **30–80 actifs**
- Une PME SaaS normale : **80–150 actifs**
- Une organisation complexe : **200–500 actifs**

  Le volume d'actifs impacte *massivement* la durée de la Phase 2.

3. De l'état actuel de la sécurité Quelques exemples :

Si aujourd'hui…	Alors la Phase 3 sera…
MFA absent	+2 à 5 jours internes
CI/CD basique	+3 à 7 jours
Gestion accès floue	+3 à 10 jours

Si aujourd'hui…	Alors la Phase 3 sera…
Sauvegardes non auditées	+2 à 6 jours
SaaS non maîtrisés	+2 à 8 jours

Si vous êtes déjà matures coûts plus bas. Si vous partez de zéro coûts plus hauts.

4. Des mesures à mettre en œuvre (Phase 3) Les coûts varient selon la profondeur des travaux :

- mesures simples (MFA, durcissement, monitoring, doc) bas de fourchette
- mesures complexes (refonte CI/CD, IAM, segmentation, PRA) haut de fourchette

5. Du niveau d'ambition ISO 27001 Il existe 3 niveaux de mise en conformité :

Niveau	Objectif	Coût
Light (PME SaaS)	structuration SMSI, risques, mesures clés	Bas
Standard (PME 50–200 pers)	mise en conformité solide	Moyen
Certification complète	conformité + preuves + audit officiel	Haut

---

10.2 Budget prévisionnel par phase

Phase	Coût
Phase 0	0 €
Phase 2	8 000 – 15 000 €
Phase 3	2 000 – 12 000 €
Phase 4 (Sans certification)	4 500 – 12 000 €
Phase 4 (Avec certification)	9 500 – 25 000 €
Phase 5 (Sans certification)	5 000 – 12 000 €/an
Phase 5 (Avec certification)	7 000 – 15 000 €/an

10.3 Budget prévisionnel *avec certification ISO 27001*

Phase	**À qui ?**	**Coût estimé**	**Charge interne estimée**
Phase 0	Interne	**0 €**	**2 à 4 j.h**
Phase 2 — Analyse des risques	Prestataire sécurité	**8 000 – 15 000 €**	**5 à 10 j.h**
Phase 3 — Mise en œuvre	Prestataire sécurité	**2 000 – 12 000 €**	**10 à 25 j.h**
Phase 4 — Pré-audit / préparation certification	Prestataire sécurité	**9 500 – 25 000 €**	**5 à 12 j.h**
Total Année 1 (avec certification, hors audit officiel)	**Prestataire uniquement**	**19 500 € – 52 000 €**	**22 à 51 j.h internes**
Phase 5 — Maintien SMSI certifié (support)	Prestataire sécurité	**7 000 – 15 000 €/an**	**5 à 12 j.h/an**
Coût annuel récurrent (Années suivantes)	**support SMSI**	**7 000 € – 15 000 €/an**	**5 à 12 j.h/an**

10.4 — Budget prévisionnel *sans certification*

Phase	À qui ?	Coût estimé	Charge interne estimée
Phase 0	Interne	**0 €**	**2 à 4 j.h**
Phase 2 — Analyse des risques	Prestataire sécurité	**8 000 – 15 000 €**	**5 à 10 j.h**
Phase 3 — Mise en œuvre	Prestataire sécurité	**2 000 – 12 000 €**	**10 à 25 j.h**
Phase 4 — Audit interne uniquement	Prestataire sécurité	**4 500 – 12 000 €**	**2 à 6 j.h**
Total Année 1 (sans certification)	**Prestataire uniquement**	**14 500 € – 39 000 €**	**19 à 45 j.h internes**
Phase 5 — Maintien sécurité (non certifié)	Prestataire sécurité	**5 000 – 12 000 €/an**	**3 à 8 j.h/an**
Coût annuel récurrent (Années suivantes)	**support sécurité**	**5 000 € – 12 000 €/an**	**3 à 8 j.h/an**

□ Synthèse ultra-courte (à mettre dans une slide)

Option	Total Année 1 (prestataire)	Charge interne Année 1	Récurrent annuel (prestataire)	Charge interne annuelle
Avec certification	**19.5k – 52k €**	**22 – 51 j.h**	**7k – 15k €/an**	**5 – 12 j.h/an**
Sans certification	**14.5k – 39k €**	**19 – 45 j.h**	**5k – 12k €/an**	**3 – 8 j.h/an**

□ Les coûts sont alignés avec les étapes.

