Alexandre Fernandez Toro

# Comprendre et mettre en œuvre la norme ISO 27001


Conseils pratiques d’implémentation

# Comprendre et mettre en œuvre la norme ISO 27001

Conseils pratiques d’implémentation

# Du même auteur

- **Sécurité opérationnelle**
  Conseils pratiques pour sécuriser le SI
  2ème édition
  Editions Eyrolles
  2016, 424 pages
  ISBN : 9 782212 144604
- **Management de la sécurité de l'information**
  3ème édition
  Editions Eyrolles
  2012, 322 pages
  ISBN : 9 782212 126976
  Epuisé.
  La 4ème édition est en cours de rédaction.


ISBN : 978-1-539-48040-2

Alexandre Fernandez Toro

# Comprendre et mettre en œuvre la norme ISO 27001

Conseils pratiques d’implémentation

# Table des matières



Connaissance de la norme et implémentation

## Mises en perspective



## Approche par l'exemple

# Avant-propos

## Objectif de ce livre

Ce livre a pour objectif d'aider le lecteur à implémenter un système de mangement de la sécurité de l'information (SMSI) conforme à la norme ISO 27001.

Il adopte pour cela une démarche résolument pratique. Le lecteur trouvera dans cet ouvrage :

- Une explication détaillée de chacun des articles de la norme.
- Des conseils pratiques d'implémentation pour chaque article.
- Des focus détaillant certains aspects liés au fonctionnement des SMSI.
- Un corpus complet de documents destinés à servir d'exemples pour implémenter un SMSI.

## Comment lire ce livre

Ce livre est conçu pour être lu de deux façons différentes. Selon l'objectif du lecteur, il pourra être lu séquentiellement ou accédé thématiquement.

- **Lecture séquentielle :** cette approche permet d'obtenir une vue complète du projet d'implémentation, depuis les étapes de conception, jusqu'à la phase de fonctionnement.
- **Accès thématique direct :** de par sa construction volontairement structurée, ce livre permet aussi une consultation thématique. Le but est d'apporter rapidement des réponses précises aux questions pratiques que l'implémenteur pourrait se poser.

Il est conseillé de commencer par une lecture séquentielle avant d'entamer la mise en place d'un SMSI. Une fois le projet en cours, un accès thématique sera plus approprié.

# Version de la norme

Ce livre se base sur la norme ISO 27001 dans sa version de 2013, qui est en vigueur aujourd'hui.

# Structure de ce livre

Ce livre est composé de trois parties, adoptant chacune un focus particulier. Ensemble, ces trois focus apportent un éclairage complet sur la norme.

## Premier focus : connaissance de la norme et implémentation

Les chapitres de cette partie étudient en détail les articles de la norme ISO 27001. Afin de faciliter la lecture, chaque chapitre contient systématiquement trois sections :

- **Objectif fondamental de l'article étudié :** l'intention de cette première section est de livrer, en une ou deux phrases, le sens fondamental de l'article dont il est question. En effet, l'objet des articles n'est pas toujours clairement exprimé dans le texte. Or, il est très important de le connaître pour faire les bons choix d'implémentation.
- **Synthèse :** certaines exigences de la norme sont très précises, alors que d'autres restent assez ouvertes aux interprétations. Un travail d'exégèse (au sens propre du terme) s'impose, c'est à dire qu'il faut expliquer clairement et en détail chacun des articles de la norme. C'est le but de cette section.
- **Conseils pratiques d'implémentation :** connaître les exigences ne suffit pas pour les implémenter. Il faut aussi connaître les recettes qui marchent et les pièges à éviter. Et pour cela, rien ne vaut l'expérience. Aussi, chaque chapitre de cette première partie comporte une section donnant des conseils pratiques d'implémentation, basés sur plusieurs dizaines de retours d'expérience.

## Second focus : mises en perspective

La seconde partie de cet ouvrage change complètement d'approche, en observant les SMSI dans leur fonctionnement. Elle met en perspective certains aspects de l'implémentation de la norme, comme par exemple :

- La difficulté à mettre en place certaines mesures de sécurité.

- Les aspects pratiques du modèle PDCA.
- Les apports du SMSI pour la sécurité.
- Le phénomène d'érosion que subissent tous les SMSI dans la durée.
- etc.

Ces problématiques, pourtant très importantes, ne sont malheureusement étudiées nulle part. Ce livre apporte un éclairage sur ces questions.

