FeelAgile

Guide 360°

ISO 27001

ISO 27001 – Le guide 360° pour piloter votre sécurité de l'information sans rigidité

Pourquoi ce guide?

Chez Feel Agile, nous avons un credo simple : "mettre de l'agilité dans la conformité."

L'ISO 27001 est souvent perçue comme un projet lourd, rigide, document-centré, réservé aux grands groupes. La réalité 2025 est tout autre :

- La certification **devient un standard attendu,** même pour des TPE/PME.
- Les exigences réglementaires (NIS2, appels d'offres, clients grands comptes) poussent de plus en plus d'organisations à se mettre au niveau.
- Les outils modernes (comme Oversecur) permettent désormais de piloter un **SMSI sans noyade documentaire.**

Cet e-book a un objectif :
Vous accompagner pas à pas, du "Est-ce que l'ISO 27001 est fait pour moi ?" jusqu'à "Comment maintenir la certification dans le temps sans y passer mes semaines ?"

Il s'adresse :

- Aux dirigeants qui veulent une vision claire, business et stratégique.
- Aux DSI / RSSI / responsables conformité qui doivent piloter le projet au quotidien.
- Aux équipes métiers qui craignent souvent un "projet ISO" lourd et théorique.

Sommaire

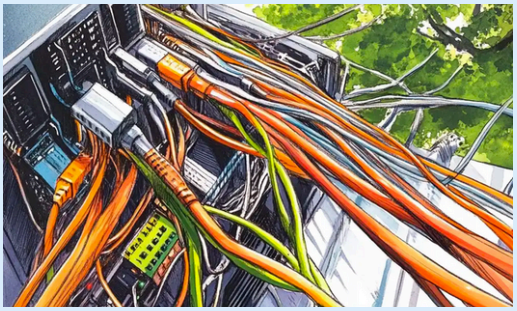
DÉCIDER

ISO 27001 est-il fait pour moi ?

01

FeelAgile

1.1 Est-ce que l'ISO 27001 est obligatoire dans mon cas ?



En 2026, la question n'est plus seulement *"Est-ce obligatoire ?"* mais plutôt :

- Mes clients l'attendent-ils ?
- Mes prospects le demandent-ils dans les appels d'offres ?
- Les nouvelles réglementations (NIS2, DORA) creusent-elles l'écart entre moi et mes concurrents ?

La directive NIS2 impose désormais des exigences renforcées en matière de cybersécurité pour les entreprises de secteurs critiques (santé, énergie, transport, services numériques). L'ISO 27001 devient un moyen reconnu de démontrer la conformité.

L'article **"Pourquoi la certification ISO 27001 va devenir obligatoire ?"** explique en détail :

- Le rôle de NIS2 et des réglementations sectorielles
- Pourquoi vos clients et partenaires font de l'ISO 27001 un prérequis implicite
- Comment l'absence de certification peut devenir un frein commercial majeur

Lire l'article "Pourquoi la certification ISO 27001 va devenir obligatoire ?"

1.2 Est-ce que ça vaut vraiment le coup ?

Beaucoup de dirigeants voient encore l'ISO 27001 comme un centre de coûts, alors qu'elle est en réalité un accélérateur de business, un cadre de structuration et un réducteur de risques. Elle ouvre l'accès à de nouveaux marchés, rassure vos clients, clarifie rôles et responsabilités, et limite l'impact financier des incidents de sécurité.

Le Guide du dirigeant met en évidence le ROI réel de l'ISO 27001, les gains commerciaux constatés et son effet sur la valorisation de l'entreprise.

Téléchargez le Guide du Dirigeant

Pour aller plus loin : Le webinaire Boostez votre chiffre d'affaires grâce à l'ISO 27001

1.3 Sommes-nous vraiment prêts pour ISO 27001 ?

Beaucoup d'entreprises pensent "On n'est pas prêts...", alors qu'elles sont souvent plus avancées qu'elles ne le croient.