---

11. Planning prévisionnel — Année 2026

Phase	Jan	Fév	Mar	Avr	Mai	Jui	Jui	Aoû	Sep	Oct	Nov	Déc
T1 — Sélection prestataire (4–5 semaines)	□□□	□□□										
T2 — Analyse des risques (3–6 semaines)		□□	□□□									
T3 — Mise en œuvre (1 à 6 mois)			□□	□□□	□□□	□□□	□□□	□□□				
T4 — Audit officiel (4–8 semaines)					□□	□□□	□□□					

- Jan : Sélection prestataire
- Fév : Sélection □ Analyse risques
- Mar : Analyse risques □ Début mise en œuvre
- Avr : Mise en œuvre
- Mai : Mise en œuvre □ Audit
- Juin : Audit
- Juil : Audit / Mise en œuvre (selon charge)
- Août : Pause ou actions internes
- Sep : Reprise mise en œuvre (si besoin)

---

12. Normes ISO prioritaires & pertinentes

Norme ISO	Rôle / Objet	Ce qu'elle contient	Utilité pour ton projet (PME / Fintech / Data SCPI)
ISO 27001	**Système de Management de la Sécurité (SMSI)**	Processus, politique sécurité, gouvernance, gestion prestataires, mise en place d'un plan sécurité.	✅ *Pilier central pour structurer ton projet "Pilotage Sécurité".*
ISO 27002	**Catalogue des contrôles sécurité**	MFA, gestion accès, sauvegardes, cryptographie, journaux, CI/CD, télétravail, etc.	✅ *Base pour écrire tes bonnes pratiques internes + exigences prestataires.*
ISO 27005	**Méthodologie d'analyse de risques**	Actifs → Menaces → Vulnérabilités → Scénarios → Risques → Plan d'action.	✅ *Norme à utiliser pour ta cartographie des risques (ton JSON).*
ISO 27701	**Extension RGPD / Privacy Information Management**	Gouvernance données personnelles, registre, consentement, minimisation.	✅ *Très utile si vous manipulez des données personnelles clients.*
ISO 27017	**Sécurité du Cloud**	Bonnes pratiques spécifiques cloud (IAM, logs, isolation, hyperviseur).	✅ *Pertinent si évolution vers le cloud ou usage massif de SaaS.*
ISO 27018	**Protection des données personnelles dans le cloud**	Clauses contractuelles, confidentialité, protection des données hébergées.	✅ *Utile si stockage client dans le cloud (ex : Scaleway, GCP).*
ISO 27019	**Sécurité des systèmes industriels**	SCADA, IoT industriels.	❌ *Pas utile pour ton entreprise.*
ISO 22301	**Continuité d'activité (PCA/PRA)**	Plan de continuité, reprise après incident, indisponibilité.	✅ *Utile si dépendance forte à vos systèmes (API, dashboards clients).*
ISO 31000	**Gestion générale des risques**	Cadre global pour la gestion des risques (pas que sécurité).	⚠ *Optionnel. 27005 est suffisant pour toi.*
ISO 9001	**Management qualité**	Processus, documentation, qualité organisationnelle.	⚠ *Peut aider en gouvernance, mais non essentiel à la sécurité.*
ISO 20000	**Gestion des services IT (ITIL-like)**	Support, tickets, gestion changements, incidents IT.	⚠ *Utile si vous formalisez un service IT interne.*

Précision ISO 27001

L'ISO 27001:2022 regroupe **93 contrôles** dans **4 grandes familles** ✅ (Ce sont les blocs que les auditeurs regardent vraiment.)

