

Guide Cyber et croissance

Faire de la cybersécurité un
avantage concurrentiel



Cyber et croissance



Les dirigeants savent que la cybersécurité est un sujet important.
Mais beaucoup n'en ont qu'une lecture court terme, souvent technique, parfois subie.

Ils voient le risque.

Mais pas la trajectoire.

Ils perçoivent la pression.

Mais pas les leviers à mobiliser.

👉 Résultat : des décisions fragmentées, des actions réactives, des investissements sans cap.

Ce qui manque, ce n'est pas la prise de conscience.

C'est la vision stratégique, la connaissance 'axes clés et la capacité à prioriser.

Ce guide vise justement à réconcilier l'urgence opérationnelle avec la construction d'un socle durable : cybersécurité, conformité et certification comme pilier de votre performance à 3 ans.

Sommaire

Stratégie de conformité et certification

01 Tendances de la cybersécurité



02 Pourquoi et comment y aller ?



03 Les erreurs à ne pas faire



04 Notre approche



05 Services pour aller plus loin



LES TENDANCES

Comprendre la cybersécurité



La cybersécurité en 2025

Du château au réseau

La cybersécurité en 2025 ne se limite plus à se défendre contre les attaques : elle devient une capacité stratégique. Fini le modèle du château fort ; aujourd'hui, l'enjeu est de protéger un système distribué, interconnecté, intelligent. Il faut garantir la disponibilité, l'intégrité, la confidentialité, mais aussi la résilience, la continuité et la souveraineté numérique. L'entreprise doit limiter ses dépendances critiques, encadrer l'usage de l'intelligence artificielle et être capable d'apporter la preuve de sa conformité et de ses actions. La cybersécurité devient ainsi un levier de compétitivité, d'autonomie et de confiance.

DISPONIBILITÉ

Assurer l'accès aux services et aux données au moment attendu, sans interruption.

RÉSILIENCE

Savoir encaisser un incident et redémarrer rapidement sans perte critique.

INTÉGRITÉ

Garantir que les données et les systèmes ne sont ni altérés ni corrompus.

CONTINUITÉ

Maintenir les activités essentielles même en cas de crise ou de cyberattaque.

CONFIDENTIALITÉ

Protéger les informations sensibles contre tout accès non autorisé.

SOUVERAINETÉ

Garder le contrôle stratégique de ses données, de ses technologies et de ses prestataires.

AUTONOMIE / DÉPENDANCE

Réduire les points de dépendance à des tiers, surtout extra-européens.

PREUVE

Être en capacité de démontrer sa conformité, sa maîtrise des risques et ses actions de sécurité.

Comprendre et répondre à ces composantes vous positionne en leader de confiance, capable de scaler durablement dans un monde numérique exigeant, où la sécurité, la résilience et la souveraineté sont devenues des critères de sélection business autant que des enjeux stratégiques.

Un changement de paradigme



Passage à une cybersécurité de masse

Le paradigme de la sécurité évolue profondément.

Avec la directive NIS 2, ce ne sont plus seulement les grands acteurs ou les opérateurs critiques qui sont visés : toutes les entreprises du numérique sont concernées, directement ou par effet de chaîne. En parallèle, les contrôles RGPD se renforcent, les attaques se multiplient, et les exigences clients explosent.

Aujourd'hui, la sécurité n'est plus perçue comme un simple coût ou une contrainte technique, mais comme un gage de qualité, de fiabilité et de maturité opérationnelle. Dans un contexte géopolitique incertain et sous tension, la souveraineté numérique devient un enjeu de compétitivité.

Les certifications comme ISO 27001, HDS, SecNumCloud, ou SOC 2 deviennent progressivement incontournables pour accéder aux marchés, sécuriser la confiance des clients, et anticiper les obligations réglementaires.

En 2025, ne pas intégrer la cybersécurité à sa stratégie d'entreprise, c'est prendre le risque d'être exclu — en amont — des opportunités les plus porteuses.

On entend souvent : "Nous allons mettre en place une certification ISO 27001."

Mais en réalité, cette formulation est incorrecte... et potentiellement trompeuse.

On ne "met pas en place une norme".

Ce que l'on met en place, c'est un système de management de la sécurité de l'information (SMSI) conforme aux exigences de la norme ISO/IEC 27001. (rôles, processus, outils, pilotage ...)

Autrement dit : une organisation structurée et pilotée, en amélioration continue — capable d'assurer la sécurité des informations critiques pour l'entreprise et ses parties prenantes.

