

# LES FOCUS SOLUCOM

## ISO 27001 : Les clés d'une mise en œuvre efficace

The power of simplicity  
*« Ce qui est simple est fort »*

**solucom**   
management & IT consulting

# ISO 27001 : Les clés d'une mise en œuvre efficace

**Aujourd'hui la norme ISO 27001 est indéniablement devenue le modèle de gouvernance de la sécurité de l'information. Amenant un pilotage de la sécurité par les risques couplé à une approche système de management, elle permet de structurer et rationaliser le pilotage de la sécurité tout en construisant une vision stratégique à moyen terme.**

**Mais comment se lancer dans sa mise en œuvre en répondant au mieux aux enjeux de sécurité des métiers et en en tirant le meilleur parti ?**

## 1. TROUVER LE SMSI GAGNANT

**Avant de démarrer : se poser les bonnes questions !**

Une étude d'opportunité et de faisabilité permet de répondre rapidement aux questions clés : pourquoi et pour qui implémenter la norme ? Quels sont les enjeux métiers et les grands risques sécurité ? D'où part-on ?

Si la lecture linéaire des exigences de la norme s'avère vite peu adaptée pour évaluer le niveau de conformité actuel de l'entreprise, une analyse des écarts en adoptant une vision « processus » (pilotage du système de management de la sécurité de l'information, gestion des risques, contrôle et mesure de l'efficacité, etc.) est plus facile à mener et souvent bien plus parlante. Conduite avec les métiers, les interlocuteurs sécurité, SI et les fonctions support, elle est également l'occasion de les sensibiliser, de comprendre leurs enjeux business et d'identifier de manière macroscopique leurs risques sécurité.

**Alignement ou certification : trouver sa voie**

Ces deux voies correspondent à des enjeux différents. L'alignement à la norme permet d'apporter cohérence et implication à la démarche de sécurité. Il donne également la possibilité de la légitimer et communiquer sur celle-ci... Il s'agit dès lors de se fixer son

propre référentiel d'exigences en sélectionnant les processus présentant le meilleur ratio efficacité / coût dans le contexte, et le degré de conformité visé. L'alignement s'inscrit dans une démarche de progrès sur plusieurs années, en fonction de la maturité initiale et de la cible : c'est la voie choisie par la majorité de nos clients.

les charges internes et les futurs besoins de contractualisation.

La stratégie de définition du système de management et de l'organisation est intimement dépendante de ce périmètre et de l'organisation de l'entreprise. Un SMSI, des SMSI ? Quel cycle de vie ? Quel(s) responsable(s), entité(s) de management, instances ?

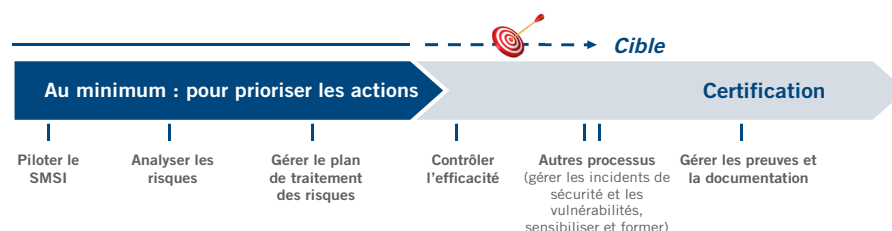


Figure 1 : Une cible d'alignement à déterminer selon le ratio gain / efforts et les objectifs

La certification répond quant à elle à des enjeux commerciaux, sectoriels, réglementaires ou opérationnels forts. Au-delà des apports de l'alignement, elle constitue un élément différenciant, la garantie externe d'un pilotage de la sécurité maîtrisé aux yeux des clients, partenaires et régulateurs.

Bien souvent, les organismes qui s'engagent dans la certification manipulent des données sensibles soumises à des réglementations fortes (santé, banque, assurance) ou sont des hébergeurs ou fournisseurs qui voient dans la certification un intérêt d'image, mais aussi opérationnellement une réduction du nombre d'audits de leurs clients !