Thématique (ISO 27001:2022)	**Éléments clés / Exemples**
Organisational Controls (37)	Politique sécurité ; rôles & responsabilités ; gestion fournisseurs (SaaS/cloud) ; classification ; journalisation/monitoring ; continuité ; gestion incidents
People Controls (8)	Sensibilisation ; formation dev (secure coding) ; gestion des accès humains
Physical Controls (14)	Sécurité locaux ; matériel en mobilité ; protections physiques coworking/fournisseurs
Technological Controls (34)	MFA ; IAM ; chiffrement (API/DB) ; développement sécurisé ; CI/CD sécurisé ; surveillance logs ; pentest ; sauvegardes

Précision sur la certification ISO 27001 et la notion de périmètre

La norme **ISO 27001** impose que toute certification s'applique à un **périmètre clairement défini**. Ce périmètre correspond à la partie exacte du système d'information, des activités et des sites couverts par le **SMSI (Système de Management de la Sécurité de l'Information)**.

Concrètement :

- **L'entreprise choisit le périmètre** qu'elle souhaite faire certifier (ex. : une plateforme SaaS, un service, un ensemble de processus, une équipe ou la totalité de l'organisation).
- Le périmètre doit être **décrit précisément** dans la documentation du SMSI et validé par l'auditeur.
- **La certification ISO 27001 est délivrée uniquement sur ce périmètre**, et non sur l'ensemble de l'entreprise si celui-ci est partiel.
- Le certificat officiel indique **explicitement le périmètre couvert**, généralement sous la forme : *« Prestations couvertes par le SMSI : développement, hébergement et exploitation de la plateforme X »,* ou *« Gestion et traitement des données financières SCPI pour le service Y ».*

Cela signifie que :

- une entreprise peut être certifiée ISO 27001 **sur une partie seulement** de son activité,
- et qu'un prestataire qui se présente comme "certifié ISO 27001" l'est **uniquement sur le périmètre précisé dans son certificat**.

 En résumé : le périmètre est un élément structurant du SMSI et fait partie intégrante de la certification. Sans périmètre défini, **aucune certification ISO 27001 n'est possible**.

Précision ISO 27005

Pour votre analyse de risques, **voici les catégories exactes** qu'ISO 27005 attend (simplifiées mais complètes) :

Niveau 1	Sous-catégorie	Éléments représentatifs
Actifs primaires	Informations métiers	Données SCPI ; informations investisseurs ; données financières ; données internes
	Processus métiers	Diffusion données SCPI ; API partenaires ; reporting ; exploitation plateforme SaaS
Actifs de support	**Humains**	Dev ; Ops ; Data ; Support ; Direction ; Prestataires externes
	Processus organisationnels	CI/CD ; gestion des accès ; gestion incidents ; gestion fournisseurs SaaS
	Matériels	Postes collaborateurs ; postes d'administration ; matériel réseau du coworking (non maîtrisé)
	Logiciels / Applications	VueJS ; Symfony/API ; CRM ; back-office ; outils internes ; runners CI/CD
	Données	Données SCPI ; données utilisateurs ; logs ; secrets ; clés API
	Services externes / Cloud	GCP/AWS ; SaaS critiques ; emailing ; monitoring ; hébergeurs ; bases partenaires

---

Précision ISO 27002

Voici une **liste ciblée pour une PME fintech avec API et applicatif web**.

Domaine 27002	Mesures clés (exemples)
Gestion des identités	MFA ; RBAC ; isolation des comptes privilégiés
Chiffrement	TLS 1.2+ ; chiffrement en base ; rotation périodique des clés
Journalisation & Monitoring	Logs centralisés ; journaux accès back-office ; alertes sur actions sensibles
Développement / DevSecOps	Revue de code ; SAST/SCA ; gestion secrets ; CI/CD sécurisé

Domaine 27002	Mesures clés (exemples)
Sauvegardes	Sauvegardes quotidiennes ; tests de restauration ; rétention conforme obligations
Sécurité Cloud & SaaS	Clauses sécurité ; IAM granulaire ; journalisation activée ; segmentation
Fournisseurs	Registre prestataires critiques ; validation sécurité ; exigences minimales

🧾 Annexe A. Glossaire Sécurité & Gouvernance

🔐 Concepts & Gouvernance

SMSI — Système de Management de la Sécurité de l'Information

Ensemble de politiques, procédures, processus et moyens permettant de gérer la sécurité de l'information dans l'entreprise, selon ISO 27001.