Les signaux de maturité :

- Vous avez déjà des politiques de sécurité (même informelles)
- Vous gérez vos accès utilisateurs de manière structurée
- Vous faites des sauvegardes régulières
- Vous sensibilisez vos équipes à la cybersécurité

Mesurez la maturité de votre organisation avec notre **auto-diagnostic ISO 27001** .

Faites votre Autodiagnostic ISO 27001

1.4 Combien ça coûte vraiment ?

Le coût d'un projet ISO 27001 dépend de trois facteurs principaux :

1. **Votre taille** (TPE, PME, ETI, grand groupe)
2. **Votre niveau de maturité** de départ
3. **Votre mode d'accompagnement** (interne, externe, mixte)

L'article **"Coûts et durée d'une certification ISO"** détaille :

- Les coûts d'accompagnement selon les approches
- Les coûts d'audit (initial et de surveillance annuelle)
- Les ressources internes mobilisées (temps, profils, charge)
- Les coûts cachés à anticiper (formations, outils, consultants ponctuels)

Lire l'article "Coûts et durée d'une certification ISO"

CHOISIR

Bien démarrer votre projet ISO 27001

02

2.1 Le principal risque : mal démarrer

Les erreurs classiques qui font dérailler les projets ISO 27001 :

- **Choisir un prestataire inadapté :** Un consultant qui ne connaît pas votre secteur, votre taille ou votre culture d'entreprise va imposer une méthode standardisée inadaptée.
- **Adopter une approche trop documentaire :** Produire 150 documents Word sans lien avec les pratiques réelles de l'entreprise. Résultat : un système qui existe "sur le papier" mais pas dans les faits.
- **Sous-estimer la dimension projet :** Absence de gouvernance, pas de priorisation, pas de jalons clairs. Le projet s'éternise et les équipes se démotivent.
- **Ne pas impliquer les bonnes personnes :** Laisser le projet uniquement entre les mains du DSI ou du RSSI, sans sponsoring direction et sans implication métiers.

> **"80% des projets ISO 27001 qui échouent ou dérapent souffrent d'un problème de méthode, pas de compétence technique."**

Dans ce chapitre, nous vous proposons des clés pour bien démarrer votre de projet de certification ISO 27001.

2.2 Comment choisir son accompagnement ISO 27001 ?

L'accompagnement est un **facteur critique de réussite** : un projet mal cadré génère retards, surcharges internes et coûts imprévus. Un bon prestataire apporte une **expertise pluridisciplinaire** (juridique, cybersécurité, organisation), une **méthode de projet claire** et un **SMSI maintenable**, adapté à votre réalité.

Ce que doit apporter un bon prestataire

- Comprendre l'esprit de la norme (pas seulement cocher des cases)
- Cadrer le projet : périmètre, délais, budget, maturité de départ
- Adapter la démarche à votre contexte (PME, ETI, secteur réglementé)
- Préparer l'audit : revue documentaire, audit blanc, choix de l'organisme certificateur

Un prestataire solide joue à la fois le rôle d'expert et de chef de projet, avec une approche opérationnelle concrète.

Pour aller plus loin :

- **Comment choisir son prestataire (1/2)** – Enjeux, ROI et leviers stratégiques
- **Comment choisir son prestataire (2/2)** – Types de prestataires et critères de sélection

2.3 A quoi ressemble un projet ISO 27001 en 2025 ?

Un projet ISO 27001 aujourd'hui, ce n'est plus :

- ❌ 150 documents Word dispersés
- ❌ 10 dossiers partagés sans cohérence
- ❌ 20 tableurs Excel à mettre à jour manuellement

C'est :

- **Une approche agile :** Itérative, orientée usage. On commence par les risques critiques et les exigences à plus forte valeur, puis on étend progressivement.
- Un pilotage outillé : Tableaux de bord centralisés, indicateurs en temps réel, workflows automatisés. La plateforme Oversecur permet de piloter votre SMSI comme un véritable projet.
- Une documentation utile : Au service des pratiques réelles. On documente ce qui est fait, pas ce qui devrait être fait. La documentation devient un outil opérationnel, pas un monument bureaucratique.

