FeelAgile

Guide

Documentation

ISO 27001

La documentation :
La clé de voûte de votre projet ISO 27001

La colonne vertébrale de mon système

La gestion documentaire constitue la véritable colonne vertébrale d'un système de management ISO 27001.

Elle permet d'organiser l'entreprise, de formaliser ses processus et de définir la manière dont chacun doit agir pour garantir la cohérence, la sécurité et la conformité. C'est à travers cette documentation que l'on fixe les politiques, les procédures et les modes opératoires qui orientent le fonctionnement quotidien. Mettre en place une gestion documentaire, c'est donc structurer l'organisation et poser les fondations d'un système de management durable.

Pourtant, cette étape est souvent sous-estimée et source de difficultés. Trop souvent, les documents sont rédigés isolément, sans coordination ni mise à jour partagée.

Or, la documentation doit être vivante et intégrée à la culture de l'entreprise. Toutes les certifications ISO, qu'il s'agisse de la 27001, de la 9001 ou d'autres référentiels, exigent une structuration documentaire claire et cohérente. Celle-ci doit également être alignée sur les exigences réglementaires : chartes de sécurité, règlements intérieurs, politiques internes, etc. La documentation n'est donc pas un exercice administratif mais un levier stratégique de conformité et de pilotage.

Une gestion documentaire efficace couvre aussi les documents externes : contrats, accords, rapports ou encore référentiels clients. Ces éléments doivent être identifiés, maîtrisés et mis à disposition de manière sécurisée. Leur gestion contribue directement à la confiance des clients et partenaires, en démontrant la capacité de l'entreprise à protéger les informations et à maîtriser son environnement documentaire.

Enfin, les enregistrements, preuves des actions réalisées, font partie intégrante de cette maîtrise documentaire. Ils garantissent la traçabilité, la transparence et la crédibilité du système de management. Une documentation bien structurée favorise non seulement la conformité, mais aussi la performance et la croissance de l'entreprise.

Ce guide a donc pour ambition de fournir à la fois des méthodes concrètes pour structurer votre documentation ISO 27001 et une réflexion sur la manière d'en faire un véritable outil de pilotage et de confiance au service de votre organisation.

Sommaire

Gestion documentaire : la colonne vertébrale de votre système ISO 27001

01 Documentation comme vecteur de performance

02 La gestion documentaire de A à Z

03 Le processus d'implémentation

04 La documentation ISO 27001 en pratique

05 Conclusion – Nos services

CONTEXTE

La documentation : vecteur de performance

01

La documentation, pilier du système ISO 27001

Pilier ou talon d'achile de votre certification ISO 27001 !

La documentation occupe une place centrale dans la mise en œuvre d'un **système de management de la sécurité de l'information (SMSI) conforme à l'ISO 27001.**
Ce référentiel ne se limite pas à imposer des pratiques de sécurité : il exige une véritable maîtrise de cette sécurité, rendue possible grâce au **formalisme documentaire.**

La documentation constitue en effet la base du pilotage du SMSI. Elle permet non seulement d'encadrer les actions, mais aussi de rendre visible et vérifiable la manière dont la sécurité est assurée.

Concrètement, la documentation recouvre plusieurs niveaux :
- **les politiques de sécurité** qui définissent les orientations stratégiques,
- **les processus** qui décrivent la manière d'appliquer ces politiques,
- **et les enregistrements,** qui servent de preuves objectives du bon fonctionnement du système.

Elle transforme une sécurité implicite, parfois informelle ou intuitive, en une sécurité maîtrisée, structurée et démontrable.
C'est là toute la valeur ajoutée de l'ISO 27001 : passer d'un modèle de gestion « orale » à une culture **du processus et de la traçabilité.**

Cette formalisation, parfois perçue comme contraignante, constitue en réalité le cœur du système. Elle garantit la continuité, la cohérence et la capacité de l'organisation à prouver, à tout moment, qu'elle contrôle effectivement la sécurité de son information.

Une source d'erreurs fréquente et de dérives

Si la documentation est indispensable, elle représente aussi l'un des points les plus délicats à maîtriser dans la mise en œuvre de l'ISO 27001.
De nombreuses organisations échouent non pas sur le fond — la sécurité technique ou les processus — mais sur la **forme documentaire.**

Trop souvent, les documents sont rédigés pour « faire plaisir à l'auditeur » plutôt que pour piloter réellement l'activité. Résultat : des procédures figées, copiées-collées, rarement lues ou appliquées, qui deviennent rapidement obsolètes.

Les principales erreurs tiennent à un excès de formalisme ou, à l'inverse, à un manque de rigueur.
Certains multiplient les documents jusqu'à perdre en clarté et en cohérence ; d'autres se contentent de fichiers épars, sans structure ni validation. Dans les deux cas, la documentation ne joue plus son rôle de support à la maîtrise : elle devient une contrainte administrative.

Une autre dérive fréquente consiste à externaliser la réflexion documentaire : confier la rédaction à un consultant ou à un modèle standard, sans appropriation interne. Or, un document n'a de valeur que s'il reflète la réalité de l'organisation, ses méthodes, ses outils et sa culture.

Enfin, le manque de mise à jour — souvent faute de processus clair ou de propriétaire désigné — conduit à des incohérences entre la pratique et le formalisme, fragilisant la conformité et la crédibilité du SMSI.

L'approche processus : un vecteur de responsabilisation et de performance

L'objectif d'une **certification ISO 27001** n'est pas seulement d'obtenir un certificat : c'est de mettre en place un **Système de Management de la Sécurité de l'Information (SMSI)** qui fonctionne réellement, qui soit utile, compréhensible et durable.

Un SMSI efficace doit vivre au quotidien dans l'organisation, sinon il devient difficile à maintenir et perd rapidement son sens.

C'est pourquoi les normes ISO, depuis plusieurs années, encouragent une approche processus comme fondement de tout système de management cohérent et performant.

Adopter une approche processus, c'est **identifier clairement les processus métiers, supports et de management**, et comprendre comment ils interagissent entre eux.
Cette cartographie rend l'organisation lisible, partagée et pilotable.

Chaque processus devient un **cadre de référence** qui relie les activités à la stratégie, tout en favorisant la responsabilité et la transparence.

Cette structuration facilite la **gestion des risques** : on peut analyser les risques spécifiques à chaque processus, définir les contrôles adaptés et documenter précisément les mesures mises en œuvre.

Cette approche permet aussi d'intégrer la documentation de manière naturelle et fonctionnelle.
Chaque processus devient porteur de ses propres documents : politiques, procédures, enregistrements.

Les responsables de processus deviennent ainsi responsables de leur documentation, de sa mise à jour et de sa conformité.
Cela évite la déconnexion entre le terrain et le système documentaire, et garantit que les documents reflètent la réalité de l'organisation.

Enfin, l'approche processus facilite l'intégration de la sécurité dans tous les domaines de l'entreprise.

Par exemple, dans le processus Ressources Humaines, on intégrera la sécurité dès l'onboarding, dans la gestion des habilitations ou la sensibilisation du personnel.

Ce principe d'intégration par processus transforme la sécurité en **composante naturelle** du fonctionnement global, et non en contrainte isolée.

Ainsi, au-delà de la certification ISO 27001, cette démarche favorise la **cohérence, l'engagement des collaborateurs et la création de valeur.**

Un système vivant, documenté et compris de tous devient un véritable levier de performance et de confiance, bien plus qu'un simple exercice de conformité.

Dans la suite de ce guide, nous approfondirons cette notion de processus et ses liens étroits avec la documentation, afin de comprendre comment articuler efficacement le pilotage opérationnel, la sécurité et la maîtrise documentaire au sein de votre organisation.

Je veux me certifier ISO 27001, avec des processus solides et intégrés

Les avantages d'une bonne documentation

Clarifier les rôles et les responsabilités : un pilier de l'efficacité organisationnelle

L'un des premiers bénéfices d'une **documentation bien structurée** réside dans la définition claire des **rôles** et des **responsabilités**.
Quand la documentation est élaborée à partir des processus, elle permet d'attribuer à chaque acteur une place précise dans le fonctionnement du système de management.

Cette étape est essentielle : elle évite les zones d'ombre, les doublons ou les oublis et donne à chacun une vision claire de son périmètre d'action.

Documenter les responsabilités au sein du SMSI, c'est rendre explicite **qui fait quoi, comment et sous quelle autorité**. Cela concerne aussi bien les fonctions de pilotage (responsable sécurité, comité de direction) que les fonctions opérationnelles (chefs de service, utilisateurs, prestataires).
Par exemple, le reporting en matière de sécurité, la supervision des incidents, la tenue des registres ou encore la conformité réglementaire (RGPD, NIS2, etc.) doivent être clairement affectés et tracés.

Cette structuration ne se limite pas à la sécurité : elle s'applique à l'ensemble des processus de l'entreprise. Chaque processus documenté précise les rôles associés, les interactions avec les autres services et les décisions attendues.
En clarifiant ces responsabilités, la documentation devient un **outil de gouvernance à part entière** : elle favorise la responsabilisation, fluidifie la communication et permet à chacun de comprendre sa contribution à la performance globale du système.
Une documentation claire sur les rôles et responsabilités, c'est donc plus qu'une exigence ISO : c'est un moyen de renforcer **la coordination, la transparence et la confiance** au sein de l'organisation.

Maîtriser les actions et la réalisation des objectifs de sécurité

Une documentation bien conçue permet avant tout de **maîtriser ce que l'on prévoit de faire, ce que l'on réalise et ce que l'on atteint.**
En formalisant les objectifs, les plans d'action et les méthodes, l'organisation gagne en rigueur et en visibilité sur son avancement.
Chaque processus, chaque procédure documentée, devient un repère qui relie les actions quotidiennes aux objectifs de sécurité fixés par la direction.
Ce formalisme évite les approximations, réduit les erreurs opérationnelles et favorise la cohérence entre les équipes.
La documentation devient ainsi un outil de mesure et d'amélioration continue du système de management.
La définition de la politique de sécurité apporte une précision sur les niveaux de sécurité et les mesures à mettre en place.
La définition de procédures permet de garantir que les collaborateurs respectent les bonnes pratiques, tandis que les revues de mesures permettent de vérifier que les mesures de sécurité sont correctement mises en place.

Ainsi, la documentation constitue un référentiel commun pour faire une sécurité maîtrisée.

Les avantages d'une bonne documentation

On ne peut maîtriser que ce que l'on connaît

Donner de la visibilité sur les risques et mieux piloter

La documentation est également un **vecteur de transparence** sur les risques. Elle permet de recenser, d'évaluer et de suivre les risques identifiés dans chaque processus.
En associant les documents à ces risques (plan de traitement, analyse de risques, Déclaration d'applicabilité), l'organisation développe une vision claire **des points critiques et des priorités.**

Cette visibilité renforce le pilotage : les décisions sont prises sur la base d'informations fiables et à jour.
La documentation devient alors un **instrument de gouvernance** qui éclaire les arbitrages et soutient la stratégie de sécurité globale.

Assurer la traçabilité et démontrer la conformité

Les **enregistrements** jouent un rôle clé dans le SMSI : ils constituent les preuves concrètes de ce qui a été réalisé.
Ces documents attestent de la mise en œuvre effective des politiques et procédures, et permettent de démontrer la **conformité** à l'auditeur, mais aussi aux clients et partenaires.

Cette traçabilité crée une relation de **confiance.** En cas de doute, d'incident ou d'audit, l'entreprise peut prouver ses actions, justifier ses choix et montrer qu'elle agit selon un cadre maîtrisé.
La documentation devient ainsi un gage de **crédibilité et de fiabilité** pour l'écosystème.

Renforcer la maîtrise en cas d'incident et la continuité d'activité

Enfin, une documentation bien structurée offre un avantage décisif en situation de crise.
Lorsqu'un incident de sécurité survient, disposer de procédures à jour, de plans de continuité et de consignes claires permet de réagir vite et de manière coordonnée.
Les documents définissant les rôles, les actions à mener et les priorités assurent la résilience de l'organisation.

Au-delà de la conformité, c'est la capacité de l'entreprise à maintenir son activité et à protéger ses actifs critiques qui est en jeu. Une documentation maîtrisée, c'est donc la garantie d'une réponse efficace, d'une reprise rapide et d'une continuité opérationnelle assurée.
Une documentation bien gérée n'est pas une contrainte : c'est un facteur de maîtrise, de performance et de confiance. Elle relie la stratégie à l'action, la conformité à la réalité, et transforme la sécurité en avantage concurrentiel durable.

Avec ces exemples, vous voyez que la documentation ne s'arrête pas à une simple procédure.
Il est essentiel de concevoir l'ensemble du formalisme avec cohérence pour bénéficier pleinement de la démarche ISO 27001.

La gestion documentaire de A à Z

02

Documentation et information documentée

👉 Qu'est-ce que la documentation ?

Pour bien comprendre la place de la documentation dans un système ISO 27001, il faut d'abord revenir à la définition qu'en donne l'ISO.

Dans le langage des normes, toute information et son support constituent une **« information documentée »**. Cette notion est volontairement large : elle englobe aussi bien les politiques écrites que les enregistrements, rapports, formulaires ou tableaux de suivi, qu'ils soient au format papier ou numérique.
Dans la norme, les exigences documentaires sont toujours formulées sous la forme d'une **« information documentée à conserver » ou « à tenir à jour ».**

Par exemple, la politique de sécurité de l'information doit exister sous la forme d'une information documentée tenue à jour, tandis que les preuves d'audit interne ou les résultats de mesure d'efficacité sont des informations documentées à conserver.

