Guide ISO 27001

Pour les dirigeants

Feel Agile
Certified & Protected

Guide pour les décideurs

Pourquoi engager un projet de certification ?
Quels sont les avantages concurrentiels ?
Quel est l'impact de l'ISO 27001 sur mon business ?

Faire de la cybersécurité un outil de protection et d'innovation

Depuis 20 ans, la certification ISO 27001 joue un **rôle essentiel dans la gestion de la sécurité de l'information**. Au fil des années, la norme et la certification ont considérablement évolué.

Nous avons cherché dans ce guide à présenter les **dernières évolutions de la norme ainsi que les avantages d'un projet ISO 27001**. Nous y dévoilons également les **clés** pour transformer ce projet en un véritable levier de croissance pour les PME et les ETI.

Nous allons vous partager les **meilleures pratiques** et astuces pour faire de votre projet ISO 27001 un projet d'entreprise à part entière, capable d'améliorer significativement votre **cybersécurité et votre conformité.**

L'ISO 27001 est un **outil complet** qui permet de mettre en œuvre une vraie démarche de cybersécurité à la fois performante et économiquement rentable.

Les avantages de cette norme ne sont plus à prouver : c'est un outil polyvalent qui convient à toutes les étapes et à tous les niveaux de la gestion de la cybersécurité.

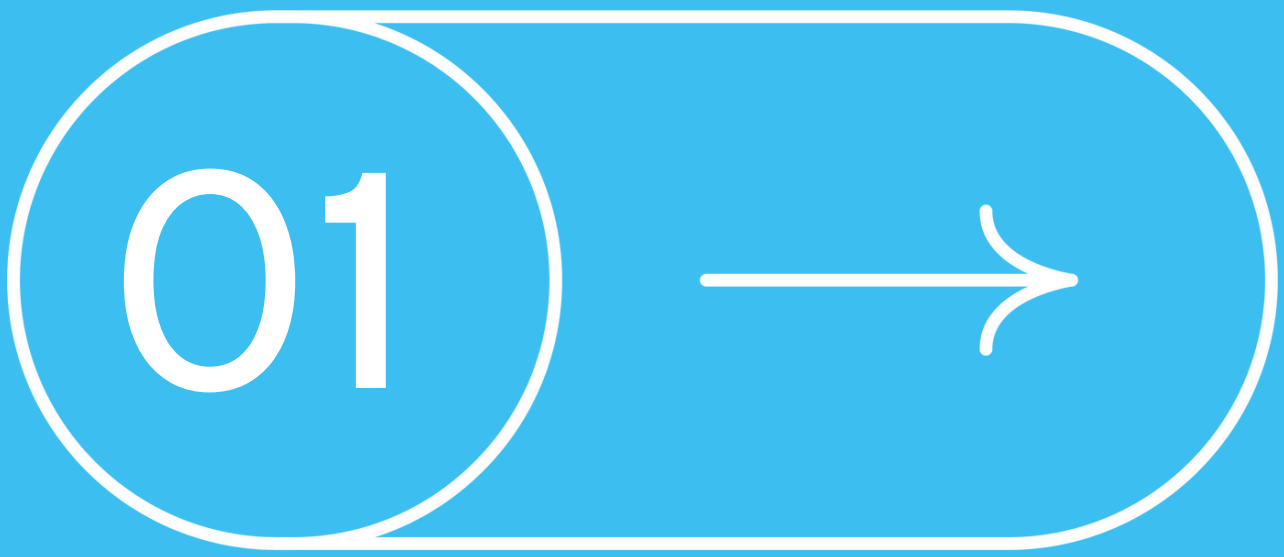
Faire de la cybersécurité un véritable investissement

Guide pour les décideurs

Feel Agile
Certified & Protected

COMPRENDRE

Qu'est-ce que l'ISO 27001 ?



Feel Agile
Certified & Protected

Faire de la cybersécurité un outil de protection et d'innovation

La cybersécurité est un enjeu fondamental qui peut affecter la survie même des entreprises. Le risque cyber représente parfois une menace existentielle, et dans tous les cas, il constitue un risque majeur que les dirigeants de PME et ETI doivent impérativement traiter.

Par conséquent, les directions doivent prendre les bonnes décisions en matière de cybersécurité. Bien entendu celle ci vont chercher à mettre en place des mesures proactives pour améliorer leur posture de sécurité de l'information et communiquer cette posture de manière claire aux clients actuels et potentiels.