Les objectifs

Passage à une cybersécurité stratégique

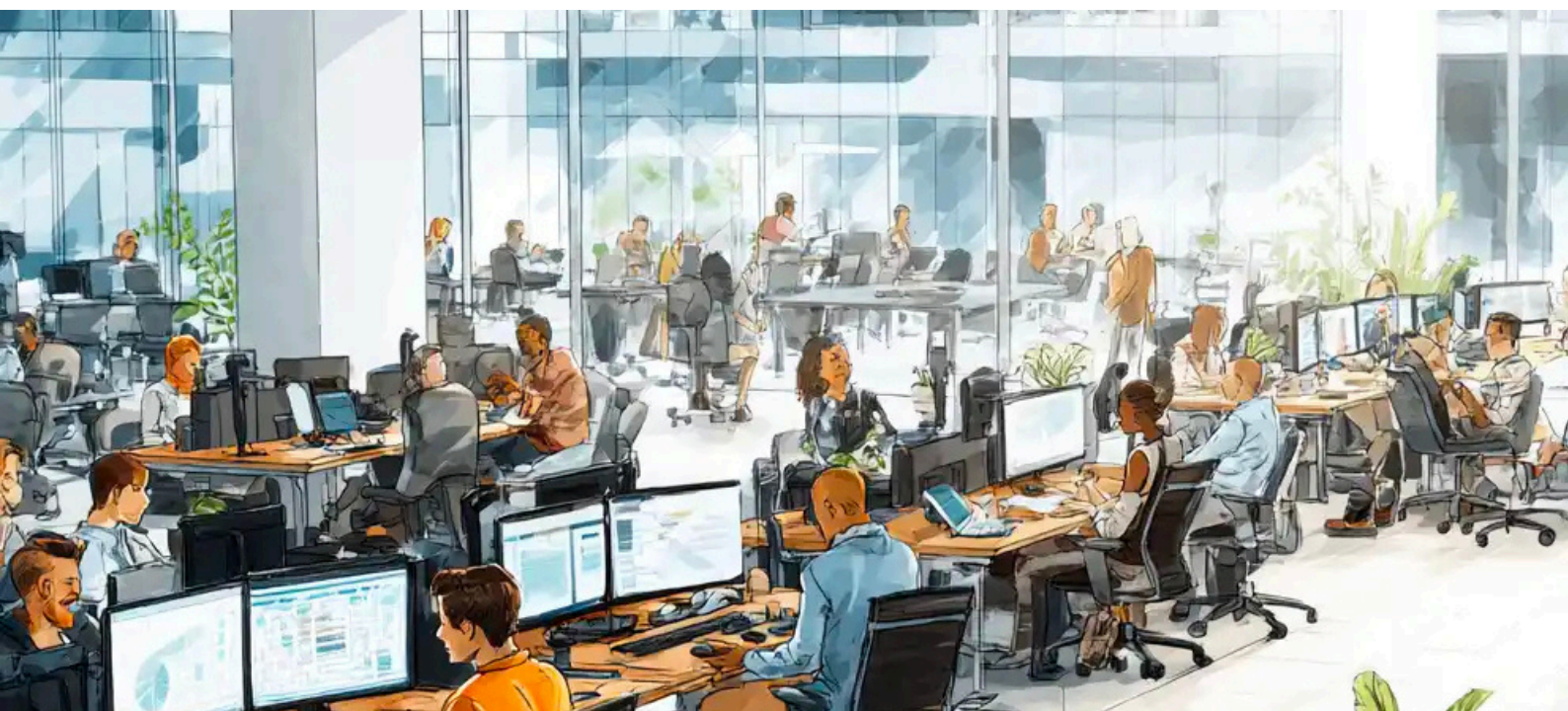
Quel que soit votre secteur, même pour les acteurs de l'IT, la cybersécurité peut être un avantage stratégique.

L'objectif est de se positionner sur 3 volets :

- une cybersécurité réellement maîtrisée et pilotée
- une conformité agile
- une certification bien pensée et bien maintenue

Je vais essayer dans ce guide de vous donner :

- Les erreurs à ne pas faire dans votre démarche de cybersécurité
- les repères pour avancer de façon pragmatique et efficace dans chacun de ces objectifs
- Notre méthode et nos outils



AVANTAGES ET RISQUES

Pourquoi et comment y aller ?



Si on ne fait rien

Ne rien faire en matière de cybersécurité, c'est prendre le risque de tout perdre sans s'en rendre compte.

Aujourd'hui, une simple négligence peut entraîner une attaque, une perte de données, ou l'exclusion silencieuse d'un marché.

Pendant que certains subissent, d'autres investissent et transforment la sécurité en avantage concurrentiel. Les conséquences sont réelles, visibles, et déjà à l'œuvre.