Catégories de documents dans le SMSI

Il existe plusieurs catégories de documents au sein du SMSI :

- Les documents rédigés : politiques, procédures, fiches de processus, plans ou instructions, qui décrivent la manière d'agir.
- Les enregistrements : preuves concrètes de la réalisation d'activités ou de l'atteinte d'un résultat (rapports, relevés de logs, tableaux de suivi, procès-verbaux, etc.).

Ainsi, une politique peut formaliser des objectifs de sécurité, tandis que les indicateurs et résultats associés à ces objectifs constituent des enregistrements.
Ce qui relie ces deux dimensions, c'est le formalisme : toute information utile au pilotage, à la preuve ou à la maîtrise d'un processus devient une documentation.

Rôle et enjeux de la documentation

En d'autres termes, tout ce qui est écrit, enregistré ou archivé dans le cadre du SMSI relève du domaine documentaire. C'est ce qui permet de rendre le système **visible, vérifiable et maîtrisable.**

Ces notions sont aujourd'hui d'autant plus essentielles que les systèmes d'information modernes intègrent déjà une grande partie de la documentation sous des formes variées : outils de ticketing, plateformes collaboratives, bases de données, solutions RH ou CRM.

De nombreuses informations critiques — preuves d'actions, suivis de conformité, indicateurs — existent déjà dans ces systèmes.

L'enjeu n'est donc plus seulement de créer des documents, mais de les identifier, maîtriser et relier au SMSI.

Une bonne gestion documentaire consiste désormais à intégrer les données issues des systèmes d'information dans une logique de **pilotage, de traçabilité et de preuve**, afin que la sécurité de l'information soit réellement alignée avec les outils et la réalité opérationnelle de l'entreprise.

Cela permet à la fois de simplifier la gestion documentaire mais aussi de **maîtriser l'information partout où elle est présente.**

Les politiques de sécurité

Les politiques sont les documents de plus haut niveau dans le système documentaire. Elles expriment la vision, les engagements et les principes directeurs de l'organisation en matière de sécurité de l'information. Leur rôle est de fixer le cadre de référence qui guidera l'ensemble des processus, des procédures et des actions opérationnelles.

1. La politique de sécurité de l'information (PSI)

La politique de sécurité de l'information (PSI) constitue le document central exigé par la norme ISO 27001. Elle formalise les orientations stratégiques de l'entreprise en matière de sécurité de l'information, ainsi que l'engagement de la direction pour la mise en place, le maintien et l'amélioration continue du système de management de la sécurité de l'information (SMSI) selon la norme ISO27001.

Cette politique traduit les attentes de la direction en objectifs concrets, tels que :

- garantir la confidentialité, l'intégrité et la disponibilité des informations ;
- assurer la conformité réglementaire et contractuelle ;
- prévenir les incidents de sécurité ;
- instaurer une culture de sécurité au sein de l'organisation.

La PSI doit être validée par la direction, diffusée à l'ensemble du personnel ainsi qu'aux parties intéressés concernés, et reconnue comme contraignante : elle engage l'entreprise au plus haut niveau.

Au-delà de cette politique globale, il est recommandé — et souvent obligatoire — de décliner des politiques thématiques pour préciser les principes applicables à certains domaines sensibles. Ces politiques complètent la PSI en définissant les règles et niveaux de sécurité attendus pour des sujets spécifiques.

2. Les politiques thématiques

Les politiques thématiques traduisent le cadre général en exigences opérationnelles adaptées à chaque domaine.

Elles constituent une passerelle entre la vision stratégique et la mise en œuvre quotidienne de la sécurité.

Bien structurées, elles assurent la cohérence dans les pratiques, clarifient les attentes et renforcent la responsabilisation des acteurs.

Elles doivent être courtes, claires et stables dans le temps, tout en étant suffisamment précises pour orienter les procédures et les contrôles.

Ces politiques complètent la PSI en définissant les règles et niveaux de sécurité attendus pour des sujets spécifiques tels que :

- la politique de gestion des accès (droits, habilitations, règles de mot de passe, authentification),
- la politique de protection des données personnelles (RGPD),
- la politique de sécurité des systèmes et réseaux,
- la politique de classification de l'information,
- la politique d'utilisation des ressources informatiques,
- la politique de gestion des fournisseurs et prestataires.

3. Pour les TPE - faire une politique de sécurité des systèmes d'information

Il est tout à fait possible de rédiger un seul document couvrant toutes les politiques de sécurité. applicable à l'ensemble de l'organisation, regroupant tous les sujets de sécurité. Ce document est particulièrement recommandé pour les petites structures, qui peuvent ainsi centraliser toutes leurs règles de sécurité dans un document unique. La PSSI peut également être utilisée comme document de référence à destination des clients, en proposant une synthèse globale des mesures de sécurité mises en œuvre au sein de l'organisation.

Les procédures et documents prescriptifs

Les documents prescriptifs : traduire la politique en actions concrètes

Les documents prescriptifs décrivent comment la politique de sécurité et les exigences du système de management sont appliquées au quotidien. Là où la politique fixe les niveaux de sécurité, ces documents précisent les règles de fonctionnement, les méthodes et les moyens concrets à mettre en œuvre.
Ils constituent le cœur opérationnel de la documentation : c'est à travers eux que l'organisation détermine le **Comment.**

Les procédures : décrire les opérations
La procédure est le document prescriptif le plus courant. Elle définit le mode opératoire ou les règles de fonctionnement à suivre dans un domaine donné. Elle précise comment appliquer la politique, qui intervient, dans quel ordre et avec quels contrôles.

Les procédures traduisent la stratégie en pratiques concrètes, par exemple :

- la procédure de gestion des incidents
- la procédure d'habilitation des utilisateurs
- la procédure de sauvegarde et de restauration.

Leur forme peut varier selon la culture et la taille de l'entreprise : certaines organisations préfèrent des procédures formelles et détaillées, d'autres utilisent des fiches synthétiques, des diagrammes de flux ou des check-lists opérationnelles.

On rencontre aussi d'autres termes équivalents selon les contextes : instructions, modes opératoires, fiches pratiques, etc. L'important est que la procédure soit claire, comprise et applicable par ceux qui doivent la mettre en œuvre.

Les plans : organiser la mise en œuvre et la réponse
Les plans sont des documents prescriptifs orientés vers la préparation, la coordination ou la réponse à des situations particulières. Ils détaillent les ressources, les responsabilités, les actions et les délais à respecter pour atteindre un objectif spécifique.

Dans un SMSI, les plans les plus courants sont :

- Le Plan d'Assurance Sécurité (PAS), qui formalise les mesures de sécurité à appliquer pour un projet, un contrat ou un service donné ;
- Le Plan de Continuité d'Activité (PCA) et le Plan de Reprise d'Activité (PRA), qui définissent la stratégie de maintien ou de restauration des activités critiques en cas d'incident ;
- Le Plan de Sensibilisation ou le Plan de Communication Sécurité, qui encadrent les actions de formation et d'information du personnel.

Ces plans traduisent les engagements de la direction en actions coordonnées et mesurables. Ils assurent la préparation, la cohérence et la réactivité du système de management face aux aléas.

Ensemble, procédures et plans forment la structure opérationnelle du SMSI. Ils permettent de passer de l'intention à l'action, de la stratégie à la pratique, et garantissent que la sécurité de l'information est appliquée de manière cohérente, mesurable et maîtrisée dans toute l'organisation.

Les processus et fiches processus

Les processus : structurer les activités et leurs interactions

Les processus constituent la colonne vertébrale de toute organisation. Ils représentent un ensemble d'activités coordonnées visant à produire un résultat mesurable et prévisible.
Dans le cadre des normes ISO, et particulièrement de l'ISO 27001, les processus permettent de structurer le fonctionnement de l'entreprise et de clarifier les responsabilités.

Les processus de l'organisation

On distingue généralement trois grandes catégories de processus :

- **Les processus métiers,** directement liés à la création de valeur pour les clients (ex. : développement produit, exploitation de services, support client) ;
- **Les processus support,** qui contribuent au bon fonctionnement global de l'organisation (ex. : ressources humaines, informatique, achats, maintenance) ;
- **Les processus de management,** qui assurent la planification, la supervision et l'amélioration du système (ex. : revue de direction, gestion des risques, planification stratégique).

Dans le cadre de l'ISO 27001, il est recommandé de définir cette cartographie des processus qui servira de base à l'analyse des risques et à l'intégration des documents et actions dans l'organisation.

Dans le contexte spécifique de l'ISO 27001, certains processus sont directement orientés vers la sécurité de l'information : le processus de gestion des incidents de sécurité, le processus de contrôle des accès, le processus de gestion documentaire, ou encore le processus d'analyse et de traitement des risques. Ces processus forment la cartographie du SMSI, c'est-à-dire la représentation des activités qui concourent à la mise en œuvre et au pilotage de la sécurité.

La cartographie des processus : comprendre le fonctionnement global

La cartographie des processus est une représentation visuelle de l'organisation, illustrant la manière dont les processus interagissent et s'enchaînent pour produire de la valeur.
Elle constitue un outil de gouvernance et de communication essentiel :

- elle rend l'entreprise lisible,
- permet d'identifier les interdépendances, interfaces et responsabilités,
- et sert de base à la structuration documentaire.

Deux niveaux de cartographie peuvent être distingués :

- la cartographie d'entreprise, qui représente l'ensemble des processus métiers, supports et de management ;
- la cartographie du SMSI, plus ciblée sur les processus liés à la sécurité de l'information et la conformité ISO 27001.

Cette double approche permet d'intégrer la sécurité dans la vie réelle de l'entreprise, en reliant processus techniques et organisationnels à la stratégie globale.

La fiche processus : formaliser le fonctionnement

Chaque processus peut être décrit à l'aide d'une fiche processus, document de référence qui précise les caractéristiques principales. Elle comporte généralement l'objectif du processus (ce qu'il vise à produire ou garantir), le responsable du processus (propriétaire ou pilote), les entrées et sorties (ce que le processus reçoit et produit), les activités principales (les étapes clés du déroulement), les interactions avec d'autres processus ou services, les indicateurs de performance et de conformité, les risques associés et mesures de maîtrise, ainsi que les documents associés (procédures, formulaires, enregistrements).

Les enregistrements : les preuves de la mise en œuvre et des résultats

Les enregistrements constituent les preuves du système de management de la sécurité de l'information. Ils représentent les preuves tangibles que les politiques, processus et procédures sont effectivement appliqués. Ils doivent donc être protégés de toute modification. Dans la terminologie ISO, un enregistrement est une information documentée conservée, c'est-à-dire une donnée qui atteste qu'une activité a été réalisée ou qu'un résultat a été atteint conformément aux exigences du SMSI.
Concrètement, un enregistrement peut prendre des formes variées : rapports d'audit, journaux d'événements (logs), tickets d'incident, procès-verbaux de réunion, registres d'habilitation, relevés de sauvegarde, tableaux de suivi, etc. Ces documents sont essentiels : ils ne décrivent pas ce qu'il faut faire, mais montrent ce qui a été fait.

Deux catégories principales d'enregistrements

On distingue généralement deux types d'enregistrements selon leur finalité :

1. **Les preuves de réalisation d'une activité :** Ce sont les traces laissées par l'exécution d'un processus ou d'une procédure. Exemples : un ticket d'incident clôturé, un rapport de sauvegarde, une feuille de présence à une session de sensibilisation, un compte rendu de revue de direction. Ces enregistrements démontrent que l'action prévue a bien été effectuée selon les règles définies.
2. **Les preuves d'un résultat ou d'une performance :** Ces enregistrements attestent de l'atteinte d'un objectif ou du respect d'un indicateur de sécurité. Exemples : les résultats d'un test de restauration, les rapports d'audit interne, les indicateurs de conformité, ou encore les tableaux de bord du SMSI. Ils permettent d'évaluer l'efficacité du système et d'alimenter la boucle d'amélioration continue.

Ces deux types d'enregistrements sont complémentaires :

- les premiers prouvent l'action,
- les seconds prouvent le résultat.

Ensemble, ils forment la base de la traçabilité et de la crédibilité du SMSI.

Les critères essentiels de gestion des enregistrements

Pour que les enregistrements soient exploitables et fiables, leur gestion doit répondre à plusieurs critères essentiels :

- **Identification claire :** chaque enregistrement doit être identifiable (titre, date, référence, auteur, lien au processus concerné).
- **Intégrité et authenticité :** les enregistrements doivent être protégés contre toute modification non autorisée, altération ou suppression.
- **Accessibilité et disponibilité :** ils doivent être facilement consultables par les personnes autorisées, notamment lors des audits internes ou externes.
- **Confidentialité :** leur accès doit être limité selon les règles de sécurité et de protection des données, certains enregistrements pouvant contenir des informations sensibles.
- **Durée de conservation :** la durée de rétention doit être définie en fonction des exigences légales, contractuelles ou organisationnelles.
- **Support et archivage :** les enregistrements peuvent être conservés sur des supports physiques ou numériques, mais doivent être stockés de manière sécurisée et durable.
- **Lien avec les procédures :** chaque procédure doit préciser les enregistrements attendus, leurs responsables et leurs modalités de gestion.