La vidéo **"Les approches et solutions actuelles"** présente ces nouvelles façons de faire, avec des démonstrations concrètes et des retours d'expérience.

Regarder la vidéo "Comment faire ISO 27001 en 2025 ? Approches & solutions actuelles"

Réussir sa certification sans s'épuiser

03

3.1 Les causes d'échec les plus fréquentes

Les projets qui s'épuisent partagent les mêmes symptômes :

- **Manque de méthode :** Tout est urgent, rien n'est priorisé. Les équipes courent dans tous les sens sans vision claire de l'avancement.
- **Manque de pilotage :** Pas de visibilité sur l'état d'avancement, pas de jalons formalisés, pas de gestion des risques projet. On découvre les problèmes trop tard.
- **Approche trop théorique :** La conformité devient une fin en soi, déconnectée du business. Les équipes métiers ne voient pas l'intérêt et résistent passivement.
- **Perfectionnisme paralysant :** Vouloir tout documenter parfaitement dès le premier coup. Résultat : le projet n'avance jamais.
- **Sous-estimation de la conduite du changement :** On oublie que l'ISO 27001 implique des changements d'habitudes, de processus, de responsabilités. Sans accompagnement humain, la résistance est forte.

> **Selon nos observations, 60% des projets ISO 27001 dépassent leur délai initial de plus de 6 mois, principalement par manque de méthode et de priorisation.**

3.2 Une méthode pour aller vite et bien

Le webinaire **"Obtenir ISO 27001 en moins de 6 mois"** présente la méthode développée par Feel Agile, qui a accompagné plus de 200 organisations à décrocher leur certification sans alourdir les équipes ni freiner les projets en cours.

- **Le défi :** obtenir la certification rapidement tout en évitant la bureaucratie, les procédures complexes et la surcharge interne.
- **La solution :** une approche agile et pragmatique qui allège la charge des équipes, instaure un système de sécurité réel (pas du "document pour le document"), et garantit l'obtention de la certification dans les délais.
- **L'objectif :** accélérer sans sacrifier la qualité, en éliminant les tâches à faible valeur et en préservant vos équipes d'un rythme insoutenable.

Webinaire : Obtenir ISO 27001 en moins de 6 mois
- Avec témoignages concrets et plan d'action applicable