1. Conséquences directes d'une attaque

- Perte de données critiques ou confidentielles (clients, contrats, R&D...). Perte opérationnelle.
- Chiffre d'affaires en chute suite à l'interruption d'activité

2. Perte de confiance des clients et partenaires

- Rupture de contrats en cours
- Clients qui basculent chez des prestataires jugés plus fiables
- Image publique durablement abîmée

3. Perte d'accès aux marchés stratégiques

- Écarté d'appels d'offres pour absence de certification (ISO 27001, HDS...). Certaines entreprises se font écartées sans même le savoir.
- Non-conformité réglementaire : RGPD, NIS 2, DORA, etc.
- Blocage à l'export ou avec des grands comptes

4. Avantage laissé aux concurrents

- Ceux qui investissent obtiennent des certifications de sécurité reconnues

Ils deviennent les partenaires de confiance pour les grands groupes.

- Ils s'imposent sur les marchés où la conformité est un critère

5. Sanctions juridiques et financières

- Amendes RGPD (jusqu'à 4 % du CA mondial)
- Responsabilité civile ou pénale du dirigeant en cas de négligence
- Frais de justice, d'expertise, d'assistance technique...

Exemple : Clearview AI condamnée à 20 millions d'euros d'amende par la CNIL

Les avantages

Mettre en place une véritable démarche de cybersécurité et de conformité, ce n'est pas simplement « se protéger », c'est renforcer les fondations de son entreprise.

Cela permet de proposer des produits sûrs et fiables, d'anticiper les exigences réglementaires, et de se positionner comme un acteur de confiance sur son marché.

Pour le dirigeant, c'est aussi une source de sérénité : savoir que l'essentiel est sécurisé, que les équipes sont structurées, et que l'entreprise est prête à passer à l'échelle sans craindre les blocages liés à la sécurité. (Nous recommandons de commencer dès le plus jeune âge d'une entreprise)

À la clé : une meilleure productivité, plus de crédibilité, des marchés accessibles... et une vraie longueur d'avance.

Les avantages d'une stratégie volontaire et bien exécuté

Gain de part de marché

- Être perçu comme un acteur fiable, mature, structuré
- Gagner la préférence dans les appels d'offres, partenariats, levées de fonds

Une valorisation de l'entreprise

- La certification rassure les investisseurs et pérennise la structure
- Elle devient un actif à valoriser en cas de revente

Des produits plus sur

- Intégrer la sécurité by design : moins de vulnérabilités pour vos clients
- Réponds aux exigences du **cyber resilience act** (produits numériques)

Répondre à la réglementation

- Éviter les amendes et difficultés lors des contrôles
- Mieux expliquer aux partenaires et clients pourquoi et comment nous sommes conformes

Structuration

- Une bonne démarche bien exécutée va apporter des process
- Renforcer les processus d'on-boarding, RH, Achat ...

Notre approche génère des bénéfices internes concrets : meilleure organisation, maîtrise des risques, efficacité opérationnelle. Mais surtout, elle vous permet de mieux expliquer votre démarche et de convaincre vos clients que vous êtes un acteur fiable et structuré.



ISO
27001

Étude de cas – Oversecur

Conformité, sécurité et souveraineté au cœur de la croissance d'un SaaS français

Oversecur est un logiciel SaaS développé pour répondre aux enjeux de conformité réglementaire, de cybersécurité et de pilotage agile des certifications (ISO 27001, RGPD, HDS, NIS 2, etc.). Dès sa conception, nous avons fait le choix d'une approche résolument souveraine, sécurisée et conforme "by design".

Objectifs

Offrir une solution souveraine de pilotage de conformité pour les PME, ETI et prestataires numériques.

Intégrer nativement les exigences des principales normes et réglementations européennes.

Valoriser la sécurité et la transparence comme facteurs de différenciation commerciale.

Actions stratégiques mises en œuvre

- Développement 100 % interne, hébergement en France
- Intégration directe des référentiels ISO 27001, SOC 2, RGPD, HDS, NIS 2 dans la plateforme.
- Audit et certification ISO 27001 de l'organisation dès la première année.
- Mise en place d'un socle de sécurité avancée (authentification forte, chiffrement, journalisation & supervision).
- Rédaction et publication d'une politique de souveraineté claire pour nos clients.

Résultats obtenus

- Accélération des cycles de vente : la transparence sur la conformité et la sécurité rassure les décideurs.
- Attribution de marchés sensibles (secteurs publics, santé, ESN), grâce à la souveraineté de la solution.
- Valorisation de notre marque en tant qu'acteur de confiance, ancré dans l'écosystème européen.