Dans un SMSI, les enregistrements assurent la traçabilité complète des actions de sécurité, facilitent les audits, renforcent la confiance des parties prenantes et constituent une base objective pour l'amélioration continue.

Les documents d'origine extérieure

L'ISO 27001 impose à toute organisation de maîtriser également les **informations documentées d'origine externe.** Selon la clause 7.5.3 de la norme, « les informations documentées d'origine externe que l'organisation juge nécessaires à la planification et au fonctionnement du système de management de la sécurité de l'information doivent être identifiées comme il convient et contrôlées. »

Autrement dit, le SMSI ne se limite pas aux documents internes : il doit aussi intégrer et gérer correctement toutes les sources externes d'information qui influencent la sécurité, la conformité ou les pratiques de l'entreprise.

1. Qu'est-ce qu'une information documentée d'origine externe ?
Il s'agit de tout document ou donnée émis par une partie externe (client, fournisseur, autorité, organisme de certification, etc.) et utilisé par l'organisation dans le cadre du SMSI.
Ces documents peuvent contenir des exigences, des engagements contractuels, des réglementations ou des données techniques nécessaires au fonctionnement du système.
Ils jouent souvent un rôle clé dans la conformité et la relation de confiance avec les partenaires externes.

2. Exemples d'informations documentées d'origine externe
Voici quelques exemples typiques à maîtriser :

- Contrats clients et exigences contractuelles : clauses de sécurité, accords de confidentialité (NDA).
- Contrats fournisseurs et prestataires : politiques de sécurité fournisseurs ou clients, plans d'assurance sécurité fournisseurs, rapports d'audit SOC 2 ou ISO 27001 des prestataires cloud.
- Textes réglementaires et légaux : RGPD, directives NIS2, IA ACT.
- Référentiels normatifs et guides : normes ISO applicables (ISO 27002, ISO 22301, ISO 27701, ISO 42001), guides de l'ANSSI ou de l'ENISA, recommandations de la CNIL.
- Documents techniques ou administratifs externes : manuels utilisateurs d'outils critiques, certificats de conformité produits, rapports de tests d'intrusion réalisés par un tiers, plans d'assurance sécurité partenaires.

3. Comment les identifier et les contrôler
La maîtrise de ces documents externes est essentielle pour garantir la cohérence et la fiabilité du système de management.
Voici les principales bonnes pratiques :

- Identification : chaque document externe pertinent doit être clairement identifié dans le registre documentaire (origine, type, référence, propriétaire interne, usage).
- Accès contrôlé : limiter l'accès à ces documents aux seules personnes concernées, tout en garantissant leur disponibilité lorsqu'ils sont nécessaires.
- Mise à jour : vérifier régulièrement que les versions utilisées sont à jour (ex. : nouvelle version d'une norme, d'un contrat ou d'une réglementation).
- Archivage : conserver les anciennes versions lorsque cela est nécessaire pour la traçabilité (notamment en cas de litige ou d'audit).
- Intégration documentaire : relier ces documents aux processus ou politiques internes correspondants (par exemple, rattacher un contrat client à la procédure de gestion des exigences contractuelles).

4. Conseils pratiques

- Centralisez ces documents dans un espace sécurisé (GED, plateforme documentaire, outil comme Oversecur) avec des métadonnées claires.
- Établissez un responsable par type de document externe (ex. : juridique pour les contrats, RSSI pour les normes, conformité pour la réglementation).
- Automatisez les alertes de mise à jour, surtout pour les contrats et les réglementations.
- Créez une procédure spécifique de "Gestion des informations documentées d'origine externe" pour encadrer ces pratiques et répondre précisément à l'exigence ISO 27001.
- En audit, soyez en mesure de démontrer où et comment ces documents sont identifiés, contrôlés et utilisés dans le SMSI.

Exigence ISO 27001 : clause 7.5 – “Information documentée” 1/2

La clause 7.5 de la norme ISO 27001 définit les exigences générales applicables à la documentation du système de management de la sécurité de l’information (SMSI).
Elle encadre la manière dont les informations documentées doivent être créées, mises à jour et contrôlées, afin de garantir leur fiabilité, accessibilité et intégrité.
Cette clause constitue la base du pilotage documentaire du SMSI : elle précise non seulement quoi documenter, mais aussi comment le faire.
Nous allons, sur deux pages, vous expliquer comment interpréter cette clause et l’adapter à votre organisation.

Exigence - 7.5.1 – Généralités : ce qu’il faut documenter
L’organisation doit inclure dans son SMSI :
a) les informations documentées exigées par la norme ISO 27001
(ex. : politique de sécurité, déclaration d’applicabilité, plan de traitement des risques, résultats d’audits, etc.) ;
b) les informations documentées que l’organisation juge nécessaires à l’efficacité du système
(ex. : procédures internes, guides, check-lists, tableaux de suivi, etc.).

Autrement dit, la norme fixe un socle minimum, mais chaque organisation reste libre d’adapter le niveau de formalisme selon ses besoins.
La documentation doit donc être proportionnée à la taille, à la complexité et à la maturité du système.
Une note associée précise que l’étendue de la documentation dépend de trois facteurs principaux :

- La taille de l’organisation, ses activités, produits et services ;
- La complexité des processus et de leurs interactions ;
- La compétence des personnes (plus les collaborateurs sont autonomes et formés, moins le formalisme nécessaire est lourd)

En résumé, un petit organisme peut avoir une documentation allégée, tandis qu’un grand groupe ou un environnement complexe exigera un système documentaire plus complet et structuré.

7.5.2 – Création et mise à jour : garantir la qualité des documents
Lors de la création ou de la mise à jour des informations documentées, l’organisation doit s’assurer de leur qualité et de leur traçabilité.
Trois critères fondamentaux sont à respecter :
a) Identification et description : chaque document doit comporter un titre clair, une date, un auteur, un numéro ou code de référence, et idéalement un lien avec le processus concerné.
b**) Format et support :** les documents peuvent être sur papier ou électroniques, en texte, schéma, tableau, ou tout autre format adapté (langue, version logicielle, etc.).
c) Revue et approbation : tout document doit être vérifié et validé avant sa diffusion, pour s’assurer de sa pertinence et de sa conformité. Il faudra également suivre les revues documentaires.

Ces exigences garantissent la crédibilité du système documentaire et permettent d’éviter les doublons, les erreurs de version ou les incohérences.

Exigence ISO 27001 : clause 7.5 – “Information documentée 2/2

7.5.3 – Contrôle des informations documentées : assurer la maîtrise

Une fois créées, les informations documentées doivent être contrôlées pour en garantir la disponibilité, la confidentialité et l’intégrité.

La norme impose de s’assurer que :

- les documents sont disponibles là où ils sont nécessaires (par exemple, lors d’un audit, d’un incident ou d’une revue de direction). Et surtout qu’ils soient communiqués au bon endroit pour les collaborateurs tout en respectant le besoin de savoir.
- ils sont protégés contre toute perte, altération ou accès non autorisé.

Pour ce faire, plusieurs activités doivent être mises en œuvre :

- Distribution, accès, récupération et utilisation : définir qui peut consulter ou modifier un document, et selon quelles autorisations ;
- Stockage et conservation : garantir la lisibilité et la pérennité des documents, quel que soit le support utilisé ;
- Contrôle des modifications : assurer un suivi clair des versions (numérotation, historique des révisions, auteur des modifications) ;
- Durée de conservation et suppression : définir combien de temps chaque document est conservé, et selon quel mode il est archivé ou supprimé.

L’organisation doit également maîtriser les informations documentées d’origine externe qu’elle juge nécessaires à la planification et au fonctionnement du SMSI (par exemple, les contrats clients, réglementations, référentiels, ou rapports fournisseurs). Ces documents externes doivent être identifiés et contrôlés au même titre que les documents internes.

Enfin, la note précise que la notion d’accès implique différents niveaux d’autorisation : certains utilisateurs peuvent seulement consulter, d’autres peuvent modifier ou approuver selon leur rôle dans le système.

En résumé

La clause 7.5 impose à l’organisation de mettre en place une gestion documentaire structurée et maîtrisée, garantissant :

- la traçabilité des documents (qui les a créés, quand et pourquoi) ;
- leur accessibilité et leur protection ;
- leur mise à jour continue ;
- et leur alignement avec les exigences de la norme et les besoins internes.

La bonne application de cette clause est essentielle : elle conditionne la cohérence, la fiabilité et la durabilité du SMSI.

Nous avons dans ce guide donné tous les conseils pour mettre en pratique cette documentation.
En pratique, un outil de gestion documentaire centralisé (GED, plateforme collaborative, ou solution comme **Oversecur**) facilite grandement le respect de ces exigences et la démonstration de conformité lors des audits.

Le processus de gestion documentaire 1/3

La gestion documentaire : socle du SMSI

La gestion documentaire constitue le socle de tout système de management efficace.
Dans un SMSI (Système de Management de la Sécurité de l'Information), elle garantit la cohérence des pratiques, la traçabilité des décisions et la maîtrise de l'information. Ce n'est pas une simple exigence administrative, mais un mécanisme vivant qui structure la gouvernance et assure que la sécurité repose sur des bases fiables et vérifiables.

Pourquoi un processus de gestion documentaire ?

La norme ISO 27001 exige que l'organisation maîtrise ses informations documentées, c'est-à-dire toutes les données qui servent à décrire, appliquer et prouver le fonctionnement du système.
Ce processus a deux grands objectifs :

- **Assurer la cohérence et la conformité :** chaque document doit refléter les pratiques réelles et être aligné avec les exigences du SMSI.
- **Garantir la traçabilité et la maîtrise :** à tout moment, l'organisation doit savoir quels documents sont en vigueur, qui les a validés, et où les trouver.

Une bonne gestion documentaire permet donc de disposer d'un système réel, où politiques, procédures et enregistrements évoluent avec les pratiques de l'entreprise.

Les étapes du cycle de vie documentaire

La gestion documentaire suit un cycle de vie structuré, inspiré du principe PDCA (Plan-Do-Check-Act). Chaque étape vise à garantir la fiabilité et la pertinence de l'information.

1. Création et validation

Tout commence par la rédaction du document. L'auteur (souvent le responsable du processus concerné) formalise les pratiques, les règles ou les méthodes.
Le document est ensuite vérifié par un acteur compétent (RSSI, responsable qualité, manager) qui s'assure qu'il est applicable, compréhensible et conforme aux exigences normatives.
Il est enfin approuvé par une autorité désignée (direction, RSSI ou responsable de domaine) qui en autorise la diffusion officielle.
Cette chaîne de validation — rédacteur, vérificateur, approbateur — assure un double contrôle : sur le fond (pertinence du contenu) et sur la forme (cohérence avec la charte documentaire).

2. Diffusion et accessibilité

Une fois approuvé, le document doit être facilement accessible à ceux qui en ont besoin.
La diffusion se fait aujourd'hui préférentiellement par des plateformes collaboratives (SharePoint, Oversecur, GED interne) permettant de maîtriser les accès et les droits de modification.
Chaque collaborateur doit pouvoir trouver rapidement le bon document, dans sa version à jour.
Un document introuvable ou obsolète est aussi problématique qu'un document inexistant.

Le processus de gestion documentaire 2/3

3. Mise à jour et révision
Un document n'est jamais figé. Il doit évoluer avec les pratiques, les technologies ou les exigences réglementaires.
Le RSSI (ou le propriétaire du document) veille à ce qu'une revue périodique ait lieu au moins une fois par an.
Toute modification suit le même processus de validation que la création initiale.
Les versions précédentes sont archivées afin de conserver une trace du raisonnement et des évolutions — un élément crucial lors des audits.

4. Archivage et suppression
Les documents obsolètes ne doivent pas disparaître sans contrôle.
Ils sont archivés pendant une durée déterminée (par exemple 10 ans), puis supprimés de manière sécurisée et tracée.

L'organisation doit pouvoir prouver qu'elle maîtrise le cycle de vie complet : de la création à la destruction.
Attention à bien respecter les règles de conservation et d'archivage légaux.

Les rôles dans la gestion documentaire

Le succès d'un système documentaire repose sur une claire répartition des rôles :

- **Le rédacteur :** connaît le processus, traduit les pratiques en consignes écrites, veille à la clarté du message.
- **Le vérificateur :** garant de la cohérence, vérifie que le document est applicable, conforme et compréhensible.
- **L'approbateur :** engage la direction en validant la version finale.
- **Le RSSI :** supervise le processus global, s'assure que le système reste cohérent et que les documents critiques sont bien gérés.

Cette gouvernance évite les erreurs de version, les incohérences et les décisions non tracées.

L'importance du registre documentaire

Pour maîtriser l'ensemble, il est essentiel de tenir un registre documentaire.
Ce registre agit comme une carte du système documentaire : il recense tous les documents actifs, leur version, leur propriétaire, leur statut et leur emplacement.
Il permet aussi d'identifier les dépendances entre les politiques, procédures et plans, et d'éviter les doublons.
Lors d'un audit, ce registre constitue une preuve précieuse : il démontre la maîtrise du système et la capacité de l'organisation à garantir la cohérence de sa documentation.