PILOTER

Les bons outils pour piloter efficacement

04

4.1 Le problème des fichiers dispersés

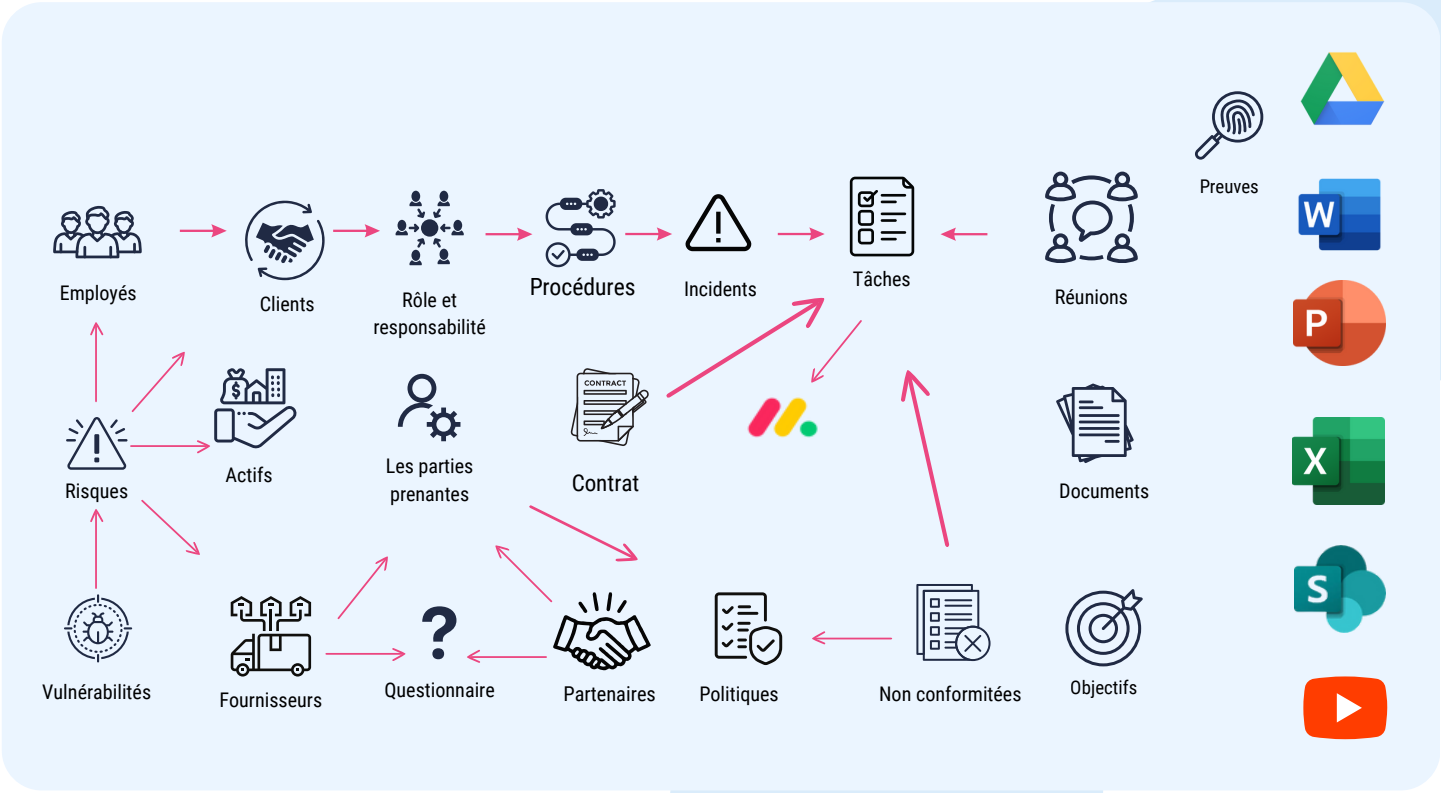
Un SMSI piloté uniquement avec des fichiers Word, Excel et des mails finit tôt ou tard par :

Perdre en fiabilité
Versions multiples qui circulent, erreurs de mise à jour, informations contradictoires. Impossible de savoir quelle est la version valide.

Générer de la lassitude
Mise à jour manuelle pénible, duplication des informations, recherche chronophage. Les équipes passent plus de temps à maintenir les fichiers qu'à améliorer la sécurité.

Complexifier les audits
Recherche d'information difficile, preuves dispersées, difficulté à démontrer la traçabilité. Les auditeurs passent des heures à reconstituer le puzzle.

Limiter la visibilité
Impossible d'avoir une vue d'ensemble en temps réel. Les indicateurs sont calculés manuellement avec plusieurs jours de retard.



4.2 Oversecur : un cockpit pour votre ISO 27001

Oversecur est la plateforme GRC (Governance, Risk & Compliance) développée par Feel Agile pour centraliser et automatiser la gestion de votre SMSI.

Fonctionnalités clés

- **Cartographie des risques :** Identifiez les données sensibles, les supports qui les traitent, et les mesures de protection déjà en place. Évaluez les risques réels avec précision.
- **Gestion des plans d'actions :** Définissez les plans de traitement des risques, assignez les responsables, suivez l'avancement en temps réel avec des indicateurs clairs.
- **Centralisation des preuves :** Toutes les preuves de conformité sont centralisées et accessibles en un clic. Moins de stress pendant les audits, tout est prêt à présenter.
- **Tableaux de bord en temps réel :** Visualisez vos indicateurs (non-conformités, incidents, audits internes) avec des vues adaptées aux dirigeants, équipes opérationnelles et auditeurs.
- **Traçabilité complète :** Chaque décision est validée par les propriétaires de risques, avec historique complet et traçabilité des actions.