**Identifier les scénarii gagnants à présenter à sa direction**

Le périmètre est un élément structurant du système, qui doit être centré sur les enjeux métiers. Il peut prendre la forme d'un site (un datacenter), d'une organisation (la DSI), d'un processus ou encore d'une offre proposée aux clients.

Au-delà de ce qu'il comprend, il est important d'identifier précisément ses frontières avec les différentes interfaces (fournisseurs internes, externes, clients, etc.) pour évaluer

Les différents scénarii imaginés doivent être confrontés aux enjeux métiers et aux investissements. N'oublions pas que ces derniers sont en partie déjà prévus : les risques sont dans tous les cas traités, et la charge du pilotage du SMSI est déjà intégrée aux missions récurrentes du RSSI. Des arguments qui peuvent faire mouche auprès de la direction à qui le projet sera présenté !

## 2. CONSTRUIRE EFFICACEMENT SON SMSI

Une fois les orientations validées, il s'agit de se lancer dans l'implémentation à proprement parler : quels sont les facteurs clés de succès pour assurer une mise en œuvre efficace ?

**Optimiser le planning de mise en œuvre**

Tout en respectant les très nombreuses dépendances entre les processus du SMSI, il est tout à fait possible d'optimiser leur implémentation pour paralléliser les tâches et ainsi raccourcir le planning de mise en œuvre.

La mise en place d'un SMSI peut ainsi s'organiser en deux grands chantiers principaux :

- D'une part, **la mise en place du système de management en lui-même**. Il faut définir les processus (pilotage, sensibilisation, contrôle et mesure de l'efficacité, etc.), et les implémenter. Le processus de pilotage sera bien entendu le premier à être étudié.
- D'autre part, **la mise en place de la gestion des risques, pilier de la démarche**. Elle débute par la définition du processus de gestion des risques et la réalisation de l'appréciation des risques. Souvent, une première analyse rapide et macroscopique a déjà été menée lors de l'étude d'opportunité, afin d'identifier les chantiers de sécurité à démarrer au plus vite (PCA, IAM, chiffrage, etc.). Lors de cette deuxième étape, il s'agit de réaliser l'analyse détaillée des risques de sécurité répondant aux exigences de l'ISO 27001. Elle permettra d'affiner et compléter les chantiers de sécurité qui auront été lancés en parallèle.

### Faire adhérer les opérationnels à la démarche

Si le responsable SMSI – bien souvent le RSSI, même s'il peut également être un acteur métier – et son équipe sont les pilotes du projet, il ne faut pas négliger la contribution des opérationnels avec lesquels il est nécessaire de mettre en place une coordination forte.

L'enjeu va bien au-delà de la réalisation des projets sécurité selon le planning et les modalités prévues. En effet, passée la phase projet, ce sont eux qui maintiendront les mesures de sécurité implémentées et la documentation : leur appropriation garantira la pérennité du niveau de sécurité ciblé.

### Construire pour le futur

L'amélioration continue occupe une place clé dans les principes de l'ISO 27001. Dès lors, il est tout à fait acceptable de commencer par mettre en place une cible pragmatique dans la situation actuelle de l'organisme, tout en se projetant dans une stratégie d'évolution du SMSI plus ambitieuse à moyen terme.

Bien que le premier cycle Plan-Do-Check-Act soit principalement celui de la mise en place et de la découverte, il est également celui où les fondations du SMSI sont posées. Il est donc important d'avoir dès ces premières phases les potentielles évolutions du SMSI en tête (une extension du périmètre par exemple). C'est particulièrement vrai pour la définition et la mise en place des processus, qui doivent pouvoir survivre aux changements de périmètre et d'organisation sans devoir subir une refonte complète.

La mise en place du SMSI doit ainsi être considérée comme un projet à part entière, mais ce n'est qu'un début : c'est également un tremplin pour assurer la pérennité de la démarche et l'adhésion des acteurs dans le temps ! Une fois le SMSI implémenté, se profile déjà un nouveau défi pour le RSSI : comment entretenir la démarche pour continuer à en tirer au maximum parti ?