Le processus de gestion documentaire 3/3

Les documents d'origine externe

Les documents d'origine externe occupent une place particulière : ce sont les informations émanant de tiers (clients, fournisseurs, autorités, organismes de certification, etc.) et nécessaires au bon fonctionnement du SMSI.
Cela inclut les contrats clients, les exigences réglementaires, les rapports d'audit externes, ou encore les normes et guides applicables.
Ces documents doivent être identifiés, contrôlés et mis à jour au même titre que les documents internes.
Ils doivent figurer dans le registre documentaire, avec leur origine, leur date de validité et le responsable interne chargé de leur suivi (juridique, RSSI, conformité, etc.).
Une négligence dans la gestion des documents externes peut avoir des conséquences importantes : non-respect contractuel, perte de conformité, ou erreurs d'interprétation réglementaire.

Traçabilité, protection et amélioration continue

La norme ISO 27001 met un accent fort sur la protection et la traçabilité des informations documentées.
Cela signifie que l'organisation doit être capable de garantir à tout moment :

- L'intégrité (aucune modification non autorisée),
- La confidentialité (accès limité aux personnes habilitées),
- La disponibilité (accès possible quand nécessaire).

Les outils numériques modernes facilitent cette maîtrise : versionnage automatique, workflows d'approbation, historisation, alertes de révision.

Mais la technologie ne suffit pas : la discipline documentaire dépend avant tout de la culture organisationnelle.
L'audit interne joue ici un rôle essentiel : il permet de vérifier régulièrement que les documents sont bien maîtrisés, que les versions sont à jour et que les pratiques suivent le processus prévu.

Des indicateurs simples — taux de documents à jour, nombre de non-conformités documentaires, délai moyen de validation — permettent de suivre la performance du processus et d'alimenter la revue de direction.

Une démarche vivante, pas une contrainte

Trop souvent, la gestion documentaire est perçue comme un exercice administratif lourd.
En réalité, bien menée, elle devient un outil de pilotage : elle structure les responsabilités, clarifie les pratiques et renforce la confiance dans le système.
Un document bien rédigé, clair et accessible, facilite le travail quotidien et simplifie la formation des nouveaux collaborateurs.

C'est aussi un moyen puissant de démontrer la maturité du SMSI : lors d'un audit, un corpus documentaire cohérent est souvent la première preuve tangible d'une gouvernance efficace.
La documentation n'est donc pas une fin en soi : c'est le langage commun du management de la sécurité.
Elle relie la stratégie, les processus et les actions, pour que la sécurité ne soit plus un sujet implicite, mais un système visible, maîtrisé et durable.

Notre solution Oversecur permet de réaliser ce processus de façon collaborative

La classification des documents et la confidentialité

La classification des documents et la confidentialité

Dans un Système de Management de la Sécurité de l'Information (SMSI), tous les documents n'ont pas la même sensibilité. Certains contiennent des informations publiques ou anodines, d'autres renferment des données stratégiques, confidentielles ou à caractère personnel. C'est pourquoi la classification de l'information constitue une étape essentielle du pilotage documentaire et un lien direct avec les exigences de l'ISO 27001.

1. Pourquoi classifier les documents ?

La classification vise à adapter les mesures de protection au niveau de sensibilité des informations contenues dans un document. Sans classification claire, la confidentialité repose sur des **habitudes individuelles,** et non sur une politique maîtrisée.

2. Les niveaux de classification les plus courants

Chaque organisation définit ses propres niveaux, mais une structure à quatre catégories reste la plus répandue et cohérente avec les bonnes pratiques ISO 27001 :

Niveau	Exemple de contenu	Exigences de protection
Public	Documents de communication externe, plaquettes, politiques publiques	Diffusion libre, pas de restriction d'accès
Interne	Procédures, guides, politiques internes, fiches processus	Accès limité aux collaborateurs
Confidentiel	Rapports d'audit, plans de sécurité, SoA, analyse de risques	Accès restreint selon le besoin de connaître ("need to know")
Strictement confidentiel / sensible	Données clients, informations personnelles, contrats sensibles	Chiffrement, restrictions d'accès, stockage sécurisé, traçabilité des consultations

Chaque document du SMSI (politique, procédure, enregistrement) doit indiquer clairement son niveau de classification. Cette information figure dans le bandeau, la page de garde ou les métadonnées du fichier.

3. Lien avec les exigences ISO 27001

La classification documentaire répond directement à une exigence de l'annexe A :

- **Annexe A.5.12** – **"Classification de l'information"** : les informations doivent être classées en fonction de leur valeur, de leur sensibilité et des conséquences d'une divulgation non autorisée.

Elle permet d'appliquer la politique de sécurité à l'ensemble des documents, et pas seulement aux systèmes informatiques :

- Définir une politique de classification simple, partagée et appliquée à tous les types de documents (papier et numérique).
- Indiquer la classification directement dans chaque document (page de garde ou métadonnée).
- Limiter les accès dans les outils de GED selon le niveau de sensibilité.
- Former les collaborateurs à la manipulation et au partage des documents selon leur classification.
- Revoir régulièrement la classification des documents critiques lors des mises à jour ou des changements d'activité.

Cette démarche garantit que chaque information du SMSI — qu'il s'agisse **d'une politique, d'une procédure, d'un rapport d'audit ou d'un contrat** — bénéficie du niveau de sécurité adapté à sa valeur et à son risque. Bien appliquée, elle renforce la confidentialité, facilite la conformité ISO 27001 et contribue à la maturité globale du système de management de la sécurité de l'information.

L'intégration réglementaire dans la documentation

La documentation d'un **Système de Management de la Sécurité de l'Information (SMSI)** ne peut pas être conçue sans intégrer les contraintes réglementaires.
Elle s'inscrit dans un écosystème réglementaire, contractuel et normatif qui influence directement son contenu, sa structure et ses exigences de preuve.
L'un des rôles essentiels du processus documentaire est donc d'assurer la cohérence entre les exigences ISO 27001 et les obligations légales ou normatives qui s'appliquent à l'organisation. Et parfois même produire les documents exigés par la règlementation s'ils concernent la sécurité de l'information.

Prendre en compte les obligations légales et contractuelles

Toute entreprise est soumise à un ensemble d'obligations qui doivent être traduites dans son système documentaire. Ces exigences ne sont pas seulement juridiques : elles façonnent les politiques, les procédures et les enregistrements du SMSI.

- **Le RGPD (Règlement Général sur la Protection des Données)** impose la documentation de la conformité : registre des traitements, procédures d'exercice des droits, gestion des violations de données, clauses contractuelles avec les sous-traitants, etc. Ces éléments peuvent être intégrés directement dans le SMSI, notamment dans les politiques de sécurité et les plans de gestion des incidents.
- **Le droit du travail** encadre la protection des données des salariés, la sensibilisation à la sécurité et les modalités de contrôle. Les chartes d'utilisation du système d'information, les règles internes et les politiques RH doivent être documentées et validées par les instances concernées.
- **Les clauses contractuelles clients** constituent souvent des obligations documentées : exigences de reporting sécurité, plan d'assurance sécurité, tests de vulnérabilité, niveaux de service, conformité RGPD ou certification ISO exigée. Ces éléments doivent être recensés et suivis dans la documentation du SMSI (par exemple dans le registre des exigences externes).

En d'autres termes, la documentation du SMSI devient le lien entre les obligations externes et la conformité interne. Elle permet de prouver que l'organisation sait identifier, formaliser et maîtriser ses engagements légaux et contractuels.

Le rôle du juriste dans la conformité documentaire

Dès qu'un document touche à des aspects légaux ou contractuels, il est fortement recommandé de faire valider son contenu par un juriste.
Cela concerne notamment les politiques de confidentialité, les clauses contractuelles clients ou fournisseurs, et les engagements de conformité (RGPD, sécurité, sous-traitance).
Selon votre secteur, cette relecture peut être essentielle : un juriste spécialisé e-santé, fintech ou secteur public saura adapter la documentation aux exigences réglementaires propres à votre domaine.
Cette vérification juridique garantit que vos documents ne présentent ni risque légal, ni non-conformité réglementaire, et qu'ils protègent efficacement votre organisation.

En conclusion, la documentation n'est pas un simple outil de conformité : c'est le point de convergence entre les exigences ISO, les obligations réglementaires et les engagements contractuels.

Bien intégrée, elle devient un levier stratégique pour piloter simultanément la qualité, la sécurité, la protection des données, tout en offrant une vision claire et maîtrisée de la conformité globale de l'organisation.

L’intégration normative et le lien avec les autres certifications

Articuler la documentation avec les autres normes ISO

La norme ISO 27001 fait partie d’un ensemble cohérent de référentiels ISO partageant la même structure de haut niveau (HLS – High Level Structure).
Cela facilite une intégration documentaire multi-normes, essentielle pour éviter la duplication et renforcer la cohérence du management global.

- **ISO 9001** – Management de la qualité : les deux normes reposent sur les mêmes principes de management et la même architecture documentaire. Les politiques, les revues de direction, la gestion documentaire et les audits internes peuvent être mutualisés.
  - Une procédure unique de gestion documentaire peut couvrir à la fois les exigences qualité et sécurité.
- **ISO 27701** – Management de la protection des données personnelles : cette extension de la 27001 introduit la notion de “rôles RGPD” (responsable de traitement, sous-traitant) et demande de documenter la gouvernance des données personnelles.
  - Les politiques de sécurité et de confidentialité doivent intégrer ces exigences, tout en s’appuyant sur les procédures déjà en place dans le SMSI.
- **ISO 22301** – Management de la continuité d’activité : cette norme complète la 27001 sur la gestion de crise et la résilience.
  - Les plans de continuité, les procédures de reprise et les enregistrements de tests sont des documents communs aux deux systèmes et peuvent être intégrés dans le référentiel documentaire du SMSI.
- **ISO 42001** – Management de l’IA : centrée sur la gouvernance des systèmes d’intelligence artificielle, cette norme introduit de nouveaux types de documentation (évaluation des impacts, registres d’IA, politique d’éthique et d’explicabilité).
  - Elle s’appuie sur les mêmes principes de documentation que la 27001 : preuve, traçabilité, validation et mise à jour contrôlée.

L’intérêt de cette approche intégrée est de rationaliser la gestion documentaire : une même structure, des modèles communs, et des processus partagés permettent de répondre à plusieurs référentiels simultanément.

Vers une documentation intégrée et cohérente

Une organisation mature ne gère plus ses référentiels de manière indépendante : elle construit une cartographie documentaire unifiée, où chaque document sert plusieurs cadres.

Par exemple :

- Une politique de sécurité peut répondre à la fois aux exigences ISO 27001 et 27701.
- Un registre de risques peut couvrir les aspects sécurité (27001), continuité (22301) et IA (42001).
- Une procédure de gestion documentaire unique peut servir de socle commun à toutes les normes.

Cette intégration documentaire permet :

- de réduire la complexité du système de management ;
- d’assurer la cohérence entre les exigences légales, normatives et internes ;
- de renforcer la lisibilité du corpus documentaire pour les collaborateurs comme pour les auditeurs ;
- et de faciliter la conformité continue, en évitant la duplication et l’obsolescence des documents.

Technologie et outils de gestion documentaire

La maîtrise documentaire ne repose pas uniquement sur des règles et des processus : elle s'appuie de plus en plus sur des outils technologiques capables **d'automatiser, de tracer et de sécuriser le cycle de vie des documents.**
Les plateformes modernes de gestion électronique de documents (GED) et les solutions intégrées de management jouent un rôle central dans l'efficacité et la conformité du SMSI.
Elles permettent non seulement de gagner en fiabilité, mais aussi de démontrer facilement la maîtrise documentaire lors des audits.

1. Les solutions de GED et plateformes intégrées

Les systèmes de GED (Gestion Électronique de Documents) offrent un environnement structuré pour créer, stocker, classer, versionner et diffuser les documents de manière sécurisée.
Parmi les solutions les plus couramment utilisées :

- **Oversecur**, qui intègre la gestion documentaire dans une logique de conformité multi-normes (ISO 27001, 9001, 27701, 42001, etc.), avec fonctions de suivi, d'approbation et de génération automatique de rapports d'audit.
- **Microsoft SharePoint**, souvent utilisé pour centraliser les documents du SMSI, gérer les droits d'accès et les flux de validation.
- **Confluence**, qui facilite la rédaction collaborative, la documentation vivante et le lien direct avec les processus opérationnels.

Ces plateformes remplacent avantageusement les répertoires partagés classiques, en apportant traçabilité, cohérence et sécurité.
Elles assurent la conservation des métadonnées (auteur, version, date, statut) et garantissent que chaque utilisateur accède à la bonne version du document, au bon moment.

2. Les fonctionnalités clés à intégrer

Un système documentaire efficace ne se limite pas à stocker des fichiers. Les outils modernes offrent des fonctionnalités essentielles qui répondent directement aux exigences de la clause 7.5 de l'ISO 27001 :

- Signature électronique : permet d'assurer la validité et la traçabilité des approbations (utile pour les politiques, plans de sécurité, procédures critiques).
- Historisation et versionnage : chaque modification est enregistrée, avec la possibilité de revenir à une version antérieure et d'auditer le cycle de validation.
- Alertes et échéances : rappels automatiques pour les revues documentaires, les mises à jour périodiques ou les renouvellements de politiques.
- Workflows de validation : circuits d'approbation automatisés (rédacteur → vérificateur → approbateur), réduisant les erreurs et accélérant la publication.
- Recherche intelligente et filtrage : classification par type de document, processus, domaine ISO ou date de mise à jour.
- Gestion des accès : contrôle fin des droits de lecture, modification ou approbation selon les rôles, garantissant la confidentialité et l'intégrité des informations.
- Archivage sécurisé : conservation automatique des anciennes versions et suppression contrôlée à échéance.