Clés de succès

Notre réussite repose bien sûr sur la qualité technique d'Oversecur, mais elle tient surtout à notre capacité à prouver notre conformité, à rendre visible notre sécurité, et à garantir une indépendance stratégique à nos clients.

HEXATRUST
CLOUD CONFIDENCE & CYBERSECURITY



Membre HEXATRUST

Certifié 27001

 **OVERSECUR**
By FeelAgile

Trouver sa voie

Les questions à se poser pour passer à la vitesse supérieure

Se poser les bonnes questions en matière de cybersécurité, c'est bien plus qu'une démarche défensive : c'est un axe stratégique.

Cela permet d'anticiper les risques, de mieux comprendre ses points de fragilité, mais surtout de transformer une contrainte en avantage concurrentiel.

Une entreprise qui sait démontrer sa maîtrise des enjeux de sécurité — certifications, conformité RGPD, résilience face aux incidents — inspire confiance à ses clients, partenaires et investisseurs.

Elle se positionne comme un acteur sérieux, fiable, prêt à opérer sur des marchés réglementés ou stratégiques. À l'inverse, celles qui évitent ces questions prennent le risque d'être écartées sans même le savoir : rejet d'appels d'offres, perte de contrats, dégradation de l'image.

En clair, la cybersécurité ne se subit pas, elle se pilote — et bien pilotée, elle devient un véritable levier de croissance.

Vous voulez faire de la cybersécurité un levier de compétitivité ?

Commencez par vous poser les bonnes questions :

✓ **Suis-je vraiment sécurisé ?**

Les attaques externes font la une, mais 80 % des incidents viennent d'erreurs internes ou de négligences chez des partenaires.

✓ **Que se passera-t-il le jour où je perds mes données ?**

Impact opérationnel, perte de clients, atteinte à l'image... Êtes-vous prêt ?

✓ **Quelle réglementation ou certification peut me faire sortir d'un appel d'offre ?**

Les nouvelles réglementations comme NIS 2, DORA ou le RGPD sont devenues des critères d'entrée.

✓ **Est-il possible que j'ai été éliminé d'un appel d'offres sans le savoir ?**

Par absence de certification ou de preuves de sécurité ? Beaucoup d'exigences sont implicites.

✓ **Quand un client me demandera une certification, combien de temps faudra-t-il pour l'obtenir ?**

Anticiper, c'est gagner du temps (et des contrats).

✓ **Suis-je réellement conforme au RGPD et aux exigences de sécurité ?**

Ou est-ce une simple case cochée dans un dossier ?

✓ **Mes concurrents sont-ils déjà certifiés ?**

S'ils l'affichent, c'est qu'ils en font un avantage commercial. Et vous ?

✓ **Ai-je les bonnes compétences en cybersécurité ?**

Est-ce que j'ai développé une vision 360 de la sécurité ?

Les erreurs à éviter



L'illusion de sécurité

👉 Pourquoi les entreprises n'y arrivent pas

vous avez compris le principe est simple, se sécuriser et valoriser sa démarche.

Mais alors pourquoi, si peu d'entreprise y arrive.

C'est très simple, la cybersécurité est aujourd'hui de plus en plus complexe et nécessite une vraie expérience.

👉 L'illusion de la sécurité – Une méconnaissance du pilotage de la cybersécurité

Beaucoup d'entreprises pensent être sécurisées parce qu'elles ont mis en place des outils : un antivirus, un pare-feu, une sauvegarde.

Mais en réalité, elles ne pilotent pas leur cybersécurité. Elles réagissent, au lieu de structurer une démarche proactive, alignée sur les vrais risques et les exigences du marché.

La différence entre être sécurisé et se croire sécurisé, c'est le pilotage. C'est ce qui permet de :

- identifier ce qui est réellement à protéger : les données
- piloter par les risques
- savoir si les mesures mises en place sont efficaces : les audits
- suivre l'évolution des menaces,
- s'assurer que les règles sont bien appliquées,
- rendre des comptes à la direction ou aux clients.

Être "sécurisé" ne veut rien dire en soi. C'est une illusion rassurante, mais vide de sens si elle n'est pas fondée sur une analyse concrète. Ce qui compte vraiment, c'est de comprendre ses risques, de savoir ce qu'on protège, contre quoi, et pourquoi. Et surtout, d'être capable de vérifier que les mesures de sécurité mises en place sont bien adaptées, maîtrisées et suivies dans le temps. Sans cette approche structurée, la sécurité reste un décor — pas une réalité.