## 3. MAINTENIR UNE DYNAMIQUE DE CONSTRUCTION

Si le premier cycle Plan-Do-Check-Act est souvent dynamique et mobilisateur,

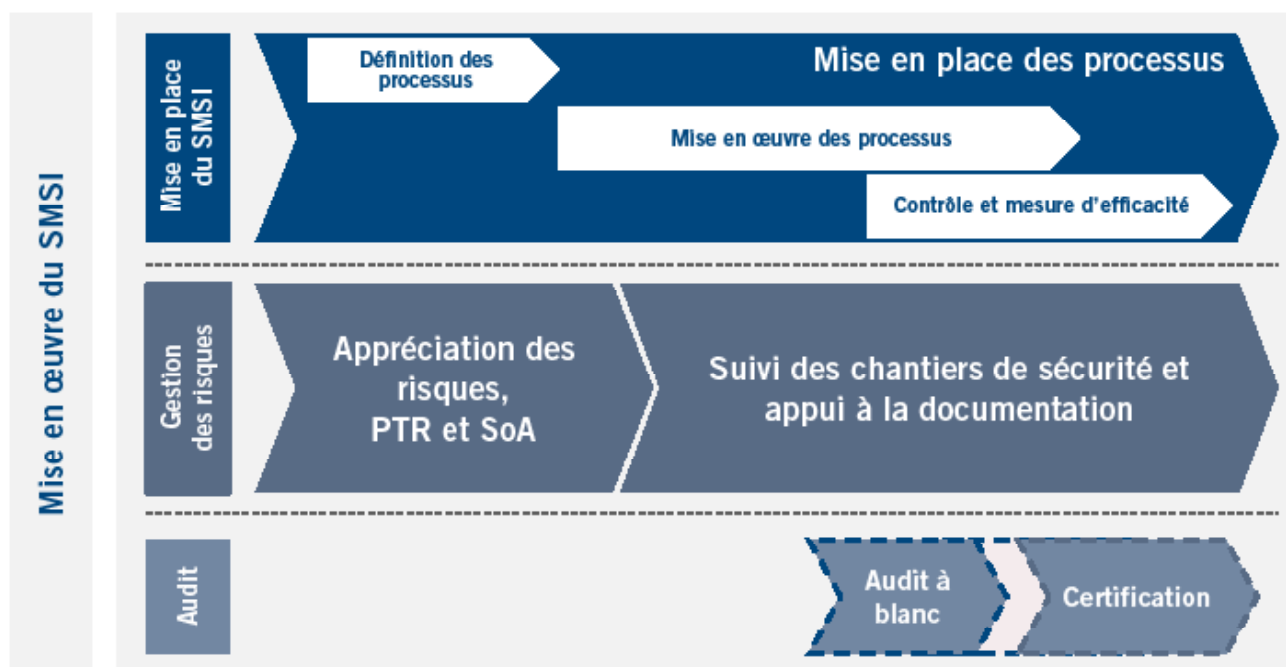
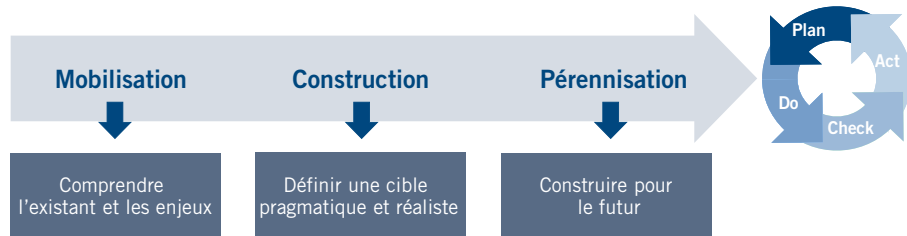


Figure 2 : Optimiser le planning de mise en œuvre

Figure 3 : Construire dans une logique d'amélioration continue



la deuxième année peut se révéler pavée d'écueils si elle n'est pas soigneusement préparée. La dérive la plus fréquemment rencontrée est bien sûr la démobilisation des collaborateurs : passée la phase projet et l'aboutissement de l'implémentation des processus ou de la certification, il ne faut pas « laisser le soufflé retomber », même si des projets d'autres entités occupent désormais le devant de la scène auprès du management.