Ces fonctionnalités rendent le système documentaire vivant, pilotable et conforme aux bonnes pratiques ISO.

Technologie et outils de gestion documentaire

3. L'automatisation au service du pilotage

L'apport de la technologie dépasse la simple gestion des fichiers.
Les outils de GED modernes, **ou les plateformes intégrées comme Oversecur**, permettent d'automatiser la gestion documentaire dans une logique de pilotage :

- génération automatique des registres de documents ;
- suivi en temps réel des documents à réviser ;
- notifications au RSSI et aux propriétaires de processus ;
- reporting consolidé pour les audits internes et revues de direction.

Cette automatisation libère les équipes des tâches répétitives et réduit les risques d'erreurs manuelles (oubli de mise à jour, mauvaise version utilisée, etc.).
Elle favorise une approche préventive et proactive de la conformité documentaire.

4. La sécurité de l'information dans les outils

Parce qu'ils centralisent souvent des informations sensibles, ces outils doivent eux-mêmes respecter des exigences fortes de sécurité :

- hébergement sécurisé et conformité RGPD ;
- sauvegarde et redondance des données ;
- gestion des habilitations et des authentifications (MFA, SSO) ;
- journalisation des accès et traçabilité complète des actions.

Le choix d'un outil doit donc tenir compte du niveau de sensibilité des documents gérés et des exigences contractuelles ou sectorielles de l'organisation (ex. : HDS pour la santé, SecNumCloud pour le cloud souverain).

5. Vers une documentation connectée et intelligente

L'évolution actuelle va au-delà de la simple GED : les systèmes de management modernes tendent vers une documentation connectée, reliée aux processus, aux risques et aux plans d'action.
Par exemple, dans Oversecur, chaque document peut être relié à un contrôle de l'annexe A, à un risque identifié ou à un plan de traitement.
Cette approche intégrée transforme la documentation en outil de pilotage en temps réel de la conformité et de la performance du SMSI.
Demain, l'intelligence artificielle contribuera encore à cette dynamique : analyse des versions, détection des incohérences, génération automatique de modèles documentaires ou assistance à la rédaction conforme ISO.

En résumé

Les outils de gestion documentaire sont un levier essentiel pour la maturité d'un SMSI. Ils garantissent la traçabilité, la conformité et la réactivité du système, tout en simplifiant la vie des utilisateurs.
Bien choisis et bien configurés, ils permettent de passer d'une documentation subie à une documentation pilotée, intégrée et sécurisée, au service de la gouvernance et de l'efficacité globale du système de management.

ROADMAP

Le processus d'implémentation

03

Le processus de déploiement

Intégrer la documentation dans la mise en place du SMSI

La documentation n'est pas une étape isolée du projet ISO 27001 : elle doit être intégrée à chaque étape.
Une erreur fréquemment observée consiste à vouloir rédiger dès le départ l'ensemble du corpus documentaire exigé par la norme. Cette approche conduit souvent à un décalage entre la documentation produite et les besoins réels du système de management ou de la certification.

Le résultat est une **sur-documentation inutile ou des documents mal adaptés,** qui ne reflètent ni les pratiques de l'organisation ni les exigences effectives du SMSI.

Plutôt que de rédiger les documents à la fin du projet, la bonne approche consiste à intégrer le processus documentaire dès le démarrage, au fil des étapes de mise en œuvre du système de management de la sécurité de l'information (SMSI).

Une approche intégrée à chaque étape du projet

L'idée est simple : à mesure que le SMSI se construit, la documentation se structure.
On ne rédige pas tout d'un bloc, mais au rythme des jalons du projet.

- **Lors du diagnostic initial,** on identifie les documents existants, les manques, les sources d'information et les acteurs clés.
- **Lors de la phase de lancement et de cadrage**, l'objectif est d'établir le contexte du SMSI et d'identifier les parties intéressées ainsi que leurs exigences.
- **Lors de la phase d'analyse de risques**, on identifie de manière détaillée les documents nécessaires à la maîtrise des risques. A cette étape, nous allons vérifier qu'aucun document n'est absent pour répondre aux exigences normatives et règlementaires
- **Lors de la phase de définition du SMSI,** on entre dans le cœur de la construction documentaire. C'est à ce moment-là que l'on rédige la majorité des documents : politiques, processus, procédures, plans de continuité, etc. L'objectif est de décrire précisément le fonctionnement du système, tout en répondant aux exigences de l'annexe A de la norme ISO 27001.
- lors de la phase de mise en oeuvre, nous allons nous assurer du respects des documents et de la production des preuves.
- Enfin, lors des audits internes et des revues de direction, la documentation joue son rôle de preuve de conformité et d'outil de pilotage.

Les documents deviennent prêts : mis à jour, commentés, améliorés à chaque cycle de vérification. Ainsi, la documentation accompagne chaque étape du projet ISO 27001. Ile se construit en parallèle du système, en lien étroit avec la réalité opérationnelle.

Les bénéfices de cette approche intégrée

- Gain de temps et de cohérence : les documents sont produits au moment où les décisions sont prises, ce qui évite les rédactions "a posteriori" déconnectées du terrain.
- Appropriation par les équipes : les acteurs du projet participent à la création documentaire, favorisant une meilleure compréhension et une utilisation effective.
- Qualité et conformité : la documentation reflète fidèlement la réalité du SMSI, réduisant le risque d'écart en audit.
- Amélioration continue : le processus documentaire s'inscrit dans la dynamique PDCA — il évolue en même temps que le système.

Votre roadmap projet et la documentation

Étape	Objectif de l'étape	Lien avec la documentation
1 - Diagnostic et feuille de route	Cette première étape permet de comprendre comment la norme s'applique à votre organisation et d'adapter son cadre à votre contexte spécifique.	Recensement des documents existants, identification des manques en termes de documentation. Identifier le périmètre règlementaire et les documentations applicables. Sensibiliser les équipes sur les bonnes pratiques documentaires
2 - Cadrage du SMSI (1 mois)	Définir le contexte, les objectifs, les parties intéressées, le périmètre du SMSI et la gouvernance du projet.	Formalisation des documents de cadrage : **procédure de gestion documentaire**, politique de sécurité initiale, plan projet, cartographie des parties intéressées, domaine d'application.
3 - Analyse des risques (1 mois)	Identifier, évaluer et hiérarchiser les risques sur les actifs d'information. Déterminer les traitements à mettre en œuvre.	Élaboration de la méthode de gestion des risques, registre des actifs, critères d'impact et de vraisemblance, plan de traitement. Identification des documents nécessaires pour traiter les risques.
4. Définition du SMSI (2 à 6 mois)	Construire la structure du SMSI, définir les processus, politiques, procédures et plans nécessaires à la maîtrise des risques et à la conformité.	Rédaction du corpus documentaire principal : politiques, procédures, processus, plans de continuité, fiches processus, déclarations d'applicabilité. Réponses documentées à l'annexe A.
5. Mise en place du SMSI (1 à 3 mois)	Déployer les mesures définies, former les équipes, appliquer les procédures et suivre les indicateurs.	Production des enregistrements : preuves d'application, rapports d'audit interne, comptes rendus de comités, indicateurs de suivi, registres opérationnels.
6. Audit blanc (1 semaine)	Vérifier la conformité du système avant l'audit de certification, identifier les non-conformités et les points d'amélioration.	Compilation et vérification de l'ensemble du corpus documentaire. Relecture critique des documents clés (SoA, politiques, plans). Liste les ajustements et corrections sous forme de non-conformités.
7. Préparation audit et revue de direction (3 semaines)	Finaliser les actions, valider l'efficacité du SMSI, démontrer la conformité à la direction et aux auditeurs.	Mise à jour des documents en fonction des non-conformités. Production du rapport de revue de direction, synthèse documentaire, mise à jour des plans d'action et des indicateurs. Organisation des preuves pour l'audit.
8. Audit de certification	**Évaluation formelle par un organisme tiers de la conformité du SMSI à la norme ISO 27001.**	Présentation et mise à disposition de l'ensemble de la documentation exigée. Traçabilité des preuves, registres et rapports. Ajustements post-audit selon les observations.

Étape 1 - le diagnostic et la feuille de route

Poser les bases documentaires

Le diagnostic initial constitue la première étape clé du projet ISO 27001.
Au-delà de l'évaluation du niveau de conformité et de la définition de la feuille de route, cette phase joue un rôle fondamental dans la construction du futur système documentaire.
Elle permet de dresser un état des lieux précis, d'identifier ce qui existe déjà, ce qui manque, et de préparer la structuration du corpus documentaire qui accompagnera tout le projet.

1. Identifier les documents existants

Le diagnostic commence souvent par une exploration de la documentation déjà en place dans l'organisation :

- de documents de sécurité déjà rédigés (politique de sécurité, procédures techniques, etc.)
- de documents internes comme un règlement intérieur, une charte informatique…
- de clauses contractuelles intégrant des exigences de sécurité avec les clients et fournisseurs
- de documents liés au RGPD (registre des traitements, politique de confidentialité, …).

Cette étape permet d'identifier les points d'appui existants et d'éviter de repartir de zéro.
Les documents déjà conformes ou partiellement exploitables peuvent être intégrés au plan d'action documentaire dès le lancement du projet.

2. Identifier les manques et structurer le plan documentaire

En parallèle, le diagnostic permet de repérer les lacunes documentaires : procédures absentes, politiques non formalisées, enregistrements inexistants ou non maîtrisés.
Cette analyse débouche sur la création d'un plan documentaire précisant :

- les types de documents à produire (politiques, procédures, plans, registres, etc.) ;
- les modèles et outils à utiliser (GED, modèles Word, templates dans Oversecur, etc.) ;
- les rôles et responsabilités dans la rédaction et la validation.

Ce plan devient la feuille de route documentaire du projet ISO 27001 et accompagne toutes les étapes suivantes.

3. Sensibiliser et impliquer les acteurs

Le diagnostic joue également un rôle de prise de conscience.
C'est souvent la première fois que la direction et les collaborateurs mesurent l'ampleur du travail documentaire à venir.
Cette étape permet donc d'expliquer la logique de la documentation ISO 27001 : pourquoi elle est essentielle, comment elle va structurer l'organisation, et comment chacun sera impliqué.

En résumé

L'étape de diagnostic n'est pas seulement un audit de départ : c'est le socle du système documentaire.
Elle permet de recenser, évaluer et planifier la documentation nécessaire à la mise en œuvre du SMSI.
C'est à partir de cette analyse que se construit la cohérence entre les exigences normatives, les pratiques existantes et les besoins réels de l'entreprise.
Bien menée, cette première étape garantit que la documentation ISO 27001 ne sera pas un exercice théorique, mais le reflet concret et maîtrisé du fonctionnement de l'organisation.

Étape 2 - Cadrage du SMSI : définir le cadre documentaire et les fondations du système

Après le diagnostic, la phase de cadrage du SMSI marque le véritable lancement du système de management de la sécurité de l'information.
C'est à ce moment que l'on définit le contexte, le périmètre, les enjeux, les objectifs et les parties intéressées, mais aussi la structure documentaire qui soutiendra l'ensemble du système.
Cette étape est essentielle, car elle pose les règles du jeu : comment les documents vont être créés, validés, diffusés et tenus à jour tout au long du projet.
C'est ici que commence réellement la production des premiers documents officiels du SMSI.

1. La procédure de gestion documentaire : le premier document à rédiger

Le premier document à formaliser à ce stade est la procédure de gestion documentaire.
Elle définit le mode de fonctionnement du système documentaire.
C'est une étape incontournable, car cette procédure servira de cadre pour la rédaction de toutes les autres politiques, procédures et plans du SMSI.
Elle peut être accompagnée d'une procédure complémentaire sur la gestion des enregistrements, qui définit comment seront conservées les preuves, journaux et rapports produits dans le cadre du système.

2. Les documents ou livrables fondamentaux du SMSI à rédiger au cadrage

Une fois la gestion documentaire en place, on commence à formaliser les documents de base du système de management. Ils structurent le SMSI et seront utilisés tout au long du projet.

Document	Rôle dans le SMSI
Contexte et domaine d'application	Décrit les activités couvertes par le SMSI, les frontières du périmètre, les exclusions éventuelles et les interfaces avec d'autres systèmes.
Liste des parties intéressées et de leurs exigences	Identifie les acteurs internes et externes concernés (clients, fournisseurs, autorités, partenaires, collaborateurs) et leurs attentes en matière de sécurité.
Liste des réglementations et exigences contractuelles	Recense les lois, règlements et obligations sectorielles applicables (RGPD, Code du travail, clauses clients, etc.).
Liste des enjeux internes et externes	Décrit les facteurs de contexte (technologiques, économiques, réglementaires, organisationnels) qui influencent la sécurité de l'information.
Objectifs de sécurité de l'information	Définissent les finalités mesurables du SMSI (ex. : disponibilité, intégrité, conformité, résilience).
Politique de sécurité de l'information	Premier document stratégique du système : elle traduit l'engagement de la direction, les orientations de sécurité et les principes de gouvernance.

L'étape de cadrage transforme le diagnostic en plan d'action structuré et maîtrisé.
Elle permet à la fois de définir le cadre du SMSI et d'installer la méthode documentaire qui guidera tout le projet.