### Troisième focus : approche par l'exemple

La mise en application des exigences de la norme va nécessairement impliquer la rédaction d'un nombre important de documents. Cet aspect documentaire est souvent redouté par les implémenteurs, qui ne savent pas toujours ce que la norme attend d'eux. Ils ont peur de trop documenter ou, à l'inverse, de sous-estimer les exigences dans le domaine. Nombreux sont ceux qui aimeraient pouvoir disposer d'exemples concrets pour s'en inspirer.

Pour répondre à ce besoin, la dernière partie de cet ouvrage regroupe un ensemble complet de documents inspirés de SMSI réels. L'objectif est que l'essentiel des documents nécessaires à l'implémentation d'un SMSI soient présents. On y trouvera donc des exemples de descriptions de périmètre de SMSI, une liste des parties prenantes, une politique de sécurité des systèmes d'information, différentes procédures, ……

Le lecteur pourra donc s'en inspirer pour les adapter librement à son propre contexte.

## Conventions de lecture

Certains termes sont très utilisés dans cet ouvrage. Il est donc important de bien clarifier leur sens avant d'entamer la lecture.

- **SI :** désigne le système d'information.
- **SMSI :** cet acronyme signifie « système de management de la sécurité de l'information ».
- **Le projet :** ce terme désigne le projet de mise en place d'un SMSI.
- **La norme :** l'objet de cet ouvrage est la norme ISO 27001 dans sa version actuelle, qui date de 2013. Aussi, chaque fois que l'on parlera de « la norme », sans autre

précision particulière, cela désignera la version actuelle de l'ISO 27001.

- **Article :** la norme contient dix articles. Certains préfèrent parler de « chapitres », d'autres de « clauses ». Tous ces termes sont synonymes et désignent donc la même chose. Dans cet ouvrage, on utilisera exclusivement le terme « article ».
- **Entreprise / organisme :** tous les organismes peuvent mettre en place la norme ISO 27001, tant les organismes publics comme les sociétés privées. Par facilité de rédaction, on utilisera essentiellement dans cet ouvrage le terme « entreprise », mais il désignera autant les organismes publics que les sociétés privées.
- **Implémenteur :** tout projet d'implémentation de la norme nécessite de désigner un chef de projet. Cette personne aura la responsabilité de construire tous les processus nécessaires au SMSI. Dans cet ouvrage, c'est avec le terme « implémenteur » que l'on désignera cette personne.
- **RSSI :** c'est le responsable sécurité du système d'information. Comme il est souvent chargé d'implémenter le SMSI, on le confondra souvent dans cet ouvrage avec « l'implémenteur ».

# Information importante

Ce livre explique en détail l'ISO 27001 et propose de nombreuses approches pratiques pour implémenter les différents aspects de la norme. Toutefois, cet ouvrage ne remplace pas la norme, il en est un complément. Le lecteur est informé que l'achat de la norme auprès d'un éditeur autorisé est indispensable à tout projet d'implémentation.

# PARTIE I

# Connaissance de la norme et implémentation

Pour présenter la première partie de cet ouvrage, mettons-nous un instant dans la situation d'un chef de projet à qui on vient d'annoncer qu'il va devoir mettre en application la norme ISO 27001 dans la société où il travaille.

Ce chef de projet (que nous appellerons dorénavant « l'implémenteur ») sera immédiatement confronté à une foule de questions : qu'est qu'un système de management ? Qu'est-ce qu'un SMSI ? Quelles sont les normes les plus importantes de la série ISO 27000 ? Quel est l'intérêt d'implémenter un SMSI ?

Ensuite, l'implémenteur achètera la norme ISO 27001. Il constatera alors rapidement que les exigences de cette norme n'occupent pas plus de dix pages. Or, face à un document aussi resserré, comment comprendre en profondeur le sens des articles de cette norme ? Et quand bien même l'implémenteur aurait la réponse à cette question, où trouver les recettes pour mettre en œuvre concrètement chacune de ces exigences ?

L'objet de cette première partie est précisément de répondre à ces questions. Le tout premier chapitre présente les généralités sur les systèmes de mangement, sur les SMSI et sur les différentes normes. Quant aux chapitres suivants, ils reprennent systématiquement chaque article de la norme ISO 27001 et, pour chacun d'eux, ils expliquent le sens profond du texte, puis proposent des approches très concrètes pour implémenter.

# Chapitre 3
# Engagement de la direction

Maintenant que les bases du SMSI sont posées (contexte, parties prenantes, périmètre), il va devenir possible de commencer à construire le SMSI. Cependant, comme nous sommes en présence d'un projet d'entreprise, tous les services seront impactés de près ou de loin par le système de management. L'acceptation de la démarche ISO 27001 ainsi que le changement de certaines vieilles habitudes entraînera nécessairement des résistances de-ci de-là. Pour surmonter ces freins, la direction doit s'engager pleinement dans la démarche et montrer à tous l'importance de la sécurité de l'information. Voici comment la norme demande à la direction de s'engager.