Les webinaires et vidéos sur Oversecur montrent des démonstrations concrètes de la plateforme en action.

Démo

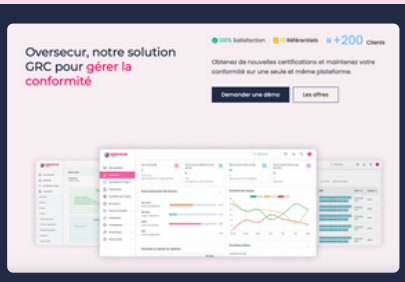
Piloter ISO 27001 avec Oversecur

Voir la démo

Playlist complète

Passer ISO 27001 en 10 vidéos avec Oversecur

Accéder à la playlist



Page produit

Découvrir Oversecur et nos offres

En savoir plus

FeelAgile

STRUCTURER

Une documentation utile

05

5.1 La documentation : peur légitime, erreurs fréquentes

La documentation **est une des premières cause de non-conformités en audit** ISO 27001. Pas à cause de la technique, mais à cause d'erreurs évitables : documents obsolètes, versions multiples, décalage entre ce qui est écrit et ce qui est appliqué.

Les pièges les plus fréquents :

- Utiliser des modèles "prêt à l'emploi" sans adaptation
- Gérer la doc de manière éclatée (Excel, SharePoint, Drive...)
- Écrire pour l'auditeur au lieu des utilisateurs
- Surproduire (150 documents inutiles) ou sous-documenter

L'article **"Les erreurs fréquentes en documentation ISO 27001"** vous révèle ce que les auditeurs attendent vraiment, les pièges à éviter et comment structurer une documentation audit-ready

Lire l'article "Les erreurs fréquentes en documentation ISO 27001"

5.2 Construire une documentation utile, cohérente, opérationnelle

Le **Guide de la documentation ISO 27001** transforme la conformité documentaire en levier stratégique plutôt qu'en fardeau administratif.

Ce que contient le guide :

- Les 6 documents obligatoires ISO 27001 et leur raison d'être
- La structure documentaire efficace (niveaux, processus, responsabilités)
- La maîtrise du cycle de vie (création, validation, mise à jour, archivage)
- La feuille de route pour un système documentaire conforme et vivant
- La checklist pratique pour éviter les erreurs qui coûtent cher en audit

Ce guide vous donne les méthodes concrètes pour réussir et accélérer votre documentation.

Téléchargez le Guide de la documentation ISO 27001

ORGANISER ET GOUVERNER

Organisation, rôles et conformité

06

6.1 Quand le projet devient transverse

Dans les ETI et organisations multi-métiers, l'enjeu n'est pas uniquement technique. Il devient :

- **Humain :** Obtenir l'adhésion des équipes qui voient souvent l'ISO 27001 comme une contrainte supplémentaire. Comment embarquer les métiers ?
- **Organisationnel :** Définir les rôles (RSSI, DPO, propriétaires de risques, sponsors), créer les comités de pilotage, organiser les revues régulières.
- **Politique :** Arbitrer les priorités, allouer les budgets, gérer les résistances internes, obtenir le sponsoring de la direction générale.

Sans gouvernance claire, le projet ISO 27001 devient un "projet du DSI" que personne ne s'approprie vraiment.