De plus, il est crucial de se conformer aux réglementations telles que le RGPD et, prochainement, la directive NIS 2, pour garantir la protection des données personnelles et la résilience des réseaux et systèmes d'information.

Un excellent point de départ pour renforcer votre sécurité est la mise en œuvre d'un cadre de sécurité tel que l'ISO 27001. En effet cette démarche va vous permettre d'encadrer, d'optimiser et de valoriser votre cybersécurité pour en faire un levier de développement pour votre activité.

Si vous envisagez d'implémenter ce programme, cette documentation vous fournira toutes les informations nécessaires pour prendre une décision éclairée sur l'adoption de l'ISO 27001.

L'ISO 27001 est le meilleur cadre pour piloter sa cybersécurité !

Comprendre l'ISO 27001 en 2 minutes

Avant d'aprofondir le ROI, les avantages d'une démarche de certification ISO 27001 il est important de bien comprendre ce qu'est l'ISO 27001 !
ISO 27001- Exigences pour un Système de Management de la Sécurité de l'Information (SMSI) est une norme certifiable pour les entreprises qui prouvent leur maitrise de la sécurité.

L'ISO 27001 est un cadre qui va vous permettre d'organiser et de valoriser votre démarche de cybersécurité.

Norme internationale

Certification et norme internationale reconnue dans plus de 150 pays qui vise à définir un cadre d'organisation de la sécurité et les socles de sécurité à appliquer.

Amélioration continue

La certification (cycle de 3 ans) ne vise pas un niveau de sécurité précis mais une démarche d'amélioration continue sur plusieurs années.

Annexe A

La démarche de certification est l'occasion de mettre en place des bonnes pratiques de sécurité sous formes de 93 mesures de sécurité qui doivent être implémentées et que l'on retrouve dans l'annexe A de la norme ISO 27001

Organisation

Au dela des mesures de sécurité la norme exige la mise en place d'une organisation pour piloter la sécurité. Cet ensemble de process, documents et responsabilités est désigné Système de Management de la Sécurité de l'information.

Pilotage de la sécurité

Mise en place des responsabilités et KPI pour piloter et rendre compte de la sécurité. Donner la garantie du niveau de sécurité visé et de l'atteinte des objectifs.

Analyse des risques

L'analyse des risques est la base du travail à effectuer avec l'ISO 27001, c'est une étape fondamentale pour déterminer les mesures de sécurité applicables.

Thomas DE MOTA
VOUS EXPLIQUE TOUT
SUR L'ISO 27001

RETROUVEZ NOTRE FAQ DÉDIÉE SUR NOTRE CHAÎNE YOUTUBE POUR ENCORE PLUS D'INFORMATIONS !

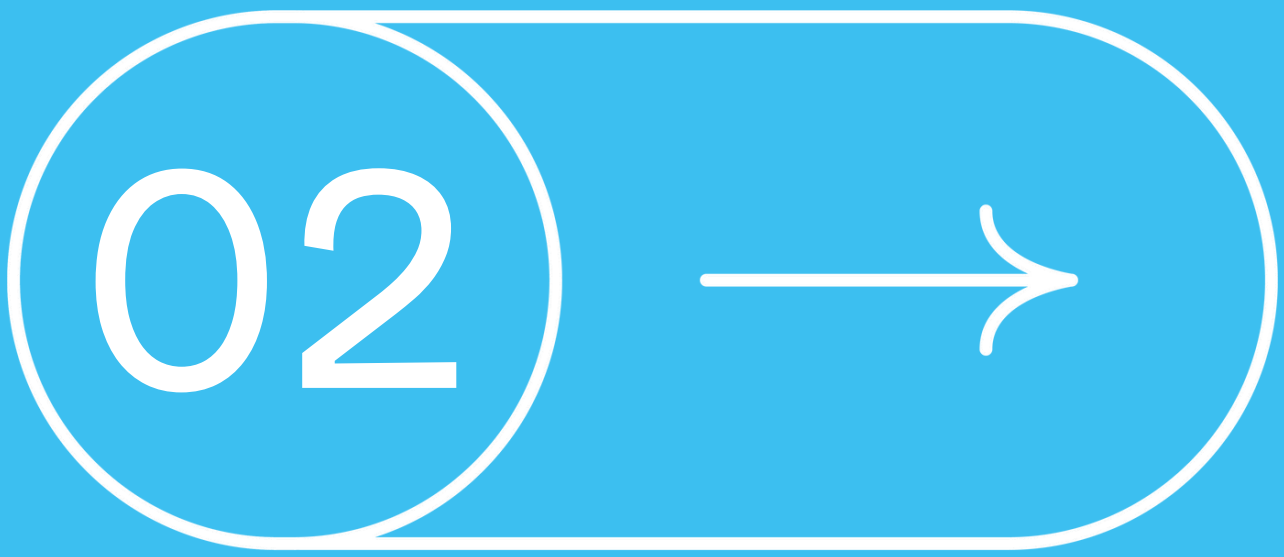
Les principaux objectifs du management de la sécurité sont **la satisfaction des exigences sécurité** et **l'amélioration continue** de la posture de sécurité de l'entreprise.