C'est à ce stade que l'organisation commence à produire des documents pérennes, qui deviendront les références du système de management.

Étape 3 – Analyse des risques : piloter la documentation à partir des risques

L'analyse des risques constitue le cœur du SMSI et le point d'ancrage de toute la documentation ISO 27001.
C'est à ce stade que l'on identifie ce qu'il faut protéger, contre quoi, et comment.
La procédure d'analyse des risques fait partie des documents fondamentaux du système, car elle décrit la méthode, les critères d'évaluation, les responsabilités et la fréquence de mise à jour.

1. Des enregistrements essentiels au SMSI

Les résultats de l'analyse de risques — registre des actifs, registre des risques, plan de traitement, et déclaration d'applicabilité (DdA) — sont parmi les enregistrements les plus importants du SMSI.
Ils matérialisent les décisions de sécurité, les priorités et les mesures choisies.
C'est à partir d'eux que se construit l'ensemble du corpus documentaire : les politiques, procédures et plans ne sont pas créés de manière théorique, mais en réponse directe aux risques identifiés.

2. Du risque à la mesure documentaire

Chaque risque majeur appelle une ou plusieurs mesures de sécurité, qui peuvent être :

- Techniques (contrôle d'accès, chiffrement, sauvegarde) ;
- Organisationnelles (règles internes, formations, gouvernance) ;
- Documentaires (création d'une politique ou d'une procédure).

Ainsi, lorsqu'un besoin de maîtrise concerne un processus spécifique (gestion des accès, incidents, continuité, etc.), il conduit à la création ou à la mise à jour d'un document : politique, procédure, plan ou enregistrement.
Cette étape permet donc de compléter le diagnostic initial en produisant une documentation ciblée et utile.

3. Garantir la cohérence et préparer la DdA

Un des points clés de cette phase est de vérifier la cohérence entre :

- les enjeux et objectifs de sécurité,
- les risques identifiés,
- et les documents produits pour y répondre.

En fin d'analyse, cette cohérence se formalise dans la déclaration d'applicabilité (SoA), qui liste les contrôles choisis, les mesures associées et les documents en réfrence à l'annexe A (pour vérifier que l'on a oublier aucun document)

La SoA devient alors un pivot documentaire vivant : elle guide la rédaction, les mises à jour et les audits du SMSI tout au long de son cycle de vie.

En résumé, l'analyse des risques n'est pas seulement une étape de conformité : elle oriente la production documentaire, hiérarchise les priorités et garantit que chaque document du SMSI a une raison d'être opérationnelle et démontrable.

Étape 4 – Définition du SMSI : structurer et rédiger les documents du système

La phase de définition du SMSI est celle où l'on passe concrètement à la construction du système de management et à la rédaction du **corpus documentaire.**

C'est le moment où le SMSI prend forme à travers ses **politiques, procédures, plans et enregistrements.**
L'objectif n'est pas de tout écrire d'un coup, mais de structurer le travail thème par thème, en gardant le bon équilibre entre exhaustivité et efficacité.

1. Organiser la rédaction thème par thème

La démarche consiste à aborder la mise en place par grands sujets de sécurité : gestion des accès, sauvegardes, gestion des incidents, continuité, sécurité physique, relations fournisseurs, etc.

Pour chaque thème, on détermine :

- les risques identifiés à traiter (issus de l'analyse précédente),
- les contrôles ISO 27001 concernés (Annexe A),
- et les documents nécessaires pour formaliser les pratiques (politiques, procédures, instructions, plans).

Exemple : pour le thème gestion des accès, on rédigera la politique de contrôle d'accès, la procédure d'attribution des droits et éventuellement une fiche d'enregistrement de création et suppression de comptes.
Cette approche permet de progresser de manière structurée et cohérente, tout en gardant une logique de priorisation par risque.

2. Rédiger utile et équilibré

L'enjeu n'est pas de tout documenter, mais de produire l'essentiel.
Chaque document doit avoir une finalité claire : maîtriser un risque, démontrer une exigence ou formaliser une pratique.
On s'appuie sur l'existant, on complète ce qui manque et on évite la sur-documentation.

3. Co-construire et suivre les actions

La rédaction doit se faire avec les acteurs concernés, pour favoriser l'appropriation et lancer la mise en œuvre en parallèle.
Chaque document validé alimente un **plan d'actions du projet,** véritable outil de pilotage du projet, qui permet le suivi des actions à réaliser. Attention aussi à bien suivre l'ensemble des mesures à contrôler.

4. Maintenir le référentiel et les validations

Les documents suivent le circuit de validation défini (rédacteur, vérificateur, approbateur) et sont intégrés dans le référentiel documentaire.
Ce référentiel devient la base de pilotage de la conformité documentaire, utile pour les audits internes et la revue de direction.
Ce registre assure la traçabilité, la mise à jour et la cohérence du système documentaire.

En résumé

La définition du SMSI consiste à rédiger juste ce qu'il faut, avec les bons acteurs, en construisant un corpus documentaire cohérent, applicable et directement relié aux risques et aux priorités du système.

Étape 5 – Mise en place du SMSI : déployer, prouver et tracer

Après la phase de définition et de rédaction, vient la mise en œuvre concrète du SMSI. Cette étape consiste à appliquer les politiques, procédures et plans, tout en assurant la traçabilité des actions réalisées. L'objectif est double : déployer les mesures de sécurité et produire les preuves de leur application.

1. Mettre en œuvre le plan d'action

Le point de départ est le plan d'action issu des documents du SMSI.
Chaque mesure identifiée doit être traduite en actions concrètes : contrôle d'accès, sauvegarde, formation, mise à jour, revue de droits, etc.
Ce plan doit être suivi, mis à jour et piloté régulièrement, démontrant ainsi la cohérence entre risques, décisions et mesures appliquées.

2. Produire les enregistrements et les preuves

La mise en œuvre ne se limite pas à appliquer les mesures : elle génère des enregistrements qui prouvent leur efficacité.
Parmi eux : **comptes rendus, registres d'incidents, indicateurs de sécurité, preuves de sensibilisation, et tous documents démontrant la mise en place effective des mesures.**
Ces preuves sont essentielles pour attester la conformité et la maîtrise opérationnelle de la sécurité.

3. Suivre les mesures et la traçabilité

Un suivi rigoureux est indispensable : chaque mesure doit être vérifiée, contrôlée et tracée dans le temps.
Des outils comme **Oversecur** intègrent documentation, plan d'action, mesures et vérifications dans un environnement unique, facilitant la cohérence entre politiques, contrôles et preuves.
Ils centralisent indicateurs, résultats de tests, alertes et preuves d'application, garantissant une vision claire et actualisée du niveau de conformité.

4. La logique de traçabilité continue

Le SMSI repose sur un principe fondamental : tout doit pouvoir être démontré.
Cette traçabilité permanente — audits, contrôles, enregistrements, indicateurs — constitue le socle de confiance du système.
Plus la preuve est précise, plus le SMSI résiste aux audits et prouve sa robustesse.

En résumé

La mise en œuvre du SMSI transforme les documents en actions et les actions en preuves.
Cette phase donne vie à la documentation, renforce la conformité et crée la matière factuelle pour démontrer la maîtrise du SMSI lors des audits.

Étape 6 – Audit blanc : vérifier, corriger et fiabiliser la documentation

L'audit blanc marque la dernière grande étape avant la certification.
C'est un exercice de vérification à blanc destiné à tester la conformité du SMSI et à corriger les écarts restants, tant sur le plan opérationnel que documentaire.
Il permet de valider que le système est complet, appliqué et maîtrisé avant le passage de l'audit officiel.

1. Vérifier la conformité du SMSI

L'objectif principal de l'audit blanc est de simuler l'audit de certification :

- s'assurer que toutes les exigences de la norme ISO 27001 sont couvertes ;
- évaluer la pertinence des mesures de sécurité mises en œuvre ;
- et vérifier que la documentation correspond bien à la réalité des pratiques.

Le focus se porte sur la cohérence entre les documents rédigés, les preuves disponibles et les mesures réellement appliquées.
Un SMSI conforme n'est pas seulement bien documenté : il est vivant, traçable et cohérent.

2. Contrôler la complétude documentaire

L'audit blanc est aussi une revue documentaire approfondie.
Il s'agit de s'assurer que :

- tous les documents obligatoires sont présents et à jour (politiques, procédures, plans, SoA, etc.) ;
- les enregistrements (preuves d'application, indicateurs, rapports, comptes rendus) sont disponibles et accessibles ;
- les documents répondent bien à leur objectif et respectent le formalisme défini dans la procédure de gestion documentaire.

C'est également le moment d'identifier les documents manquants ou ceux qui doivent être mis à jour avant la certification.

3. Identifier les écarts et lancer les actions correctives

Chaque écart ou non-conformité détecté lors de l'audit blanc doit donner lieu à une action corrective documentée.
Ces actions sont intégrées au plan d'amélioration du SMSI, qui devient à son tour un enregistrement clé.
L'objectif est de résoudre rapidement les points critiques avant l'audit final, qu'ils concernent la sécurité, les processus ou la documentation.

4. Préparer la présentation à l'auditeur

Enfin, l'audit blanc permet de préparer la restitution du SMSI : savoir présenter la logique du système, la structure documentaire, les liens entre les politiques, les risques et les mesures.
Il sert aussi à s'entraîner à produire les preuves demandées par l'auditeur : rapports, registres, SoA, indicateurs, comptes rendus.
Une bonne préparation facilite grandement le déroulement de l'audit de certification.

En résumé

L'audit blanc est la répétition générale du SMSI : il confirme la solidité du système, la cohérence des documents et la qualité des preuves.
C'est une étape essentielle pour passer du mode projet au mode démonstration, et aborder l'audit de certification avec confiance et maîtrise.

Étape 7 – Préparation à l'audit et revue de direction : finaliser, corriger et démontrer

Après l'audit blanc, la préparation à l'audit de certification consiste à finaliser le SMSI, corriger les écarts et consolider la preuve de conformité.
C'est une étape d'ajustement : on révise les documents, on complète les preuves et on prépare la revue de direction, pièce maîtresse de cette phase.

1. Traiter les non-conformité par les actions correctives

Les actions correctives issues de l'audit blanc doivent être traitées en priorité :

- mise à jour et cohérence des documents (procédures, plans, politiques) ;
- complétude des enregistrements (rapports, indicateurs, registres) pour prouver la mise en œuvre effective des mesures ;
- traçabilité des corrections dans le plan d'action d'amélioration continue.

L'objectif : s'assurer que chaque exigence de la norme ISO 27001 est couverte et que toutes les preuves nécessaires sont disponibles.

2. Consolider les enregistrements et les preuves

Avant la certification, l'organisation doit s'assurer que son système documentaire est complet, cohérent et contrôlé.
Cela implique de :

- vérifier la présence de tous les enregistrements obligatoires (incidents, audits internes, formations, sensibilisations, sauvegardes, indicateurs) ;
- s'assurer que chaque mesure du SMSI est justifiée et vérifiable par des preuves d'application ;
- centraliser ces éléments dans l'outil de gestion documentaire ou dans **Oversecur** pour faciliter la consultation pendant l'audit.

Une attention particulière doit être portée à la déclaration d'applicabilité (SoA), qui doit être à jour, validée et alignée avec les documents et mesures réellement en place.

3. Réaliser une revue de direction complète et structurée

La revue de direction est une exigence majeure de la norme (Clause 9.3).
Elle doit démontrer que la direction suit, évalue et améliore le SMSI.
Son compte rendu doit être exhaustif et précis, couvrant l'ensemble des points demandés.
Ce document est un enregistrement clé du SMSI, que les auditeurs examinent systématiquement.
Il doit refléter la maturité du système et l'engagement de la direction.

4. Se préparer à la présentation du SMSI

La préparation finale inclut aussi la formation et la sensibilisation à l'audit de certification. Préprez une présentation en interne ou pour l'auditeur.
Cette préparation collective facilite le déroulement de la certification et renforce la confiance de l'équipe face à l'auditeur.

En résumé

La phase de préparation à l'audit est une étape de consolidation et de preuve. Elle vise à corriger les écarts, fiabiliser les documents et démontrer la maîtrise du SMSI à travers une revue de direction complète. Bien menée, elle garantit que le système est non seulement conforme, mais aussi cohérent, piloté et prêt à être certifié.

Étape 8 – Audit de certification : démontrer la maîtrise du système

L'audit de certification est l'aboutissement du travail mené depuis le diagnostic initial. Il permet de valider officiellement la conformité du SMSI à la norme ISO 27001. C'est un moment clé : l'auditeur ne vient pas seulement lire des documents, il évalue un système vivant, capable de prouver sa maîtrise, sa cohérence et son efficacité.

1. L'objectif de l'audit de certification

L'audit vise à vérifier que :

- toutes les exigences de la norme sont satisfaites ;
- les politiques, procédures et plans sont effectivement mis en œuvre ;
- les preuves (enregistrements, rapports, indicateurs, comptes rendus) démontrent la conformité et l'efficacité du système.

C'est la démonstration concrète que l'organisation applique bien ce qu'elle a défini et qu'elle maîtrise ses risques de sécurité de l'information.