> **Dans les organisations de plus de 100 personnes, le sponsoring de la direction générale est le facteur #1 de réussite d'un projet ISO 27001**

6.2 Structurer un SMSI dans une ETI

Le **Guide ISO 27001 spécial ETI** montre comment faire de l'ISO 27001 un **levier de croissance**, en l'alignant sur vos enjeux business et votre gouvernance existante, plutôt qu'un énième projet de conformité. Il explique comment intégrer le SMSI dans vos comités, vos processus et vos outils actuels, en clarifiant les rôles (direction, RSSI, métiers, IT) et les règles du jeu.

Vous y trouverez une méthode pas-à-pas pour bâtir une feuille de route, implémenter le système de management, préparer la certification puis organiser le maintien et l'amélioration continue dans la durée.

Téléchargez le Guide ISO 27001 spécial ETI

MAINTENIR ET AUTOMATISER

L’après-certification

07

7.1 Ma certification ISO 27001 est-elle définitive ?

Réponse courte : non.

La certification ISO 27001 suit un cycle de 3 ans avec des audits réguliers.

L'article **"Ma certification ISO 27001 sera-t-elle définitive ?"** explique :

- Le fonctionnement des audits de surveillance
- Les exigences de maintien entre chaque audit
- Les pièges à éviter pour ne pas perdre le bénéfice de la certification
- Comment préparer sereinement les audits de surveillance

Lire l'article "Ma certification ISO 27001 sera-t-elle définitive ?"

7.2 Automatiser et industrialiser le maintien

Le webinaire **"Automatisez vos certifications ISO"** montre comment maintenir votre certification sans surcharge : génération automatique de documents, rappels pour les revues, collecte de preuves, tableaux de bord en temps réel.

Avec Oversecur :
Workflows automatisés, centralisation des preuves, pilotage des audits de surveillance et gestion des non-conformités.

Voir le replay : "Automatisez vos certifications ISO"

Pour aller plus loin : Découvrir Oversecur et nos offres

Et pour finir...vos questions, nos réponses

Les FAQ vidéo (2 heures chacune) répondent aux questions les plus fréquentes sur la conduite de projet ISO 27001 :

- **Quel périmètre choisir ?** Faut-il certifier toute l'entreprise ou un périmètre restreint ? Comment définir un périmètre cohérent et défendable auprès des auditeurs ?
- **Suis-je éligible ?** Toutes les entreprises peuvent-elles se certifier ? Y a-t-il des prérequis de taille, de maturité ou de secteur ?
- **Comment se déroulent les audits ?** Durée, déroulement, pièges à éviter. Comment bien préparer son audit de certification ?
- **Comment gérer les risques ?** Méthodes d'appréciation des risques , plans de traitement.
- Comment organiser la gouvernance ? Rôles et responsabilités, comités, fréquence des revues, indicateurs de pilotage.
- **Comment intégrer l'IA au pilotage de mon SMSI ?** Quels liens entre ISO 27001 et ISO 42001 ?

Et bien plus de questions ainsi que toute nos réponses.

Ask the expert

FAQ ISO 27001

Voir la vidéo

Ask the expert

ISO 27001 à l'ère de l'IA

Voir la vidéo

CONCLUSION

Nos services

08

Pourquoi FeelAgile ?

Assurer sa conformité ISO 27001 avec FeelAgile : une expertise certifiée, des outils agiles, et des résultats garantis. FeelAgile est le leader des certifications ISO en France avec plus de 200 entreprises certifiées et accompagnées.

- Une garantie d'être certifié à 100%
- Une combinaison d'expertises cybersécurité, juridique et organisationnelle
- Des solutions d'automatisation
- Une équipe support
- Des financements
- Une approche agile des certifications, sur mesure

Feel Agile

ACCOMPAGNEMENT CONFORMITÉ

3 Formules d'accompagnement adaptées à votre maturité

PLAN
Classique

Certification en **Mois** **12**

- Chef de projet dédié et ateliers de travail hebdomadaire
- COPIL mensuel
- E-learning
- Modèles documentaires
- Audit blanc
- Assistance documentaire
- Passage de l'audit de certification
- Responsable du SMSI