Une démarche saine est une démarche partant de l'existant.

Feel Agile
Certified & Protected

ANALYSER

La certification devenue incontournable



Feel Agile
Certified & Protected

Le moteurs de la certification 27001

La certification ISO 27001 rencontre un succès considérable en matière de certification de cybersécurité. Les entreprises ont trouvé un réel intérêt à obtenir cette certification. Examinons ensemble les principales motivations qui poussent ces entreprises à se conformer à cette norme.

Améliorer sa cybersécurité & réduire les risques

Pour **initier une démarche de sécurité**, l'ISO 27001 constitue un **cadre adapté pour les organisations de toutes tailles**, offrant une approche pragmatique et cohérente en cybersécurité.
Cette démarche permet de **se concentrer sur les risques majeurs** grâce à l'analyse des risques (Chapitre 6 de la norme), ce qui évite de dépenser des ressources sur des actions superflues. L'approche de programmation de la **sécurité sur le long terme** permet également d'**anticiper des actions importantes et structurantes**. Étant donné que la sécurité est étroitement liée au système d'information, il est crucial de **bien structurer les bases** dès le début.

Quelque soit votre projet entourez vous de vrais professionnels de la sécurité pour implémenter l'ISO 27001, votre projet aura ainsi un vrai impact sur la sécurité sur le long terme.

Un autre avantage significatif est qu'il permet à chaque entreprise de **progresser à son propre rythme** en fonction de **ses objectifs et de ses enjeux spécifiques** en matière de sécurité. Les mesures de sécurité sont ainsi définies en tenant compte du cadre règlementaire et contractuel, ainsi que du niveau de risque que l'entreprise souhaite atteindre en matière de sécurité.

Que l'on débute ou pas en cybersécurité, la démarche portée par l'ISO 27001 présente de vrais avantages en matière de guide cybersécurité

L'annexe A et la norme ISO 27002 présentent l'**ensemble des mesures de sécurité** qu'une entreprise peut mettre en place de manière **générique**. Il s'agit d'une **excellente première étape**, équilibrée, qui combine des mesures techniques, organisationnelles et juridiques indispensables à toute entreprise.

Le moteurs de la certifications 27001

Les exigences croissantes des clients et partenaires

Nous constatons une tendance croissante à l'**externalisation** des processus métiers et des systèmes d'informations notamment vers le **cloud.**
De plus en plus de services en SaaS, sont désormais proposés aux clients.
Les grands groupes, ETI, services de l'état et autres organisations **imposent des critères de sécurité** et des **exigences contractuelles** en cybersécurité de plus en plus stricts aux PME qui fournissent ces services externalisés.

La certification ISO 27001 répond aux d'exigences de sécurité des grands groupes ou ETI. C'est un passeport vers la croissance !

Ces exigences de sécurité peuvent **prolonger le cycle de vente** de plusieurs mois et même vous **exclure du processus de sélection** des prestataires. En fin de compte, si votre organisation **ne peut pas démontrer un niveau de sécurité de base**, les clients peuvent choisir d'aller voir d'autres fournisseurs ou imposer à votre organisation des audits ou questionnaires interminables.

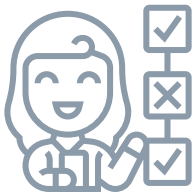
Des entreprises comme Orange, Renault, et toute Entreprise Importante ou Essentielles* exigent la certification ISO 27001 comme base d'une relation contractuelle.