Analyse de risques (ISO 27005)

Méthode structurée pour identifier :

- les actifs,
- les menaces,
- les vulnérabilités,
- les impacts,
- les risques, et pour définir les mesures de traitement associées.

Plan d'action sécurité

Liste de mesures concrètes (techniques, organisationnelles, contractuelles) mises en place pour réduire les risques identifiés.

PSSI — Politique de Sécurité des Systèmes d'Information

Document définissant les règles internes de sécurité (accès, mots de passe, journalisation, sauvegardes, gestion des incidents…).

PDCA — Plan / Do / Check / Act

Cycle d'amélioration continue imposé par ISO 27001 : **Planifier**, **Mettre en œuvre**, **Contrôler**, **Améliorer**.

📚 Normes ISO 27000

ISO 27001 — Exigences de gouvernance sécurité

Norme certifiable définissant comment structurer un SMSI complet (politiques, risques, contrôles, audits, amélioration continue).

ISO 27002 — Catalogue de bonnes pratiques

Décrit en détail comment appliquer les mesures de sécurité (contrôles) de l'annexe A.

ISO 27005 — Gestion des risques

Méthodologie dédiée pour réaliser l'analyse de risques du SMSI.

Technologie & Méthodes

SaaS — Software as a Service

Prestations logicielles hébergées chez un fournisseur tiers et accessibles via Internet.

CI/CD — Continuous Integration / Continuous Deployment

Ensemble de pipelines automatisés permettant de développer, tester et déployer du code de manière continue.

LLM — Large Language Model

Modèle de langage de grande taille (ex. GPT, Claude, Mistral) utilisé pour la génération de texte, l'analyse, l'automatisation, etc.

Identité & Réseau

AD — Active Directory

Annuaire Microsoft utilisé pour gérer les identités, permissions, groupes et postes d'un environnement Windows.

Azure AD / Entra ID

Service d'identités cloud de Microsoft utilisé pour les authentifications, les accès SaaS, et les environnements Azure.

Réglementaire

RGPD — Règlement Général sur la Protection des Données

Text européen encadrant la protection des données personnelles (licéité, minimisation, transparence, droits utilisateurs, sécurité).

Prestataires & Qualifications

PASSI — Prestataire d'Audit de Sécurité des Systèmes d'Information

Qualification ANSSI permettant à un prestataire de réaliser des audits sensibles (réseau, config, code, org, etc.). Gage de sérieux et de compétence pour les audits critiques.

Méthodologies techniques

Tiering AD

Modèle en trois niveaux pour séparer les privilèges administratifs dans Active Directory (Tier 0, Tier 1, Tier 2).

SOC — Security Operations Center

Service chargé de détecter, analyser et répondre aux incidents de sécurité (SIEM, EDR, XDR…).

PTaaS — Pentest as a Service

Pentest en mode plateforme avec suivi continu, re-tests et intégration dans le cycle DevSecOps.

🧩 12 Analyse de Risques du Projet

A. Risques Organisationnels

Risque	Impact	Proba-bilité	Niveau	Indicateur / Prévention
Ressources internes insuffisantes	Retards Phase 2 & 3	Moyen	🔴 Élevé	• Charge >80% sur dev/CTO• Absence du référent >1 semaine→ **Allouer 0,5 j/semaine dédié**
Manque de disponibilité du management	Décisions bloquées	Moyen	🟠 Moyen	• Réunion repoussée >2 fois→ **Bloquer un point mensuel sécurité**
Dépendance à un collaborateur clé	Perte d'historique	Faible/Moyen	🟠 Moyen	• Une seule personne maîtrise CI/CD/accès→ **Documenter minimum vital dès Phase 1**

B. Risques liés au périmètre

Risque	Impact	Proba-bilité	Niveau	Indicateur / Prévention
Périmètre trop large	Explosion coûts/délais	Moyen	🔴 Élevé	• Actifs >150• Trop de SaaS dans scope→ **Limiter scope à plateforme + SaaS critiques**
Périmètre trop vague	Mauvaise estimation prestataire	Moyen	🟠 Moyen	• Prestataire pose "trop" de questions→ **Rédiger périmètre préliminaire clair (Phase 1)**
Découverte tardive de dépendances	Révision budget	Moyen/Élevé	🔴 Élevé	• Nouveaux SaaS apparaissent en Phase 2→ **Inventaire SaaS complet Phase 1**