PLAN
Full

Certification en **Mois** **10**

- Chef de projet dédié et ateliers de travail hebdomadaire
- COPIL mensuel
- E-learning
- Modèles documentaires
- Audit blanc
- Assistance documentaire
- Passage de l'audit de certification
- Responsable du SMSI

PLAN
Externalisé

Certification en **Mois** **6 à 8**

- Chef de projet dédié et ateliers de travail hebdomadaire
- COPIL mensuel
- E-learning
- Modèles documentaires
- Audit blanc
- Assistance documentaire
- Passage de l'audit de certification
- Responsable du SMSI

★★★★★

Grâce à Feel Agile, nous avons réussi à obtenir la certification ISO 27001 sans aucune non-conformité, ce qui est un exploit rare.

Julien Cassagnabère - RSSI

RGPD · ISO 9001 · NIS2 · ISO 27001 · HDS · DORA · SECNUM CLOUD · SOC2 · ISO 13485 · ISO 42001 · ISO 27018 · ISO 27017 · TISAX

FeelAgile
LEARNING

FORMATIONS & SENSIBILISATION

Plateforme de sensibilisation

Sécurité de l'information
2h - 16 modules au choix

Sensibilisation au RGPD
1h30 - 7 modules

Données de santé pour HDS
1h - 8 modules

Normes, labels et réglementations
30 min - 3 modules au choix

Plateforme d'e-learning

10h
de formation

44
Modules vidéos

Formations certifiantes PECB

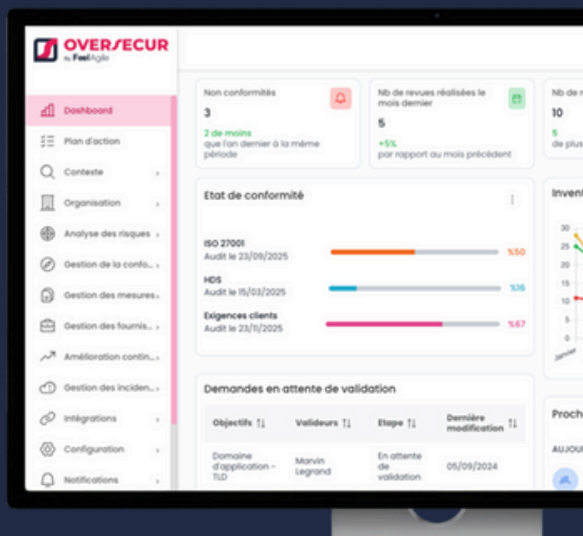
ISO 27001
ISO 27701
ISO 42001
ISO 22301

ISO 27005
ISO 31000
ISO 9001

PECB
AUTHORIZED
PARTNER

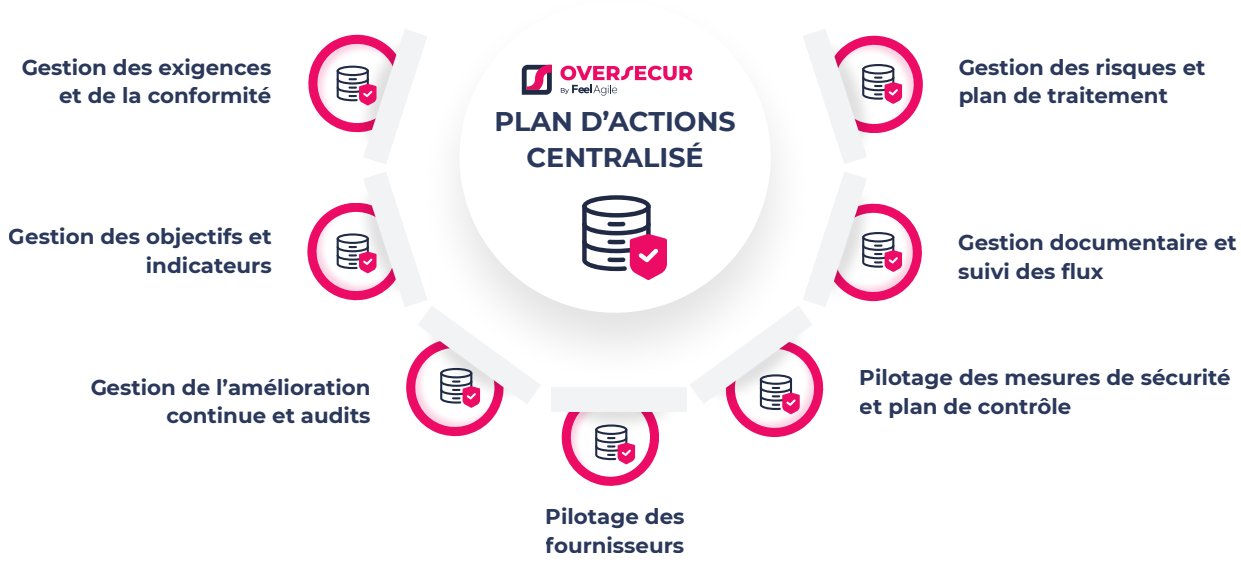
OVERSECUR
By FeelAgile

L'EXCELLENCE GRC EN TOUTE SÉCURITÉ



Un seul outil pour piloter vos risques, conformité et cybersécurité

Logique SMSI intégrée



★★★★★

OVERSECUR a été un outil clé pour travailler et présenter notre implémentation du SMSI à l'auditeur. La centralisation des informations et la navigation simplifiée sont très pratiques. Le plan d'action met en avant le travail réalisé dans la durée avec un suivi clair de l'avancement. L'auditeur a émis un avis très positif sur l'outil.