2. Le rôle central de la documentation

Pendant l'audit, la documentation est le fil conducteur :

- elle permet de présenter la structure du SMSI (politiques, procédures, plans, SoA, etc.) ;
- elle prouve la cohérence entre les risques identifiés, les mesures appliquées et les enregistrements produits ;
- elle sert de référence pour justifier chaque contrôle ou décision.

Une documentation claire, cohérente et à jour est un gage de crédibilité et de maturité.

3. La posture de l'organisation

L'audit de certification se déroule en deux temps :

- un audit étape 1, axé sur la revue documentaire et la préparation du SMSI ;
- un audit de étape 2, centré sur la mise en œuvre effective et les preuves d'application.

L'enjeu est d'adopter une posture de transparence et de maîtrise : savoir expliquer comment le SMSI fonctionne, où se trouvent les preuves, et comment les actions sont suivies.
L'objectif n'est pas de "montrer un dossier parfait", mais un système réel, structuré et piloté.

4. Après la certification

L'audit de certification ne marque pas la fin du projet, mais le début du cycle d'amélioration continue.
Les éventuelles non-conformités mineures ou observations doivent être traitées rapidement et suivies d'une mise à jour documentaire.
Chaque année, un audit de surveillance viendra vérifier que le système reste vivant et conforme.
La certification devient ainsi un outil de management permanent, pas une simple reconnaissance ponctuelle.

En résumé

L'audit de certification est la preuve ultime de la maturité du SMSI. C'est la validation que la documentation, les mesures et les preuves convergent dans un système cohérent, maîtrisé et améliorable.
Un SMSI certifié, c'est avant tout une organisation capable de démontrer, à tout moment, qu'elle protège et gouverne efficacement son information.

Bien organiser sa documentation

Une documentation bien structurée est le pilier du SMSI. Elle traduit les exigences de la norme en pratiques concrètes, assure la cohérence du système et permet de démontrer la maîtrise et la conformité.

1. Rédiger juste et utile

Chaque document doit avoir une raison d'être : répondre à un risque, formaliser une règle, prouver une action. Il ne s'agit pas de tout écrire, mais de produire l'essentiel, avec un niveau de détail adapté à la taille et à la complexité de l'organisation.

Une documentation claire, concise et pertinente sera mieux comprise, mieux appliquée et plus facile à maintenir.

2. Structurer selon la logique du système

La documentation doit suivre la hiérarchie du SMSI :

- Politiques : fixent les principes et les exigences.
- Procédures : décrivent comment ces principes s'appliquent.
- Plans : détaillent les actions à mener dans des activités spécifiques
- Enregistrements : apportent la preuve que le système fonctionne.

Cette structure garantit la cohérence et facilite la lecture du système par les auditeurs et les équipes.

3. Impliquer et centraliser

Rédiger la documentation avec les acteurs concernés (métiers, technique, conformité, RH…) favorise son appropriation. Une fois validée, elle doit être centralisée dans un référentiel unique (par exemple Oversecur ou SharePoint) pour en maîtriser le versionnage, l'accès et la mise à jour.

4. Relier aux risques et aux preuves

Chaque document doit être rattaché à un risque identifié et produire des enregistrements de conformité : indicateurs, rapports, comptes rendus, journaux d'incidents.

Cette traçabilité "risque – mesure – preuve" est au cœur de la logique ISO 27001.

5. Faire vivre la documentation

Un système documentaire n'est jamais figé. Il doit être révisé régulièrement, notamment après un incident, un audit ou un changement organisationnel.

Faire vivre la documentation, c'est faire vivre le SMSI : elle devient un outil de pilotage au service de la sécurité et de l'amélioration continue.

En résumé

Rédiger peu mais bien, impliquer les acteurs, centraliser les documents, les relier aux risques et maintenir leur mise à jour.

Une documentation claire, maîtrisée et alignée sur les pratiques rend le SMSI à la fois efficace, crédible et durable.

EXIGENCES

La documentation ISO 27001 en pratique

04

LA LISTE DES DOCUMENTS À RÉDIGER DANS LE CADRE DE LA CERTIFICATION ISO 27001

La norme ISO 27001 demande un ensemble de documents permettant de démontrer la cohérence, la maîtrise et la conformité du système de management de la sécurité de l'information (SMSI). Ces documents ne sont pas tous obligatoires au sens strict, mais sont nécessaires pour piloter le système, prouver la mise en œuvre des contrôles et structurer la sécurité. Pour clarifier, on peut regrouper la documentation en **quatre grandes typologies**, chacune jouant un rôle spécifique.

1. Les politiques (Documents d'orientation stratégique du SMSI)

Les politiques fixent les principes et engagements de l'organisation. Elles traduisent la vision de la direction en orientations concrètes de sécurité et servent de référence à toutes les procédures.
Exemples : politique de sécurité de l'information, politique de contrôle d'accès, politique de classification, politique de sauvegarde, politique RGPD, politique d'utilisation de l'IA.

2. Les procédures et plans (Documentation opérationnelle du système)

Les procédures et plans expliquent comment appliquer les politiques au quotidien. Elles précisent les étapes, les rôles et les responsabilités pour la mise en œuvre des mesures.
Exemples : procédure de gestion des incidents, plan de continuité d'activité, procédure de gestion des vulnérabilités, plan de sauvegarde, plan de gestion des accès.

3. Les documents clés du système de management

Ce sont les documents de **gouvernance** assurant la cohérence du SMSI. Liés à la gestion du système lui-même, pas à une mesure technique.
Exemples : contexte et domaine d'application, liste des parties intéressées, registre des risques, plan de traitement, déclaration d'applicabilité (SoA), revue de direction.

4. Les documents d'accompagnement et de gestion du projet

Ce sont les documents de **support** encadrant la mise en place du SMSI, la communication et le changement.
Exemples : plan de communication, plan de formation et sensibilisation, fiches de suivi du projet, comptes rendus de comités, fiches d'actions.

5. Les enregistrements

Chaque famille de documents génère ses enregistrements : les preuves que le SMSI fonctionne effectivement.
Exemples : Rapports, indicateurs, logs, comptes rendus, journaux d'incidents, fiches de formation — les enregistrements sont le reflet vivant du système.

Dans les pages suivantes, nous vous présentons une ou plusieurs listes les plus exhaustives possibles pour les documents à produire dans chaque catégorie.

LISTE DES POLITIQUES THÉMATIQUES

Cette liste doit être adaptée aux besoins de l'organisation. Certains documents pourront être regroupés d'autres pourront être ajoutés en fonction des risques.

Document / Politique	Références	Exigence couverte / Objectif
Politique de sécurité de l'information	Clause 5.2 + Annexe A 5.1	Établir et approuver la politique de sécurité de l'information, la communiquer et la rendre cohérente avec les orientations stratégiques.
Politique de télétravail	Annexe A 6.7	Définir les règles de sécurité applicables au télétravail et à l'accès distant.
Charte informatique / Charte utilisateur	Annexe A 6.2 + A 6.3	Définir les responsabilités des utilisateurs en matière d'usage du SI, d'accès, d'éthique et de confidentialité.
Politique de classification de l'information	Annexe A 5.12	Classer les informations selon leur valeur, sensibilité et exigences légales ; définir les règles d'étiquetage et de manipulation.
Politique de contrôle d'accès	Annexe A 5.15 + A 5.16 + A 5.17	Définir les règles d'attribution, de gestion et de révocation des droits d'accès ; principes de moindre privilège et d'authentification.
Politique de chiffrement	Annexe A 8.24	Déterminer les principes et méthodes de chiffrement, de gestion des clés et des algorithmes utilisés.
Politique de sécurité physique	Annexe A 7.1 à A 7.9	Protéger les locaux, les équipements et les installations contre les accès physiques non autorisés et les dommages.
Politique de gestion des changements	Annexe A 8.32	Encadrer la planification, l'évaluation et la validation des changements techniques ou organisationnels.
Politique de sauvegardes	Annexe A 8.13	Définir les modalités de sauvegarde, de restauration et de vérification des données critiques.
Politiques et procédures de transfert de l'information	Annexe A 8.12	Encadrer les échanges d'informations internes et externes, définir les canaux et mesures de protection.
Politique de développement sécurisé	Annexe A 8.25 + A 8.28	Définir les exigences de sécurité dans le développement logiciel et les cycles de vie applicatifs.
Politique de traitement des données personnelles RGPD	RGPD art. 24, 28, 30	Définir les règles de conformité au RGPD : gouvernance des données personnelles, droits des personnes, registres et clauses de sous-traitance.
Politique d'utilisation de l'IA	IA ACT	Encadrer l'usage des systèmes d'intelligence artificielle : principes éthiques, transparence, traçabilité, gestion des biais et des risques IA.
Politique de sécurité de l'information avec les fournisseurs	Annexe A 5.19 à A 5.23	Établir les exigences de sécurité, les clauses contractuelles et le suivi des prestataires et fournisseurs.

LES PROCÉDURES ET PLANS

Il est important de rappeler que la liste des procédures et des plans présentée dans ce guide n'est pas exhaustive. Elle regroupe les documents les plus couramment rencontrés dans les projets ISO 27001, mais chaque organisation doit adapter cette documentation à son propre contexte, à ses risques et à ses pratiques.
L'objectif est de disposer d'un ensemble de documents qui répondent réellement aux besoins de l'entreprise et aux exigences identifiées.
Il vous appartient donc de compléter ou d'ajuster ce plan documentaire en fonction de votre environnement, tout en veillant à ce qu'il soit cohérent et complet au regard des contrôles de l'annexe A et des exigences de la norme.

Document / Politique	Référence ISO / Clause concernée	Exigence couverte / Objectif
Règlement intérieur	Clause 7.3 + Annexe A 6.2	Encadrer les comportements et rappeler les obligations de conformité et de sécurité applicables aux employés.
Procédure de gestion des supports amovibles	Annexe A 8.10	Encadrer l'utilisation, le stockage et la destruction sécurisée des supports amovibles.
Procédure de mise au rebut des supports	Annexe A 8.11	Définir les modalités de suppression ou de réutilisation sécurisée des supports contenant des données sensibles.
Procédure de gestion des vulnérabilités	Annexe A 8.8	Identifier, évaluer, traiter et suivre les vulnérabilités techniques.
Bonnes pratiques de développement	Annexe A 8.28	Définir les règles de codage sécurisé, de revue de code et de test de sécurité applicables aux développeurs.
Politique de sécurité de l'information avec les fournisseurs	Annexe A 5.19 à A 5.23	Fixer les exigences de sécurité dans les relations fournisseurs, sous-traitants et partenaires externes.
Procédure de gestion des incidents	Annexe A 5.24 à A 5.30	Décrire la détection, la notification, le traitement et la communication des incidents de sécurité.
Plan de continuité et reprise d'activité (PCA/PRA)	Annexe A 5.29 à A 5.31 + Clause 6.1.3	Garantir la résilience, la disponibilité et la reprise rapide des activités critiques en cas d'incident majeur.

LES ENREGISTREMENTS DU SMSI

Les enregistrements obligatoires du SMSI sont les preuves indispensables exigées par l'ISO 27001. Ils démontrent que le système est piloté, contrôlé et amélioré. Sans ces traces factuelles — risques, audits, actions, revue de direction — il est impossible de prouver la conformité et le fonctionnement réel du SMSI.

Enregistrement	Explications
Revue de direction	Documente l'évaluation annuelle du SMSI par la direction : performance, incidents, risques, ressources, améliorations. C'est *la preuve* que la direction pilote réellement la sécurité.
Liste des risques	Liste l'ensemble des risques identifiés, leur analyse (impact/vraisemblance) et leur statut. C'est le cœur du SMSI : toute la sécurité repose sur ces documents.
Registre des actifs	Permet de savoir précisément ce qui doit être protégé (équipements, données, applications). Sans inventaire, impossible de faire une analyse de risques cohérente.
Plan de traitement des risques (PTR)	Trace les décisions de traitement : atténuer, accepter, éviter, transférer. Relie chaque risque à une mesure concrète.
Déclaration d'applicabilité (DdA)	Liste l'ensemble des contrôles ISO 27001, indique ceux retenus ou exclus, et la justification. C'est l'un des documents les plus importants de l'audit.
Objectifs de sécurité	Définissent les cibles mesurables du SMSI (ex. taux d'incidents, disponibilité…). Ils démontrent que l'entreprise pilote sa sécurité de façon mesurable.
Indicateurs de sécurité (KPI)	Mesurent l'atteinte des objectifs : taux de patchs appliqués, délais de résolution incidents, couverture sauvegardes. Essentiel en audit.
Rapports d'audit interne	Preuve que le SMSI est vérifié régulièrement. Ces rapports montrent la maturité, les points forts et les écarts internes identifiés.
Programme d'audit interne	Planifie les audits : dates, périmètres, auditeurs. Permet à l'auditeur externe de vérifier la rigueur du contrôle interne. A Faire sur les 3 ans
Suivi des non-conformités	Liste toutes les non-conformités détectées. Prouve que l'entreprise identifie ses écarts.
Registre des actions correctives	Documente les actions mises en place pour corriger les non-conformités. Prouve l'amélioration du SMSI.
Registre des formations / sensibilisations	Trace qui a été formé, quand, sur quel sujet. Prouve que les collaborateurs sont compétents et sensibilisés.
Registre des exigences légales et contractuelles	Recense toutes les obligations qui s'appliquent à l'entreprise (RGPD, contrats clients, NIS2…). Prouve la conformité légale.
Registre documentaire	Liste l'ensemble des documents du SMSI : versions, propriétaires, dates d'approbation. Indispensable pour maîtriser la documentation.
Comptes rendus de gouvernance / COPIL	Traçabilité des décisions de pilotage : arbitrages, budgets, évolutions, suivi. Prouve que la direction supervise réellement la sécurité.
Preuves de communication sécurité	Messages internes, annonces, notes de service. Sert à démontrer que l'information circule et que la sécurité est communiquée. plan de communication.