## Exigence

L'article 5 de la norme est divisé en trois parties. Une première assez générale, une seconde traitant de la politique de sécurité, et une dernière abordant la répartition des rôles en matière de sécurité.

### Objectif fondamental de l'article 5

L'objectif de cet article est clairement de responsabiliser la direction en la plaçant au centre du SMSI. La direction devra donc adopter plusieurs rôles : animateur de la sécurité, financier, soutien aux équipes projets, législateur de la sécurité, etc.

## Synthèse

Commençons par l'article 5.1 qui aborde des questions relativement générales. Il peut paraître un peu décousu au premier abord. Il commence par rappeler qu'une politique et des objectifs doivent être établis (article 5.1 a). Ces points étant abordés plus loin dans la norme (articles 5.2 et 6.3, respectivement), nous ne les détaillons pas ici. Précisons seulement que cet article souligne le fait que la politique et les objectifs de sécurité sont du ressort de la direction.

L'article 5.1 b est intéressant, car on croit trop souvent que la mise en place d'un SMSI se limite simplement à réalisation de quelques projets organisationnels (rédaction d'une politique de sécurité, appréciation des risques, documentation) et techniques (application des correctifs de sécurité, sécurisation des serveurs, contrôle technique des applications, etc.). Or, l'article 5.1 b précise que les exigences de la norme doivent s'intégrer dans tous les métiers. Le projet de SMSI n'est donc pas un projet informatique, piloté uniquement par la DSI, et ne concernant que les informaticiens. C'est un projet d'entreprise couvrant toutes les activités, et c'est naturellement à la direction de s'assurer de la bonne intégration de la sécurité à tous les niveaux.

Il est logique que pour que le SMSI fonctionne, il lui faille des moyens. Ainsi, la direction doit-elle s'assurer que les ressources nécessaires pour faire fonctionner le SMSI sont disponibles. C'est l'objet de l'article 5.1 c. Que faut-il entendre par ressource ? Il peut s'agir de ressources humaines, financières, matérielles ou logicielles.

**Remarque**

Un chapitre de cet ouvrage intitulé « Support » détaille ce que sont les ressources du SMSI. Le lecteur intéressé est invité à s'y reporter.

La direction doit aussi s'efforcer de faire comprendre à tous l'importance de bien opérer le SMSI (article 5.1 d).

Une fois en place, les processus du SMSI produiront des résultats. C'est la responsabilité de la direction de s'assurer que ces résultats sont conformes aux attentes (article 5.1 e). La revue de direction sera l'outil par excellence qui permettra de vérifier l'atteinte de ces objectifs.

**Remarque**

Un chapitre de cet ouvrage explique en détail ce qu'est la revue de direction. Le lecteur intéressé est invité à s'y reporter.

Les processus mis en place dans le cadre du SMSI contribueront à améliorer la sécurité. Cependant, il ne fait aucun doute que

certaines directions ou certains métiers seront réticents à appliquer les consignes imposées par le SMSI. La direction doit alors soutenir le personnel pour faire en sorte que tout le monde applique les consignes (article 5.1 f et h). De plus, la direction insistera sur l'importance de l'amélioration continue (article 5.1 g).

**Remarque**

Un chapitre de cet ouvrage couvre l'amélioration continue. Le lecteur intéressé est invité à s'y reporter.

La deuxième partie de l'article (article 5.2) traite exclusivement de la politique de sécurité. Cette question fait toujours polémique, car elle est interprétée de façons très variées. L'ancienne norme BS 7799-2, qui a inspiré la norme actuelle, parlait de « politique du SMSI ». La version 2005 de la norme ISO 27001 reprenait littéralement cette expression. La version actuelle préfère formuler : « politique de sécurité de l'information».

Curieusement, au lieu de préciser clairement le contenu d'une telle politique, ne serait-ce que pour les grandes lignes, elle se contente de rappeler quelques contraintes à respecter. L'implémenteur est donc très libre dans la rédaction. La norme attend-elle de nous un simple engagement de la direction à faire de la sécurité ? Veut-elle, au contraire, que nous rédigions un document très détaillé, allant même jusqu'à aborder des questions techniques pointues ? Impossible de le savoir. En tout état de cause, le bon sens veut que la politique de sécurité cadre les actions relatives à la sécurité de l'information.

**Remarque**

La section suivante du présent chapitre détaille plusieurs approches possibles pour rédiger une politique de sécurité de l'information.