-Anh Nguyen-Phuoc - CISO de SCALITY

12 RÉFÉRENTIELS CONSTAMMENT MIS À JOUR PAR NOTRE ÉQUIPE D'EXPERTS

RGPD · ISO 9001 · NIS2 · ISO 27001 · HDS · DORA · SECNUM CLOUD · SOC2 · ISO 13485 · ISO 42001 · ISO 27017 · TISAX

FeelAgile

VOTRE CYBERSÉCURITE

ÉVALUER & DÉTECTER

Diagnostic cyber

Audits de sécurité

Test d'intrusion (pentest)

Test de phishing

SÉCURISER & PROTÉGER

Sécurisation postes de travail (EDR, antivirus)

Sécurisation réseaux (firewall, VPN, NAC)

Gestion de crises (PCA/PRA)

Déploiement SOC

FeelAgile

Leader de l'ISO 27001

Votre partenaire expert pour une conformité agile et durable

EXPERTISE EN CERTIFICATION

20 ans

PASSÉS DANS LES ORGANISATIONS

16 Experts cyber, chefs de projet 27001, auditeurs

+ de 200 projets 27001

FeelAgile

Des services externalisés pour vos certifications ou votre conformité

FeelAgile OVERSECUR

Une plateforme SaaS pour vos certifications

FeelAgile LEARNING

Sensibilisations et formations pour vos collaborateurs

Certifié et reconnu par les meilleurs acteurs

afaq ISO 27001 Sécurité de l'information AFNOR CERTIFICATION

Qualiopi processus certifié RÉPUBLIQUE FRANÇAISE La certification qualité a été délivrée au titre de la catégorie d'action suivante : ACTIONS DE FORMATION

PECB AUTHORIZED PARTNER

numeum

CAMPUS CYBER

HEXATRUST CLOUD CONFIDENCE & CYBERSECURITY

FeelAgile

Restons en contact !

Alexis Schuhmacher, Directeur Commercial

+33 6 34 42 67 08

aschuhmacher@feelagile.com

@alexisschuhmacher

https://feelagile.com/

Prendre rendez-vous

FeelAgile est le **leader des certifications** ISO 27001 en France avec **plus de 200 entreprises certifiées** et accompagnées.