Si votre entreprise souhaite **accélérer son développement, alléger le fardeau des audits clients et croître dans un marché mondial** concurrentiel, il est essentiel d'instaurer une **confiance absolue** chez les partenaires et les clients potentiels. Par conséquent, obtenir des certifications de sécurité comme l'ISO 27001 est indispensable pour rester compétitif.

Un bon guide qui en plus va vous permettre de valoriser votre investissement via la certification !

*dans le cadre de NIS2 certaines entreprises sont concernées directement par la règlementation. Il s'agit des Entreprises Essentielles et Importantes définies en fonction des secteurs d'activités et de la taille des entreprises.

Répondre aux exigences règlementaires



Une certification ISO 27001 qui devient obligatoire !

Dans de nombreux secteurs où la cybersécurité est un enjeu important la norme ISO 27001 devient obligatoire. On peut citer l'hébergement des données de santé, les PME qui travaillent dans l'automobile, qui travaillent pour les grands groupes OIV / EE (Entreprises Essentielles), les éditeurs SaaS ...
Avec les nouvelles **réglementations européennes** (NIS 2, DORA, IA Act, CRA...), **rares sont les secteurs qui échapperont aux exigences en matière de cybersécurité**. La grande nouveauté est que ces réglementations concernent désormais **aussi les PME et TPE**. Dans ce contexte, vous avez le choix : transformer ces obligations en **avantage concurrentiel** ou **subir le risque réglementaire.**

La certification ISO 27001 permet de garantir un engagement clair dans le respect des règlementation en cybersécurité !

Pour le secteur numérique, cette certification devient incontournable si vous souhaitez rester dans la course et vous développer.
L'acte d'exécution européen NIS 2 pour les services informatiques, les services cloud renforcent la pression des acteurs du secteur en **exigeant des mesures de sécurité semblables à l'ISO 27001.** La norme devient ainsi un bon moyen d'engager un vrai chemin vers la conformité règlementaire.

Cela vous prépare aux éventuels contrôles, et audits des instances règlementaires ou clients.

Ces réglementations imposent l'obligation de signaler tout incident en cas de problème de sécurité.

En cas d'incident, les **instances CNIL ou ANSSI peuvent déclencher des audits** si des pratiques semblent non conformes à la règlementation, notamment en cas de non-déclaration d'un incident de sécurité ou de fuite de données personnelles.

La meilleure certification tout simplement

Une adoption croissante dans tous les secteurs

Les **secteurs avec l'obligation légale** ou l'obligation du fait des standards du marché de certification ISO 27001 sont de plus en plus nombreux :

- Le secteur des **services clouds**
- la **esanté**
- les **ERP et CRM en lignes**,
- **l'automobile**
- le **secteur financier** et **assurantiel**
- **..**