Est-ce que je suis sécurisé ?

- Mon niveau de sécurité correspond aux menaces auxquelles je suis confronté ?
- Je comprends mes risques et sais comment y répondre ?
- Je suis sûr du dispositif de suivi de la sécurité ?

L'usine à gaz c'est parti

👉 Pourquoi les entreprises n'y arrivent pas

J'ai maintenant compris ce qu'est être sécurisé. J'ai les bons outils au bon endroit. Cela m'a demandé de comprendre mes données sensibles, mon système d'information et mes risques. Il me faut valoriser ma démarche !

Beaucoup d'entreprises transforment la certification ISO 27001 en usine à gaz, en empilant des processus, des documents, des outils et des contraintes... qui n'apportent aucune réelle valeur. Pourquoi ? Parce qu'elles sont mal accompagnées. Plutôt que de partir des risques réels, des besoins métiers et de la maturité existante, on leur impose une vision rigide, bureaucratique, souvent copiée-collée d'un autre contexte. Résultat : des politiques qui ne sont pas appliquées, des audits internes artificiels, des indicateurs sans lien avec la réalité, et une équipe démotivée. La 27001 n'est pas censée complexifier — elle doit structurer, clarifier, protéger, valoriser. Encore faut-il être guidé par des experts qui comprennent à la fois la norme et le terrain.

👉 Mais alors, qu'est-ce que je dois faire pour être conforme à l'ISO 27001 ?

👉 Rien. (hahaha)

Enfin... rien de plus, si tu as déjà fait ce qu'il faut avant.

Parce que la vérité, c'est que la conformité ISO 27001 est une conséquence, pas un objectif à part entière.

Si tu as déjà :

- identifié tes vrais risques,
- mis en place des mesures de sécurité adaptées (techniques, humaines, organisationnelles),
- défini des responsabilités claires,
- documenté ce que tu fais et vérifié que tu le fais vraiment,
- et que tu pilotes tout ça régulièrement avec des revues, audits et indicateurs utiles...

... alors tu es déjà conforme à l'ISO 27001 dans l'esprit et dans la lettre.

La norme ne te demande pas de tout compliquer. Elle te demande de piloter intelligemment la sécurité de ton système d'information, en fonction de ta réalité. C'est pour ça que ceux qui partent des besoins réels et des risques finissent la certification plus vite, avec moins d'effort... et surtout, avec un vrai bénéfice opérationnel.

Ceux qui bricolent des usines à gaz parce qu'ils veulent "faire ISO" sans comprendre, eux, font tout... sauf ce qu'il faut.

L'ISO 27001 (ou d'autres certifications ne sont que des outils pour répondre à des risques !

Et maintenant la réglementation

Pourquoi les entreprises n'y arrivent pas avec les réglementations ?

Parce que trop souvent, les experts qui les accompagnent ne parlent pas le langage du terrain. Les juristes spécialisés en conformité produisent des documents complexes, théoriques, parfois déconnectés des enjeux opérationnels.

Ils savent lire la loi... mais rarement l'expliquer simplement à ceux qui doivent l'appliquer. Résultat : les équipes opérationnelles ne comprennent pas ce qu'on attend d'elles, les responsables techniques se sentent submergés, et les projets de conformité deviennent des listes de tâches sans sens.

Et surtout, ces approches ne prennent pas en compte la réalité de l'entreprise, ses contraintes, ses priorités, ses outils, sa culture. On applique la norme, mais on oublie la logique. Et sans logique, la conformité devient un poids — jamais un levier.

Resultat : on empile des mesures de sécurité

Mais alors, qu'est-ce que je dois faire pour être conforme aux réglementations ?
Eh bien... il fallait y penser avant !

La conformité ne se rajoute pas après coup comme une couche de peinture. Elle se conçoit dès le départ, au même titre que la sécurité. En intégrant les exigences réglementaires dès la définition des mesures de sécurité, et en les connectant aux risques réels, on évite les surajouts inutiles, les usines à gaz, et les audits qui tournent en rond. Le vrai secret ? Travailler avec des juristes qui comprennent la cybersécurité concrète, le fonctionnement des systèmes d'information, et les contraintes des équipes terrain. Des experts capables de traduire la loi en actions utiles, pas juste en documents à signer. La bonne démarche, c'est de bâtir un système solide, cohérent et adapté, dans lequel la conformité devient une simple formalité... parce qu'elle est déjà là, intégrée par design



Agile compliance & Born secure



✓ 1. Partir des risques réels

Analyser ce qu'il faut vraiment protéger, contre quelles menaces, et selon quels impacts. Toute démarche doit être ancrée dans la réalité de l'entreprise, pas dans un modèle générique.