Le fait que cette exigence figure dans l'article 5 de la norme montre que la politique est du ressort de la direction. Certes, ce n'est pas elle qui rédigera les différentes clauses du document, mais c'est bien elle qui le validera. Les raisons pour lesquelles c'est à la direction de valider cette politique sont multiples :

- **Objectifs :** il faut vérifier que la politique est adaptée aux missions de l'organisme (article 5.2 a) et qu'elle tient compte des objectifs (article 5.2 b). Or, qui d'autre que la direction est mieux placé pour s'assurer de ces deux points ?
- **Applicabilité :** il est entendu que la politique de sécurité comportera de très nombreux articles assez techniques, essentiellement centrés sur les technologies de l'information. On pourrait donc penser qu'une simple validation par la DSI suffirait. Cependant, il faut que cette politique soit applicable

à toute l'organisation, quel que soit le service. En effet, si jamais une direction métier souhaite installer un accès Internet pour son périmètre ou contracter un service dans le *cloud* sans tenir compte de l'avis de la DSI, il faut pouvoir disposer d'un document interdisant clairement ce genre de pratique dangereuse. Or, pour que ce document ait un caractère exécutoire immédiat, il faut qu'il soit signé par la direction générale.

Naturellement, la politique de sécurité doit être intégrée dans le système de documentation de l'entreprise (article 5.2 e). Ce doit donc être un document référencé conformément aux pratiques documentaires internes. Elle doit par ailleurs être publiée pour être consultable par toute personne ayant besoin d'en connaître.

Rien dans ce document n'est secret. Si l'on veut que tous les services tiennent compte des exigences formulées dans la politique de sécurité, il faut qu'elle soit accessible à un grand nombre de collaborateurs (article 5.2 f) et que ceux-ci soient informés de l'existence de cette politique et sachent où la consulter. Nous sommes tout simplement en présence d'un document à diffusion interne. Il est donc parfaitement logique de le publier sur l'Intranet de l'entreprise afin qu'il puisse être consulté par tout-un-chacun.

Ajoutons que certaines parties prenantes demanderont à consulter la politique (article 5.2 g). C'est généralement le cas des clients souhaitant prendre connaissance des pratiques de sécurité de leurs fournisseurs. On pourra alors la leur transmettre sur demande.

Il ne sert à rien de clarifier les règles de sécurité du SI dans une politique si les différents collaborateurs concernés ne sont pas responsabilisés. La dernière partie de l'article (article 5.3) traite donc de la répartition des rôles et des responsabilités. Deux aspects font l'objet d'une attention particulière :

- **Aspect sécurité de l'information :** la sécurité des systèmes d'information doit être intégrée dans toutes les fonctions pertinentes et toutes les instances de gouvernance appropriées. Ainsi, chacun doit savoir clairement quels sont ses rôles et responsabilités en matière de sécurité.
- **Aspect SMSI :** la direction doit aussi désigner des personnes chargées de s'assurer que le SMSI est conforme à la norme et de rapporter ses performances. Nous verrons plus loin dans cet ouvrage que ces deux aspects sont essentiellement traités dans le cadre de l'audit interne et d'une instance appelée « revue de direction ».

# Conseils pratiques d'implémentation

Les deux grands enjeux pour implémenter l'article 5 de la norme sont la politique de sécurité de l'information et la répartition des rôles et responsabilités. Nous allons donc détailler ces deux points.

## Rédiger une politique de sécurité de l'information

La notion de politique de sécurité de l'information varie beaucoup d'un organisme à l'autre. On désigne ce document comme « politique de sécurité » ou « politique de sécurité de l'information », voire « politique de sécurité des systèmes d'information ». Toutes ces désignations correspondent à un même concept, celui d'un document cadrant les actions en matière de sécurité des SI.

**Remarque**

L'acronyme qui s'est largement imposé pour désigner les politiques de sécurité est « PSSI », pour « politique de sécurité du système d'information ». C'est donc cette nomenclature que nous utiliserons dorénavant.