C. Risques liés au prestataire

Risque	Impact	Proba-bilité	Niveau	Indicateur / Prévention
Prestataire trop cher / corporate	Budget ×2–4	Moyen	🔴 Élevé	• TJM >1100€→ **Filtrage initial par TJM max**
Prestataire sous-qualifié	Analyse insuffisante	Faible/Moyen	🟠 Moyen	• Aucun Lead Auditor/Implementer→ **Exiger 1 certif min + références SaaS**

Risque	Impact	Proba-bilité	Niveau	Indicateur / Prévention
Dépendance forte	Coûts récurrents élevés	Moyen	Moyen	• Beaucoup d'ateliers non transférés **Inclure transfert compétence obligatoire**
Planning prestataire non tenu	Décalage global	Faible	Faible/Moyen	• Retard >1 semaine début mission **Clauses planning dans devis**

D. Risques budgétaires

Risque	Impact	Proba-bilité	Niveau	Indicateur / Prévention
Sous-estimation Phase 3	+5k à +20k €	Élevé	Élevé	• Beaucoup de risques "Élevés" dans analyse **Prioriser P1/P2 et reporter P3**
Sous-estimation coûts certification	+2 à +5k €	Moyen	Moyen	• Certif affichée "trop vague" **Valider coûts avec 1 certificateur dès Phase 1**
Mesures techniques coûteuses	Investissement non prévu	Moyen	Élevé	• CI/CD ou IAM non maîtrisés **Audit initial CI/CD optionnel Phase 1**

E. Risques planning

Risque	Impact	Probabil-ité	Niveau	Indicateur / Prévention
Retard Phase 2	Décalage planning	Moyen	Élevé	• Besoins internes pas prêts **Préparer actifs/SaaS avant signature**
Retard Phase 3	Glissement 2–6 mois	Moyen/Élevé	Élevé	• Trop de mesures "majeures" P2/P3 **Limiter scope ISO 27002 Year 1**
Audit repoussé	Décalage certification	Faible/Moyen	Moyen	• Certificateur pas disponible **Bloquer un créneau 3 mois en avance**

F. Risques techniques

Risque	Impact	Proba-bilité	Niveau	Indicateur / Prévention
Volume d'actifs sous-estimé	Analyse plus longue	Élevé	Élevé	• Liste >150 actifs **Inventaire détaillé Phase 1**
CI/CD plus complexe que prévu	Retards & budget	Moyen	Moyen	• Beaucoup de runners/secrets **État des lieux CI/CD pré-mission**
Dépendance SaaS non évaluée	Révision périmètre	Moyen	Moyen	• Permissions SaaS floues **Lister roles/permissions Google/GitHub**

G. Risques réglementaires

Risque	Impact	Probabilité	Niveau	Indicateur / Prévention
Changements RGPD	Travaux non prévus	Faible/Moyen	Faible/Moyen	• Suivi CNIL faible **Veille RGPD trimestrielle**
Évolution ISO 27001	Adaptation mineure	Faible	Faible	• Version 2022 déjà récente Aucun besoin particulier

---

H. Risques gouvernance

Risque	Impact	Probabilité	Niveau	Indicateur / Prévention
Sponsoring direction insuffisant	Projet ralenti	Faible/Moyen	Moyen	• Décisions >2 semaines **Point direction fixe mensuel**
Mauvaise communication interne	Résistance / lenteur	Moyen	Moyen	• Feedback devs négatif **Kickoff interne du projet**

Top 5 risques + indicateurs

1. **Périmètre trop large** Indicateur : >150 actifs / trop de SaaS / périmètre flou
2. **Charge interne insuffisante** Indicateur : disponibilité <0,5 j/semaine
3. **Explosion Phase 3** Indicateur : trop de mesures P2/P3 dans l'analyse
4. **Sous-estimation complexité CI/CD & IAM** Indicateur : secrets non maîtrisés / nombreux pipelines
5. **Prestataire inadéquat** Indicateur : pas de certifs, pas de références SaaS