LES ENREGISTREMENTS OPÉRATIONNELS

Les enregistrements opérationnels rassemblent les preuves issues de l'activité quotidienne : incidents, sauvegardes, accès, vulnérabilités, tests, supervision. Ils démontrent l'application concrète des mesures de sécurité prévues par le SMSI. Ces traces terrain montrent que les contrôles fonctionnent réellement et permettent à l'auditeur de vérifier l'efficacité opérationnelle du système.

Enregistrement opérationnel	Ce que prouve cet enregistrement dans le SMSI	Lien ISO (Annexe A)
Journal des incidents / tickets	Prouve que les incidents sont détectés, analysés, traités et documentés. Permet de démontrer la réactivité et l'efficacité du processus.	A 5.24 – A 5.30
Registre des vulnérabilités	Trace les vulnérabilités détectées (scans, CVE), leur criticité, leur correction. Essentiel pour prouver la gestion proactive du risque technique.	A 8.8
Rapports de sauvegardes	Prouve que les sauvegardes sont effectuées conformément à la politique. Un audit est souvent bloqué si ce rapport manque.	A 8.13
Rapports de tests de restauration	Prouve que les sauvegardes sont réellement fonctionnelles. Beaucoup d'entreprises échouent ici.	A 5.29 / A 8.13
Suivi de gestion des accès	Prouve que les droits sont attribués et retirés de manière contrôlée. Permet de valider la maîtrise du cycle de vie des accès. Et les preuves des revues.	A 5.15 à A 5.17
Journaux d'accès logiques (VPN, AD, firewall)	Prouvent la surveillance des accès sensibles et détectent les anomalies. L'auditeur les consulte souvent.	A 8.15 / A 8.16
Journaux d'accès physiques	Prouvent que les locaux sont contrôlés et que les zones sensibles sont protégées.	A 7.1 à A 7.9
Rapports de supervision / monitoring	Logs de surveillance (CPU, RAM, disponibilité, anomalies). Prouve la supervision continue des systèmes.	A 8.16
Rapports de patch management	Prouvent que les systèmes sont mis à jour dans les délais (correctifs critiques, CVE).	A 8.7
Rapports antivirus / EDR	Prouvent la détection et la neutralisation des menaces.	A 8.9
Rapports de tests d'intrusion ou audits	Preuves externes de robustesse. Très appréciés (voire exigés) dans certains secteurs.	A 8.23
Registre de gestion des changements	Trace les changements majeurs (techniques ou organisationnels) et leur validation.	A 8.32
Preuves de sensibilisation/formations	Prouvent que les collaborateurs ont participé et compris les consignes.(présence, quiz)	A 6.3
Registre de transfert d'information	Prouve la maîtrise des échanges (internes, externes, clients).	A 8.12
Registre de maintenance / interventions techniques	Prouve que les interventions sur les systèmes sont contrôlées et documentées.	A 7.4 / A 8.19
Rapports de tests PCA / PRA	Prouvent la capacité à fonctionner en cas d'incident majeur. Document stratégique en audit.	A 5.30
Rapports fournisseurs (SOC 2, ISO 27001,	Prouve que les prestataires critiques sont évalués et maîtrisés.	A 5.19 à A 5.23

LES DOCUMENTS CLÉS DU SYSTÈME DE MANAGEMENT (1/2)

Documents du système de management ISO 27001 (chapitres 4 à 10)

La norme ISO 27001 repose sur une approche structurée du management de la sécurité.
Pour démontrer la conformité du système et assurer sa cohérence, chaque exigence des chapitres 4 à 10 doit être appuyée par des documents adaptés : politiques, procédures, plans ou enregistrements.

Ces documents ne sont pas seulement des livrables de certification, mais des outils de pilotage et de preuve, indispensables au bon fonctionnement du SMSI. La liste suivante présente les documents essentiels à prévoir, classés selon les chapitres de la norme ISO 27001 v 2022.
Chaque organisation doit naturellement adapter et compléter cette base selon son périmètre, ses risques et ses contraintes réglementaires.

Chapitre 4 – Contexte de l'organisation

Définir le cadre, le périmètre et les exigences applicables au SMSI.

- Contexte de l'organisation (enjeux internes et externes)
- Domaine d'application du SMSI (périmètre et exclusions)
- Liste des parties intéressées et de leurs exigences
- Registre des exigences légales, réglementaires et contractuelles
- Politique ou procédure de gestion documentaire (cycle de vie, validation, archivage)

Chapitre 5 – Leadership

Formaliser les engagements de la direction et la gouvernance du SMSI.

- Politique de sécurité de l'information
- Lettre d'engagement de la direction (peut être intégré à la politique)
- Organigramme (gouvernance de la sécurité)
- Matrice des responsabilités (RACI)
- Compte rendu de la réunion de lancement du SMSI

Chapitre 6 – Planification

Planifier les risques, les opportunités et les objectifs du SMSI.

- Méthodologie d'analyse et de traitement des risques
- Registre des risques et des opportunités
- Registre des actifs informationnels
- Plan de traitement des risques
- Déclaration d'applicabilité (DdA)
- Liste des objectifs de sécurité et plan d'action associé
- Plan de communication et de sensibilisation sécurité

Chapitre 7 – Support

Assurer les ressources, la compétence et la communication nécessaires au SMSI.

- Plan de gestion des ressources et des compétences
- Plan de formation et de sensibilisation sécurité
- Registre de suivi des formations réalisées
- Procédure de communication interne et externe
- Modèles de documents
- Listing des documents externes ou moyens d'identification

LES DOCUMENTS CLÉS DU SYSTÈME DE MANAGEMENT (1/2)

Chapitre 8 – Fonctionnement (Opérationnel)

Décrire la mise en œuvre concrète des mesures et des contrôles de sécurité et maintenir à jour les documents du système. S'appuyer sur l'annexe A.

Chapitre 9 – Évaluation des performances

Mesurer, suivre et améliorer la performance du SMSI.

- Programme et procédure d'audit interne
- Rapports d'audit interne
- Indicateurs de performance (KPI sécurité)
- Tableau de bord de suivi du SMSI
- Compte-rendu de revue de direction
- Plan d'action d'amélioration continue

Chapitre 10 – Amélioration

Traiter les non-conformités et maintenir la dynamique d'amélioration continue.

- Procédure de traitement des non-conformités et actions correctives
- Registre des non-conformités
- Plan de suivi des actions correctives et préventives
- Rapports de traitement d'incidents majeurs

En résumé

Ces documents constituent l'ossature du **Système de Management de la Sécurité de l'Information (SMSI).**
Ils garantissent la cohérence entre les exigences de la norme, les risques identifiés et les mesures appliquées.
L'enjeu n'est pas d'avoir le plus grand nombre de documents, mais de disposer des bons documents, à jour, validés et alignés sur les pratiques réelles de l'organisation.

LES DOCUMENTS D'ACCOMPAGNEMENT ET DE GESTION DU PROJET

Au-delà des politiques et procédures, la réussite d'un SMSI repose sur une documentation de pilotage.
Ces documents d'accompagnement permettent de planifier, suivre et ajuster la mise en œuvre du système. Ils relient la dimension organisationnelle du projet à la logique de management de la sécurité.

1. La planification du projet SMSI

La première étape consiste à formaliser **une feuille de route** décrivant :

- les grandes étapes du projet (diagnostic, cadrage, analyse des risques, définition, mise en œuvre, audit, certification) ;
- les jalons clés et livrables attendus à chaque phase ;
- les responsables, ressources et échéances ;
- les dépendances entre activités.

Ce document donne une vision claire de la trajectoire et sert de référence tout au long du projet.

2. Le plan d'action : un outil pivot

Le plan d'action est le document central du projet ISO 27001.
Il consolide l'ensemble des actions pour atteindre la conformité :

- actions issues de l'analyse des risques (mesures de sécurité) ;
- actions issues des audits internes ou blancs (corrections, ajustements) ;
- actions correctives liées à des incidents ou non-conformités ;
- actions d'amélioration continue de la revue de direction.

Chaque action doit comporter : description, responsable, priorité, échéance et statut.
Ce plan devient un document vivant, mis à jour régulièrement et partagé. C'est le principal outil de pilotage et le lien entre documentation, risques et réalité opérationnelle.

3. Les autres documents d'accompagnement utiles

En complément du plan d'action, d'autres documents peuvent renforcer la cohérence et la visibilité du projet :

- Le plan de communication : pour informer et sensibiliser les collaborateurs aux enjeux du SMSI.
- Le plan de formation et de sensibilisation : pour planifier les formations sécurité et le suivi des compétences.
- Le registre de suivi des comités de pilotage : comptes rendus, décisions et points bloquants.
- La matrice de correspondance documentaire : pour relier les documents produits aux exigences ISO (utile pour l'audit).
- La feuille de route d'amélioration continue : pour structurer les actions post-certification.

Ces documents ne sont pas obligatoires, mais ils apportent une vision de gouvernance claire et partagée.

En résumé

Les documents d'accompagnement ne sont pas seulement des supports administratifs : ils assurent la cohérence, la traçabilité et la continuité du projet ISO 27001.
Le plan d'action unique en est le cœur, car il relie les risques, les mesures, les corrections et les améliorations dans une seule dynamique.
Autour de lui, les plans de communication, de formation et de suivi assurent la maturité et la pérennité du SMSI au fil du temps.

CONCLUSION

Nos services

05

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

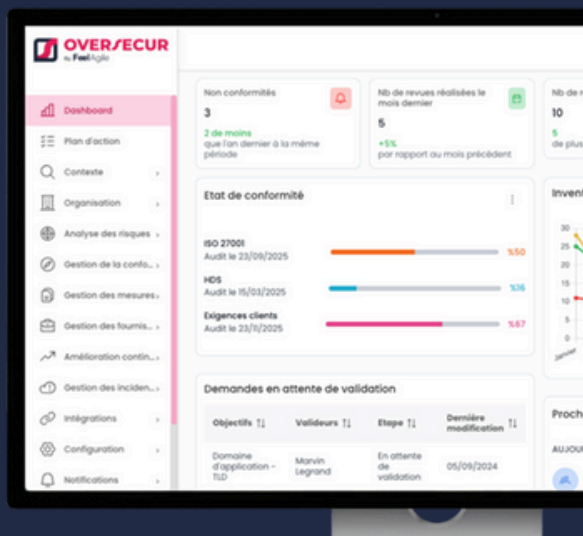
ISO 27001
ISO 27701
ISO 42001
ISO 22301

ISO 27005
ISO 31000
ISO 9001

PECB
AUTHORIZED
PARTNER

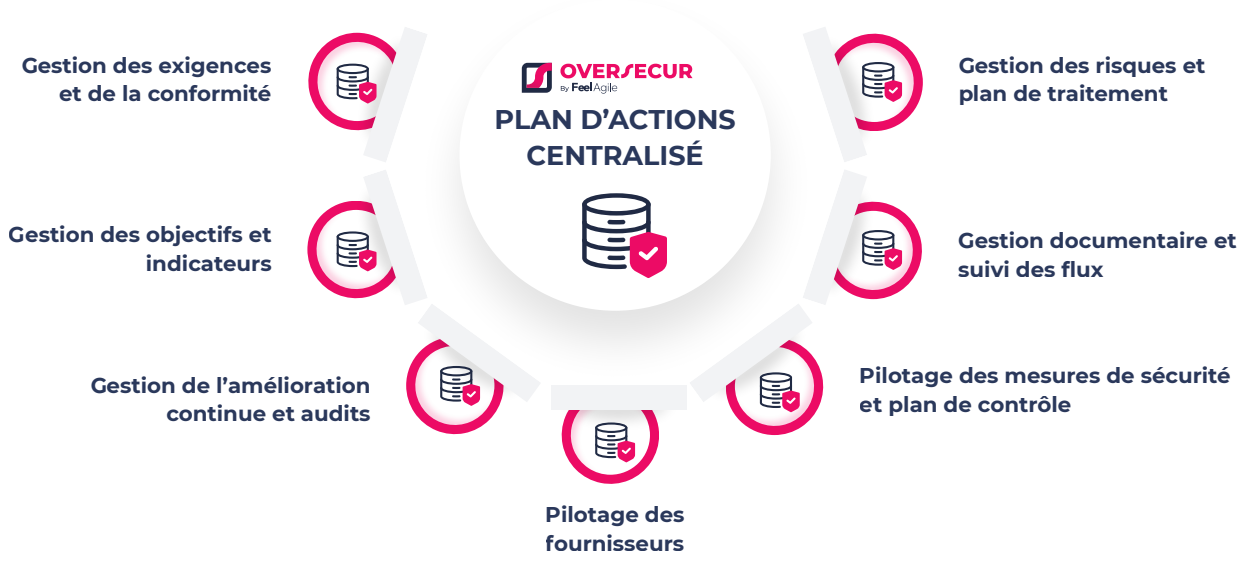
OVERSECUR
By FeelAgile

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.