✓ 2. Construire des mesures utiles et pilotables

Mettre en place des contrôles de sécurité adaptés, mesurables, compris des équipes, et alignés avec les exigences des normes (ISO 27001, HDS, etc.) et des réglementations (RGPD, NIS 2, etc.).

✓ 3. Intégrer la conformité dès la conception

Connecter sécurité, certification et obligations réglementaires dès le départ. Cela évite les doublons, réduit la charge documentaire, et transforme la conformité en avantage stratégique.



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



+33 6 34 42 67 08



aschuhmacher@feelagile.com



@alexisschuhmacher



<https://feelagile.com/>



Prendre rendez-vous

CROISSANCE³

Stratégie de croissance au cube



La stratégie de croissance au Cube C^3

Cybersécurité X Conformité X Certification

Cybersécurité, Protéger les données et services de vos clients

Conformité, Répondre aux attentes en matière de conformité
réglementaire et légale

Certification, Démontrez la conformité et la sécurité



Croissance au cube

👉 Cybersécurité -

Les entreprises n'achètent plus un logiciel ou un service cloud uniquement pour ses fonctionnalités : ils achètent la confiance. Les critères de cybersécurité sont devenus incontournables.

Cela signifie que la protection des données, la continuité de service, la résilience face aux cyberattaques et la transparence sur les pratiques de sécurité sont devenues des critères de sélection aussi critiques que le prix ou les fonctionnalités. Ne pas répondre à ces attentes, c'est s'exposer à être écarté dès la phase de recherche.

👉 Conformité - vers la multiconformité

Après RGPD, NIS 2, DORA, AI Act, ... Les textes réglementaires se multiplient, impactant les clients finaux et par ricochet les sous-traitants ou ESN.

Bien maîtriser ces référentiels est essentiel pour expliquer ce qui doit être mis en place et éviter la surinterprétation.

Les entreprises du numérique vont en plus devoir appliquer plusieurs cadres réglementaires puisque dépendant de marchés souvent différents.

👉 La certification : arme atomique

Longtemps perçue comme un simple "label", la certification (ISO 27001, SOC 2, HDS...) devient aujourd'hui une preuve de maturité et un sésame commercial. De plus en plus d'acheteurs – publics comme privés – exigent une certification comme condition d'entrée sur leur marché ou dans leur écosystème.

Au-delà du tampon, la certification professionnalise les équipes, crédibilise l'organisation et rassure les interlocuteurs : prospects, investisseurs, partenaires. Elle permet à l'entreprise de dire "nous sommes prêts", sans avoir à le prouver à chaque interaction.

Ne pas répondre à ces attentes, c'est s'exposer à être écarté dès la phase de recherche.

👉 Ce qu'il faut retenir

En tant qu'entreprise du numérique, vous participez de façon significative au système d'information de vos clients.

- **Garantir la sécurité des données et des services de vos clients est un prérequis**
- La conformité légale NIS 2, RGPD, et DORA devient une obligation contractuelle
- Le meilleur levier pour prouver et convaincre vos clients est la certification (ISO 27001 et autres)

Agile Compliance

Appliquer les principes de l'agilité à la conformité, la sécurité et la certification

Personne n'a envie de complexité et de lourdeur

Notre méthode repose sur une approche pragmatique et intégrée de la cybersécurité, fondée sur une analyse des risques réels et l'alignement avec les exigences réglementaires (ISO 27001, NIS 2, RGPD...).

Ceci est rendu possible par la maîtrise des 3 domaines : juridique, cyber et certification.

Nous combinons solutions de sécurité innovantes, souvent issues de l'open source pour garder la maîtrise technique et stratégique, avec une expertise juridique pointue, toujours connectée aux enjeux opérationnels.

La polyvalence est au cœur de notre démarche : nous croisons les compétences en cybersécurité, conformité et certification, pour transformer la sécurité en levier de croissance. Grâce à notre approche, intégrer la certification ISO 27001 dès le démarrage devient une force, pas une contrainte.

L'adaptation comme principe de base

Il ne doit pas y avoir de solution toute faite, ni de système rigide à plaquer sur une organisation. Il faut partir de l'existant. Il faut toujours partir des enjeux spécifiques de votre organisation, de votre contexte, de vos contraintes et de vos objectifs.

Cette posture va vous permettre de construire des dispositifs de sécurité, de conformité ou de certification qui ont du sens, qui sont utiles, et surtout qui respectent la réalité de l'entreprise. (ses moyens)

Il faut refuser les approches standardisées ou les systèmes de sécurité trop grand public.