### Conserver la dynamique projet

Il est important de maintenir une dynamique ambitieuse pour traiter les risques par les projets de sécurité. Ces chantiers permettront de garder un focus sur la sécurité et feront vivre le SMSI indirectement. En effet, ils sont propices à la mise en place de rendez-vous réguliers (comités de pilotage, points projets...) avec les collaborateurs et la direction sur le sujet sécurité. Le SMSI est alors utilisé au quotidien et l'avancement des projets permet de montrer des réductions des risques concrètes, et mesurées dans le temps.

### Optimiser et garantir l'adhésion au SMSI dans le temps

La construction initiale est bien souvent réalisée sur des bases nouvelles, en imaginant le fonctionnement des processus de manière optimale. Fort de l'expérience des premiers cycles, le responsable du SMSI doit être à l'écoute des collaborateurs sur le fonctionnement de ces processus, de manière directe (rencontres, questionnaires...) ou indirecte, pour déterminer où se trouvent les points d'amélioration les plus criants et apporter des modifications rapides. Cela permet d'éviter un effet de lassitude, voire même de rejet, pour des processus qui fonctionneraient moyennement.

Ces évolutions sont généralement de deux types. Il s'agit tout d'abord de l'industrialisation des tâches récurrentes par l'outillage :

même s'il n'existe pas aujourd'hui de solution « tout en un » idéale, des optimisations sur des tâches particulières sont possibles (qu'elles soient techniques, de pilotage comme les indicateurs ou administratives ou la documentation). Puis vient la rationalisation des actions existantes, particulièrement en renforçant l'intégration du SMSI dans les processus de l'entreprise. Par exemple, l'intégration de revues de direction de plusieurs systèmes de management ou encore l'unification des démarches d'audit et de contrôle interne sont de beaux défis qui nécessitent une maturité importante mais qui sont autant de vecteurs d'optimisation.

Même si ces chantiers sont peu visibles, ils vont être la clé pour démontrer l'adaptabilité, la réactivité et la légèreté du SMSI.

### Faire de l'audit de surveillance un marqueur clé

Le suivi des incidents, des crises mais aussi des non-conformités et des actions correctives et préventives sont essentielles pour montrer l'apport du SMSI. Cette analyse ne doit pas être un travail isolé mené par le responsable du SMSI mais bien une démarche collaborative avec les équipes opérationnelles. Cette revue régulière et partagée permet de montrer l'apport du SMSI dans la couverture des événements liés à la sécurité.

Bien sûr, cette dynamique ne saurait être complète sans une communication régulière auprès de l'ensemble des populations : qu'il s'agisse de sensibilisation ou de communication sur les gains de la démarche et les succès (impact auprès des clients, gains opérationnels, etc.), les piqures de rappel sont nécessaires pour ancrer dans les pratiques et les esprits la démarche sécurité et les enjeux de l'organisme.

L'audit de surveillance, voire de renouvellement, est un marqueur clé de cette stratégie de communication. Il doit être vécu comme un aboutissement chaque année. Et ceci pas uniquement car la certification est maintenue, mais bien parce que le niveau de protection est meilleur d'année en année !

### Se remettre en question pour aller plus loin

Finalement, le responsable du SMSI doit avoir un esprit d'écoute et de conquête pour d'une part comprendre les événements qui marquent son périmètre métier (nouvelles offres, fusions, rapprochement, évolution du marché...) et d'autre part identifier les actions clés pour une potentielle évolution du SMSI. Des pistes judicieuses pour faire souffler un vent de fraîcheur sur le SMSI et donner une nouvelle impulsion à la démarche.

### CONCLUSION

L'ISO 27001 a montré ces dernières années sa force en permettant aux filières sécurité de progresser à la fois sur leur management et leur niveau de sécurité. Bien au-delà de la certification, qui reste peu répandue en France, elle est devenue un outil de référence pour tous les RSSI. Les retours d'expérience le montrent, l'âge de la maturité n'est pas loin d'être atteint ! C'est d'ailleurs dans ce sens, 6 ans après sa première publication, que des évolutions sont discutées dans les groupes de normalisation et permettront certainement d'améliorer encore son apport pour ses utilisateurs.



Ce focus a été rédigé par Marion Couturier et Gérôme Billois, respectivement consultante senior et manager au sein de la *practice* Sécurité & risk management.