Annexe B. Glossaire Certifications Techniques

A. Certifications Offensives (Pentest / Red Team)

Certif	Domaine	Niveau	Notes
OSCP (Offensive Security Certified Professional)	Pentest	Intermédiaire	Très répandue
OSWE (Web Expert)	Pentest web avancé	Très élevé	Exploitation de code
OSEP (Evasion)	Pentest avancé	Très élevé	Contournement défenses
OSCE3	Expert	Extrêmement élevé	Combo OSEP/OSWE/OSEE
eWPTX	Pentest web avancé	Élevé	Web apps complexes
GPEN	Pentest réseau	Intermédiaire	SANS Institute

B. Certifications Cloud & Sécu Infra

Certif	Domaine
AZ-500	Sécurité Microsoft Azure
AWS Security Specialty	Sécurité AWS
GCIA	Analyse réseau
GCIH	Réponse à incident

C. Certifications Gouvernance / Management

Certif	Domaine
ISO 27001 Lead Implementer	Mise en place SMSI
ISO 27001 Lead Auditor	Audit ISO
CISSP	Gouvernance sécurité
CISM	Management sécurité

D. Certifications Web / AppSec

Certif	Domaine
GWEB	Sécurité applications web (SANS)
GWAPT	Pentest web (SANS)
CSSLP	Développement sécurisé

✅ Annexe C. Tableau Consolidé des Prestataires (Pentest, Audit, ISO, Red Team, Bug Bounty)

Prestataires Pentest & Audit Applicatif

Prestataire	Site Web	PASSI	Certifs disponibles	Spécialités	TJM estimé	Notes
Vaadata	vaadata.com	✅	OSCP, eWPTX	Pentest web, mobile	600–900 €	Bon ratio prix/qualité
Connect3S	pentest-nice.fr	✅	OSCP, OSWE, GWAPT	Pentest à distance	700–950 €	Très axé web
SSHack	sshack.me	✅	OSCP, OSEP	Web/API, infra	700–900 €	Experts indépendants
Intuity	intuity.fr	✅	OSCP	Web, mobile, phishing	650–850 €	Label France Cybersecurity
AlgoSecure	algosecure.fr	✅	OSCP	Pentest + audit org	600–850 €	Prestataire polyvalent
CAEIRUS	caeirus.com	✅	OSCP	Web/API, méthodo ANSSI	700–900 €	PME FR

Prestataire	Site Web	PASSI	Certifs disponibles	Spécialités	TJM estimé	Notes
SysDream	sys-dream.com	**PASSI**	OSCP, OSWE, GWAPT	Pentest web/mobile/API	950–1 200 €	Acteur historique
Wavestone	wave-stone.com	**PASSI**	OSCP, OSWE	Pentest, audit app	1 000–1 500 €	Cabinet corporate
Akyl	akyl.fr		OSCP	Pentest, 360° cyber	600–900 €	Bon sur PME
Ziwit (HTTPCS)	ziwit.com		CEH/OSCP	Pentest automatisé / SaaS	600–900 €	Beaucoup d'outillage
Heliaq	heliaq.fr		OSCP	Pentest web & API	700–900 €	Structure jeune
ACG Cybersecurity	acgcybersecu-rity.fr		OSCP/OSEP	Web, infra	700–900 €	Bon rapport qualité
Synacktiv	synacktiv.com	**PASSI**	OSWE, OSEP, GREM	Pentest avancé / R&D	1 000–1 500 €	Niveau expert ++
SEC-IT	sec-it.fr		OSCP	Pentest web / mobile	700–900 €	PME FR
Amossys	amossys.fr	**PASSI**	OSCP, CEH	Pentest + audits infra	1 000–1 300 €	Très haut niveau
Intrinsec	intrinsec.com	**PASSI**	OSCP/OSWE	Pentest + red team	1 000–1 400 €	Réf. TIBER-FR
BSSI	bssi.fr		OSCP/OSEP	Pentest web/infra	700–950 €	Très solide
XMCO	xmco.fr	**PASSI**	OSCP, OSWE	Pentest & vulnérabilités	1 000–1 300 €	Référence FR