Ex : Il est souvent plus simple et moins coûteux de monter un outil de surveillance de la sécurité et de journalisation avec des briques opensource que de s'appuyer sur des solutions du marché. (À niveau de sécurité comparable)

Notre méthode

Une approche basée sur les risques et les exigences réglementaires

Notre démarche commence toujours par une analyse pragmatique des risques : il ne s'agit pas de sécuriser pour sécuriser, mais de protéger ce qui est réellement critique pour l'activité.

En parallèle, nous intégrons les exigences des référentiels réglementaires comme l'ISO 27001, NIS 2, RGPD ou HDS dès la phase de cadrage, afin de garantir un système de sécurité cohérent, auditable et aligné sur les obligations légales.

Des solutions innovantes et maîtrisées

Nous privilégions des solutions de cybersécurité ouvertes, robustes et éprouvées, notamment dans l'écosystème open source, afin d'assurer une transparence totale et une maîtrise complète de l'environnement technique.

Cette approche permet aux entreprises de limiter leur dépendance à des éditeurs fermés, tout en bénéficiant de technologies à l'état de l'art, configurées pour leurs besoins spécifiques.

Une expertise juridique intégrée à la sécurité

Nous combinons une maîtrise fine des enjeux juridiques (RGPD, souveraineté, responsabilités contractuelles...) avec une approche opérationnelle de la cybersécurité.

Chez nous, le droit n'est pas un frein mais un levier, intégré dès le départ aux réflexions sécurité. Cette synergie permet de traduire les contraintes réglementaires en actions concrètes, utiles et soutenables dans le temps.

La polyvalence comme facteur clé de réussite

Ce qui fait notre différence, c'est notre capacité à croiser les expertises : cybersécurité, conformité, gouvernance, certification.

Ce regard transversal nous permet d'éviter les silos, d'accélérer les projets et de garantir des résultats durables. Cette polyvalence est indispensable pour faire de la cybersécurité un réel accélérateur de croissance et non un simple centre de coût.

Intégrer la certification dès le démarrage avec l'ISO 27001

Trop d'entreprises considèrent la certification ISO 27001 comme une finalité ou un audit à subir. Nous pensons au contraire qu'il faut l'intégrer dès le départ, comme cadre structurant d'un système de sécurité et de gouvernance efficace. Avec les bons outils et une méthode agile, certifier son organisation devient un accélérateur pour structurer, rassurer et se différencier.

Élaborer ma stratégie

Voici une liste de questions difficiles mais essentielles à se poser pour élaborer une vraie stratégie combinant cyber, certification et conformité réglementaire. Ces questions ne sont pas “cosmétiques” : elles exigent une réflexion de fond, une lucidité stratégique, et parfois un vrai changement de posture.

Les questions à se poser pour démarrer ?

Quels sont mes actifs critiques — et qu’est-ce que je suis prêt à perdre ?

Une stratégie cyber sérieuse commence par accepter qu’on ne peut pas tout protéger.

Il faut savoir quoi prioriser... et quoi assumer en cas de crise.

Ma sécurité est-elle alignée avec mon modèle business et mes enjeux commerciaux ?

Trop d’entreprises sécurisent techniquement sans lien avec leur stratégie produit, client ou marché.

Quelle certification je dois obtenir pour me démarquer ?

Dans 90% des cas la certification ISO 27001 est la première marche

Quels sont les critères importants pour les clients ?

La réponse dépend de leur sensibilité et de leur contexte métier. Pour certains, ce sera avant tout la protection des données personnelles. Pour d’autres, ce sera la résilience, la résistance aux attaques, ou encore l’intégrité des systèmes.

C’est précisément pour cela qu’il ne peut pas y avoir une approche unique. Le niveau de sécurité et le type de certification à viser doivent être alignés avec les attentes réelles des clients. On ne sécurise pas de la même manière un logiciel grand public, une plateforme de santé ou un prestataire de services cloud. La stratégie doit s’adapter aux enjeux business... pas l’inverse.

Élaborer ma stratégie

Ai-je les bonnes compétences en interne ?

C'est une question centrale, mais souvent sous-estimée. La réussite d'une stratégie cyber, conformité ou certification ne dépend pas que des outils ou des procédures — elle repose sur les compétences disponibles dans l'organisation.

Avez-vous, aujourd'hui, les compétences pour :

- analyser les risques de sécurité de manière concrète ?
- comprendre et traduire les exigences des normes et réglementations ?
- impliquer les métiers, gérer le changement, documenter sans alourdir ?
- faire cohabiter IT, juridique, qualité et direction autour d'un même objectif ?