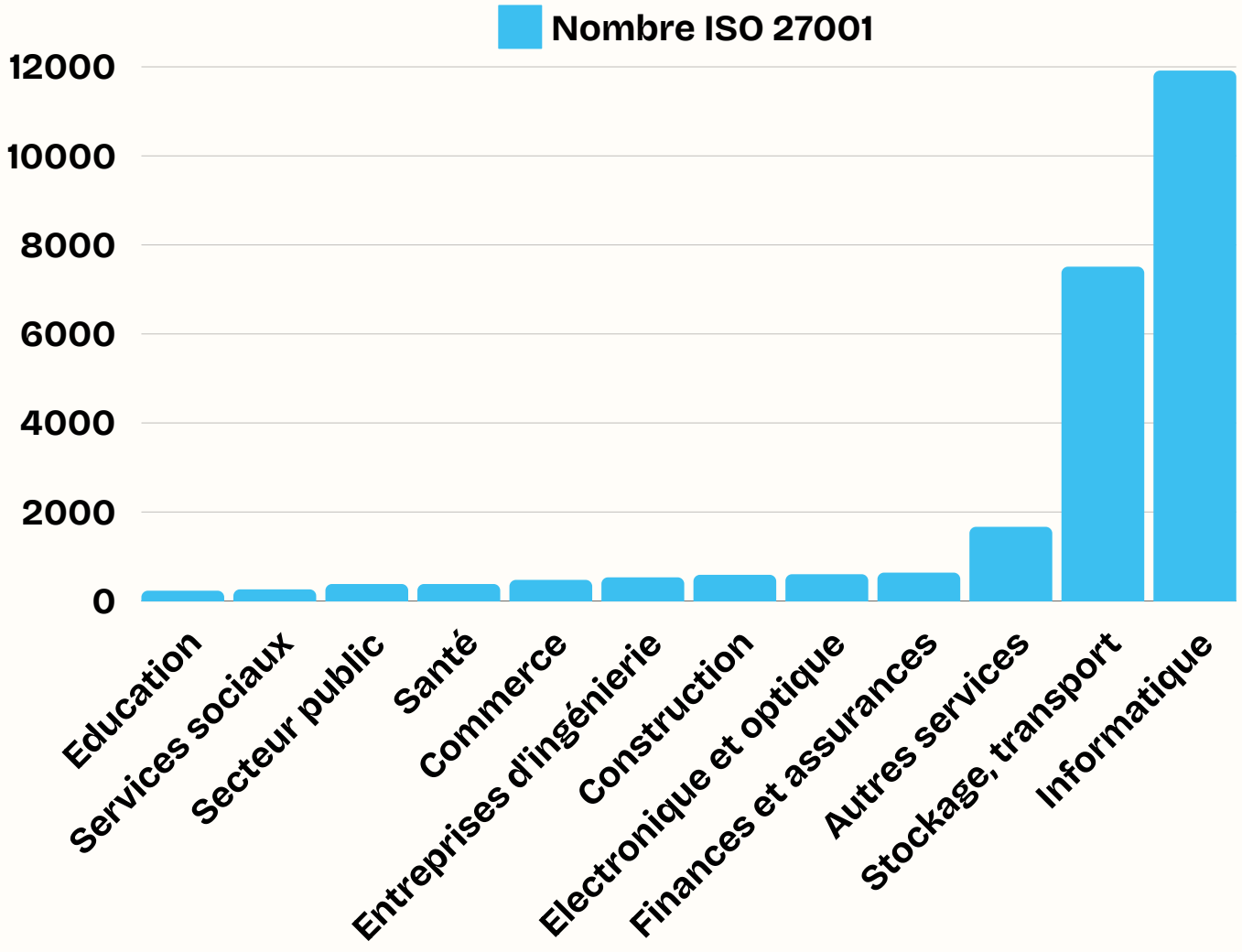
Il est également important de mentionner les secteurs où l'ISO 27001 devient la **norme minimale** à obtenir pour **continuer à travailler**. Elle devient ainsi une obligation de fait et un standard incontournable sur le marché, imposé par les **exigences du secteur**.

Ensuite il y a les secteurs dans lesquels l'adoption est croissante, comme **les ESN sous la pression des grands groupes**, les **éditeurs SaaS**, tous les **services externalisés RH**, **Sécurité**, **Financiers sous la pression des clients** et des règlementations.

Si vous êtes dans un **secteur** où les **concurrents ne sont pas certifiés** et le marché n'est pas encore sensibilisé, c'est dans ce type de secteur que vous aurez le **plus grands gains à réaliser la certification** permettant de vous différencier.

- **71 000 certificats ISO 27001 en 2020**
- **Une évolution de + 30 à 50 % annuelement en fonction des secteurs**

La meilleure certification tout simplement



Source ISO SURVEY, 2022

Un investissement pour les PME

En résumé
Les bénéfices d'une certification ISO 27001

La confiance

Vous allez renforcer rapidement le niveau de confiance de vos clients, prospects et partenaires.

Maîtrise

Mieux maîtriser l'accès à l'information et aux risques liés à la protection des données et la continuité des services

Se différencier

La démarche de certification est l'occasion de mettre en place des bonnes pratiques de sécurité sous formes de 93 mesures de sécurité qui doivent être implémentées et que l'on retrouve dans l'annexe A de la norme ISO 27001

Respect des règles

Assurer le respect de la règlementation en matière d'information (exemple, le RGPD)

Retrouvez notre FAQ dédiée sur notre chaîne Youtube pour encore plus d'informations !

Une sécurité maîtrisée

Cette norme présente les exigences en matière d'organisation (système de management) pour s'assurer que la sécurité de l'information est bien maîtrisée :

- La **gouvernance** liée à la sécurité de l'information et la stratégie,
- Les **processus** nécessaires à la maîtrise de la sécurité de l'information,
- Les **méthodes** pour analyser les risques et en rendre compte,
- Les processus de **mesure, de suivi et d'amélioration** de la sécurité,
- Les **responsabilités** liées à la sécurité de l'information.