Prestataires Audits Infrastructure & Réseau

Prestataire	Site Web	PASSI	Services	Prix	Notes
Amossys	amossys.fr		Réseau, infra, AD	5–15 k€	Excellence technique
Wavestone	wavestone.com		Infra, segmentation	15–40 k€	Pour grandes structures
Orange CyberDefense	orangecyberde-fense.com		Infra, WiFi, firewall	20–60 k€	Industriel / OIV
I-Tracing	i-tracing.com		Infra + SOC	4–12 k€	Support opérationnel
Nomios	nomios.fr		Firewall, NAC, réseau	4–10 k€	Très orienté réseau
Exaprobe	exaprobe.com		Réseau, segmentation	5–12 k€	Expertise infrastructure
NBS System	nbs-system.com		Infra + hébergement	4–8 k€	Connaît bien les hébergeurs
SEC-IT	sec-it.fr		Réseau + WiFi	3–8 k€	Très adapté PME

Prestataires Audits Organisationnels / ISO 27001 / RGPD

Prestataire	Site Web	PASSI	Services	Prix	Notes
AlgoSecure	algosecure.fr	partiel	ISO, PSSI, org	7–15 k€	Très PME-friendly
Digitemis	digitemis.com		ISO, RGPD, gouvernance	10–25 k€	Bon rapport qualité
CyberSecura	cybersecura.com		ISO 27001, RGPD	5–20 k€	Conformité complète
Advensor	advensor.fr		ISO, audit org	8–20 k€	Accompagnement SMSI
Wavestone	wavestone.com	**PASSI**	ISO, RGPD, gouvernance	20–60 k€	Niveau corporate
ChapsVision	chapsvision.com		Audit org, conformité	10–30 k€	Groupe important

---

Prestataires Audit Active Directory / Azure AD

Prestataire	PASSI	Services	Prix	Notes
Synacktiv		Audit AD très avancé	15–30 k€	Techniques offensives
Amossys		AD, Azure AD	10–20 k€	Hardening complet
Intrinsec		AD, Azure AD, Tiering	12–25 k€	Réf. TIBER-FR
I-Tracing		AD + SOC	10–20 k€	Audit + exploitation

Prestataires Red Team

Prestataire	PASSI	Type	Prix	Notes
Synacktiv	Oui	Red team logique/physique	40–90 k€	Meilleur niveau FR
Intrinsec	Oui	Red team TIBER-FR	35–80 k€	Scénarios complexes
Orange CyberDefense	Oui	Social + logique + physique	40–120 k€	Industriel
Wavestone	Oui	Red team OIV	50–150 k€	Ministères

Bug Bounty / PTaaS

Prestataire	Site Web	Spécialité	Notes
YesWeHack	yeswehack.com	Bug bounty	Très reconnu UE
Yogosha	yogosha.com	PTaaS + bounty	Secteur public & privé

Annexe C. Template de mail pour selection prestataire

On pourrais prévoir une deadline ?

```
# **Objet : Demande d'information – Accompagnement Sécurité & Analyse des Risques**

Bonjour,
```

Je vous contacte dans le cadre d’un projet d’amélioration de la sécurité au sein de **Meilleure

Nous recherchons un prestataire capable de nous accompagner sur :

* une **analyse des risques complète** de notre système d’information,
* la **proposition d’une méthodologie adaptée** (ISO 27005, EBIOS RM ou hybride),
* la **production d’un plan d’action priorisé et opérationnel**,
* un **accompagnement** à la mise en œuvre des mesures retenues
  (nous ne recherchons pas un simple audit documentaire).

Périmètre concerné

* applications web (VueJS),
* API / backend Symfony,
* services SaaS utilisés,
* données manipulées,
* organisation interne.

Le périmètre final sera affiné lors du cadrage.

Livrables attendus

1. Inventaire des actifs
2. Analyse menaces / vulnérabilités
3. Évaluation des risques
4. Plan d’action priorisé
5. Accompagnement et ateliers
6. Synthèse exécutive
7. Restitution orale

Exigences minimales

* Au moins une certification : ISO 27001 Lead Implementer / Lead Auditor, CISSP, CISM, EBIOS RM
* Capacité d’accompagnement concret (recommandations, ateliers, support post-analyse).