Et surtout : quelles compétences vous manquent pour être vraiment agiles ?

L'agilité ne vient pas d'un outil ou d'un slogan. Elle vient de la polyvalence des profils, de la capacité à décider vite, à documenter de façon utile, et à apprendre en continu. Sans cela, toute démarche de cybersécurité ou de conformité devient rigide, lente, et difficile à maintenir.

Est-ce que j'intègre les exigences réglementaires dès la conception de mes produits/services ?

Le "by design" n'est pas un luxe — c'est une nécessité pour éviter les surcoûts et les sanctions à long terme.

Mes prestataires et partenaires sont-ils réellement conformes — ou est-ce une zone grise ?

La chaîne de confiance, c'est souvent là que tout casse. Qui contrôle quoi ? Qui est responsable en cas de fuite ou d'incident ?

ALLER PLUS LOIN

Nos services



Aller plus loin

Vous avez besoin de compléter vos formations et connaissances en matière d'ISO 27001 ?



Cybersécurité 360

Rendez vous sur notre chaine YouTube !

Youtube



Autodiag ISO 27001

Réalisez votre autodiagnostic sur l'implémentation de l'ISO 27001 sur *feelagile.com*

Autodiagnostic



FeelAgile
LEARNING

Approfondissez vos connaissances avec nos formations et e-learning !

Nous contacter



RDV Commercial

Prendre rendez-vous avec un expert pour échanger sur vos projets

Contactez nous





Vous êtes décidé à
démarrer ?

découvrez nos
solutions sur la
page suivante





Nos solutions

Nous vous accompagnons dans l'obtention de votre certification ISO 27001 et la mise en place d'une gouvernance conforme, avec une approche agile adaptée aux enjeux métiers.

En Autonomie

🏠 Montée en compétences

- E-learning
- Formation sur mesure

🏠 Base de connaissances

- Accès à la base de connaissances (Templates, exemples...)

📁 Plateforme de conformité

- Outil de GRC
- CSM assistance Oversecur
- Formation à l'outil et onboarding
- Consulting
- Diagnostic & Audit blanc

[En savoir plus](#)

En Accompagnement

Premium

📁 Conseil & Formation

- Base documentaire
- Contrôler & auditer votre SMSI
- Suivi régulier avec un expert

📁 Chef de projet dédié

- Pilotage du projet de certification
- Formation des équipes & accompagnement au changement
- Assistance à la rédaction documentaire
- **Garantie de résultat**

📁 RSSI Externalisé

- Pilotage du projet de certification
- Responsable du SMSI
- Rédaction documentaire
- Passage de l'audit de certification
- **Garantie de résultat**

[En savoir plus](#)

Notre outil : Oversecur

Intégrez toutes les **données** de votre démarche de **certification**

Centralisez l'information, le suivi de vos actions et les **preuves** nécessaires pour l'audit

Utilisez une **plateforme sécurisée** sur votre cloud ou en hébergement



- Multi-référentiels
- Automatisation des relances
- Gestion des risques
- Système documentaire intégré
- Outil sécurisé & collaboratif



Formations et e-learning

Nous proposons des formations certifiantes, des sensibilisations et du e-learning pour renforcer les compétences et la culture sécurité de vos équipes.

Nos formations certifiantes PECB :

- ISO/IEC 27001 Lead Implementor
- ISO/IEC 27001 Lead Auditor
- ISO/IEC 27005 Risk Manager
- RGPD - Certified Data Protection Officer
- ISO 37001 Lead Implementer
- ISO 31000 Risk Manager
- ISO/IEC 22301 Lead Auditor
- ISO/IEC 22301 Lead Implementor

Nos sensibilisations :

- Sécurité de l'information
- Sensibilisation au RGPD
- Données de santé

Nos e-learning :

- ISO 27001
- HDS
- ISO 9001



Nous concevons également des **formations personnalisées** en cybersécurité et conformité, adaptées à vos enjeux, vos métiers et vos référentiels.

Pourquoi nous choisir ?

FeelAgile est le leader des certifications ISO 27001 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

Ensemble, construisons une conformité Agile

EXPERTISE EN CERTIFICATION

**20 ans****PASSÉ DANS LES
ORGANISATIONS****16**Experts cyber, chefs de
projet 27001, auditeurs**+ de 200
projets 27001**Nos certifications et
nos partenaires

Restons en contact !

Alexis Schuhmacher, Directeur Commercial



+33 6 34 42 67 08



aschuhmacher@feelagile.com



@alexisschuhmacher



<https://feelagile.com/>



Prendre rendez-vous



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