Editeur et hébergeur de solutions no code

anakeen

“L’ISO 27001 permet de répondre à la problématique de cybersécurité

En plus de structurer nos moyens de production, c'est une formalisation des pratiques qu'on a aujourd'hui en terme de sécurité.

C'est aussi un élément de réassurance pour nos clients qui sont demandeurs et puis du point de vue business je dirais c'est important aujourd'hui de pouvoir dire qu'on est certifiés 27001 : ça rassure aussi le prospect !

On a typiquement là depuis quelques semaines, c'est tout frais, on a un nouveau client. J’ai été en contact avec le RSSI de la société sur lequel on a pu échanger. On va héberger leur système donc c'était pour eux crucial. On a pu montrer qu'on avait l'ensemble des outils pour gérer le SMSI et donc sécuriser tous les environnements.”

voir le témoignage >

Certifié ISO 27001 v 2022

Editeur de logiciels agiles

veryswing

“J’avais peur d’une démarche qui ralentisse le business

Nous avons mis un curseur de la sécurité pour pouvoir garder notre agilité

Nous répondons à beaucoup de questionnaires de sécurité et maintenant nous sommes en mesure de rassurer nos prospects et nos clients

Cette démarche a amené une vraie culture de la sécurité pour toutes les équipes

C’est aussi un moyen de challenger nos pratiques de cybersécurité, nous avons des indicateurs qui permettent de surveiller la sécurité.”

voir le témoignage >

Certifié ISO 27001 v 2017

Editeur de logiciels

Aniah

“Nos clients sont des gros acteurs du secteur informatique, la notion de sécurité est prépondérante.

Nous avons des prérequis contractuels sur la cybersécurité.

Nous avons fait ISO 9001 et ISO 27001

Maintenant on coche la case des prérequis contractuels.

Cela nous a beaucoup apporté au niveau opérationnel, cela permet de structurer”

voir le témoignage >

Certifié ISO 27001 & 9001

Combien cela coûte et combien cela rapporte ?

La mise en place

50 - 100 K€

↘

Coût des équipes internes
Coût des formations
Passage de la certification
Solutions de sécurité

Le maintien

25 - 50 K€

↘

Coût des équipes internes
Audits annuels
Solutions de sécurité
Maintien des documents

ROI

x10

↘

+ la sécurité
+ la conformité
+ la valeur de l'entreprise

- Le retour sur investissement est de **minimum de X10**
- Nos clients réalisant un **CA entre 1 et 3 M€** de CA vont réaliser entre **500 K € et 1M€ de CA supplémentaire / an**
- Sur **10 ans** cela représente une **croissance de 5M€ supplémentaire minimum**

Feel Agile
Certified & Protected

Obtenir l'ISO 27001

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 !
Rendez-vous sur notre site web !

Autodiagnostic

Cybakademy

Approfondissez vos connaissances avec nos formations et e-learning !

Cybakademy

RDV Commercial

Prendre rendez-vous avec un commercial pour une formation ?

Contactez nous

Feel Agile
Certified & Protected

VOUS ÊTES DÉCIDÉ À DÉMARRER ?

DÉCOUVREZ NOS SOLUTIONS SUR LA PAGE SUIVANTE

Feel Agile peut vous aider !

Feel Agile est le leader des certifications ISO 27001 en France avec plus de 150 PME certifiées et accompagnées.

Vous voulez externaliser en totalité votre certification ?

Vous voulez confier votre projet à **un partenaire** qui **va conduire en qualité de chef de projet votre certification** de **A à Z** nous avons les solutions qui vont vous convenir.

OFFRE: ISO 27001 EXTERNALISÉ

Vous souhaitez être formé et guidé dans le processus de certification ?

Nous nous proposons des formations ou accompagnements réellement opérationnels pour vous permettre de réussir votre projet.

Offre CLASSIQUE
Nous faisons avec vous

OFFRE FULL
Nous faisons avec vous et pour vous

Vous voulez conduire votre projet de façon autonome ?

Nous proposons des outils partenaires, du e-learning, ou des kits de documentation pour vous aider à vous certifier rapidement.

BOX ISO 27001
Do It Yourself

Logiciel certification
Stellar

Vous êtes consultant ou partenaire ?

Nous proposons des partenariats et formations pour vous aider à implémenter les certifications avec vos clients.

Pourquoi nous choisir ?

Feel Agile est le leader des certifications ISO 27001 en France avec plus de 150 PME 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**

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 150 PME certifiées** et accompagnées.