Informations attendues dans votre réponse

1. Votre compréhension du besoin
2. Votre méthodologie
3. Vos livrables habituels
4. Votre capacité d’accompagnement
5. Certifications & compétences de l’équipe
6. Références (PME, SaaS, fintech)
7. Estimation du périmètre optimal
8. **Une indication budgétaire prévisionnelle** :

    * votre **TJM**,
    * et/ou une **fourchette indicative** pour une mission similaire
      (aucun devis formel n’est requis à cette étape)
9. Contraintes éventuelles

Processus de sélection

1. Analyse de votre réponse
2. Sélection de 2-3 prestataires
3. Échange visio (30-45 min)

```
4. Validation du périmètre final
5. Demande de devis
6. Sélection finale

Merci pour votre retour.
```

🔍 Annexe E - détail de la procédure d'audit avec l'organisme certifié

🔹 Pourquoi la Phase 1 est courte (1–2 jours)

Parce qu'elle ne vérifie **aucune pratique réelle**.

Elle sert à répondre à une seule question : 👉 *"Votre SMSI est-il suffisamment en place pour justifier un audit opérationnel (Phase 2) ?"*

L'auditeur ne cherche pas encore à vérifier si vous faites les choses, mais si vous avez :

- une politique sécurité,
- une description du périmètre,
- un registre de risques,
- un plan d'action,
- une gouvernance minimale (rôles, responsabilités),
- une revue de direction,
- un planning d'audit interne,
- des preuves initiales.

C'est pourquoi **un seul auditeur** suffit souvent, et **la visio** est largement suffisante.

🔹 Déroulé typique de la Phase 1

Durée : 0,5 à 2 jours — 100% documentaire.

1. **Réunion d'ouverture (visio)**
2. Présentation du périmètre
3. Vérification des documents obligatoires du SMSI
4. Vérification que l'analyse de risques existe et est cohérente
5. Vérification qu'il y a un cycle PDCA (même minimal)
6. Vérification que les contrôles de l'annexe A ont bien été adressés
7. Analyse des preuves documentaires (extraits, captures, modèles)
8. Points complémentaires
9. **Compte rendu — décision de passer en Phase 2 ou non**

Très souvent : 👉 *L'auditeur demande des preuves supplémentaires par email / dossier partagé.*

🔹 La Phase 2 : comment ça se passe vraiment ?

Durée : 2 à 5 jours, selon périmètre et maturité. Elle vérifie que **ce que vous déclarez, vous le faites réellement**.

Where ?

- sur site (souvent recommandé),
- en visio si l'entreprise est 100% SaaS / cloud / distancielle (assez fréquent aujourd'hui),
- parfois hybride (1 jour sur site + suite à distance).

Contenu typique

L'auditeur demande des preuves concrètes sur :

- la gestion des accès (ex : démonstration Google Workspace / Dashlane),
- la gestion GitHub (droits, MFA),
- les journaux (captures ou démos),
- les backups (preuve de restauration),
- les processus CI/CD,
- les preuves de sensibilisation,
- l'analyse de risques (preuve de mise à jour),
- la gestion des incidents,
- les revues régulières,
- les contrats SaaS (clauses sécurité).

Interlocuteurs

- CTO / dev senior pour la partie technique,
- direction pour la gouvernance,
- éventuellement dev / ops pour démonstration CI/CD.

Livrable final

- rapport Phase 2,
- liste des non-conformités (mineures / majeures),
- plan d'action de correction,
- décision du comité de certification.

Pourquoi certaines certifications sont obtenues en 3–4 jours ?

Parce que :

- beaucoup de PME ont un périmètre **réduit**,
- c'est le **SMSI**, pas la technique, qui est certifié,
- l'entreprise est souvent **100% SaaS** (pas de réseau interne, pas de firewall, pas de serveurs on-premise),
- une grande partie se valide **en visio**.

Une entreprise 100% SaaS (comme vous) a des audits significativement plus courts.

En résumé

- **Phase 1 = visio, documentaire, courte**
- **Phase 2 = démonstration, preuves, technique, plus longue**
- Déroulé très cadré et beaucoup plus simple qu'un audit technique.