Si nous demandions à un panel représentatif de RSSI de nous montrer leur politique de sécurité, on constaterait que deux grandes approches se dégagent. On trouverait d'abord les PSSI synthétiques, n'occupant qu'une quinzaine de pages. La seconde catégorie qui se dessinerait donnerait des PSSI bien plus détaillées, pouvant atteindre une centaine de pages. De façon marginale, on trouverait aussi une troisième approche, radicalement différente des précédentes, et qui ressemblerait plus à un engagement solennel de la direction plutôt qu'à une PSSI à proprement parler. Parcourons ces trois approches :

- **Politique synthétique :** cette approche est très répandue. Elle consiste à rédiger un document commençant par rappeler les principaux enjeux de l'entreprise. La PSSI enchaîne ensuite sur les grandes lignes à adopter en matière de sécurité. On y aborde les questions d'accès aux ressources du SI, le réseau, les applications, la gestion des droits, les authentifications, etc. Le but n'est pas vraiment d'entrer dans les détails techniques mais de rappeler des principes fondamentaux pour chaque domaine de la sécurité. Une quinzaine de pages suffit amplement pour exprimer ces contraintes. Une telle PSSI reste donc lisible d'un trait.
- **Politique détaillée :** une autre approche très répandue consiste à rédiger une PSSI détaillée. On constate que,

généralement, ces documents sont composés de 15 grands chapitres, eux même divisés en 35 grandes catégories, donnant lieu au final à une PSSI de 114 articles. Ici, nous reconnaissons clairement le plan de la norme ISO 27002. En fait, ces PSSI se calquent sur cette norme et déclinent chacun de ses articles par rapport aux pratiques locales le l'entreprise. Cette approche est très contestable pour plusieurs raisons. La première est qu'elle conduit à des documents très longs, pouvant atteindre une centaine de pages. Qui va lire un tel document dans son entier ? La seconde raison est que, très souvent, les implémenteurs qui retiennent cette approche pour rédiger la PSSI ne formalisent pas ce qui est effectivement appliqué dans l'entreprise, mais plutôt ce qu'ils aimeraient voir appliquer. On se retrouve donc avec une PSSI ne correspondant pas du tout aux pratiques internes. Dès le départ, il y a un écart entre les exigences de la PSSI et la réalité opérationnelle de la sécurité. Ce point est très négatif du point de vue de l'ISO 27001, car cela conduit à des documents ne correspondant pas à la réalité, et jamais consultés. Autant dire que c'est une démarche à éviter.

- **Engagement solennel de la direction :** une dernière approche existe. Elle est radicalement différente des deux précédentes. Dans cette approche, la direction rappelle l'importance de s'impliquer dans la sécurité des systèmes d'information et s'engage personnellement à ce que la sécurité soit prise en compte à tous les niveaux de l'entreprise. C'est donc un engagement solennel de la direction. Ce document ne fait qu'une page et est signé personnellement par la direction générale. Il est généralement affiché dans les lieux les plus fréquentés : affichages institutionnels de la direction, salles café, salles de réunion, etc. En fait, cette approche est directement issue des pratiques du monde de la qualité. Naturellement, cet engagement est tellement de haut niveau qu'il est nécessaire de le compléter avec une PSSI plus classique, entrant un peu plus dans les détails techniques.

Maintenant que nous avons passé en revue les trois grandes options pour rédiger une PSSI, il nous faut en choisir une pour le SMSI. Sur ce point, la norme ne nous aide pas du tout. En effet, l'ISO 27001 ne donne strictement aucun indice quant à la stratégie à adopter. On peut tout juste remarquer le fait que la PSSI est placée dans l'article 5, qui énonce les différents engagements de la direction. La PSSI est donc un document de haut niveau, signé par la direction générale.

Dans cet ouvrage, nous présentons une approche hybride, commençant par un engagement solennel de la direction, et se poursuivant par des grandes lignes synthétiques. Il faut porter

une attention particulière sur deux points. D'une part, la structure du document et, d'autre part, son style de rédaction.

Pour ce qui est de la structure, voici un plan type de PSSI :

- Rappel du contexte de l'entreprise.
- Rappel des objectifs en sécurité.
- Sécurité des infrastructures système.
- Sécurité des infrastructures réseau.
- Sécurité des applications.
- Gestion des identités.
- Accès aux locaux et protection des salles machines.
- Sécurité des postes de travail.
- Equipements mobiles.
- Règles de sécurité à respecter par les tiers.
- Continuité d'activité/reprise d'activité.
- Conformité avec les réglementations et les licences.

Il s'agira, pour chaque chapitre, de rappeler les règles élémentaires à respecter. En tout, il ne faudra pas dépasser une quinzaine de pages.

**Remarque**

Un exemple complet de PSSI est fourni en annexe de cet ouvrage. Le lecteur intéressé est invité à s'y reporter.

Les aspects relatifs au style sont tout aussi importants que la structure du document. En effet, la rédaction d'une PSSI est un domaine où la qualité de la langue est primordiale, car le document doit être clair, concis et non équivoque. Aussi, les phrases doivent-elles être courtes et grammaticalement simples. Au risque de paraître trop scolaire, il faut privilégier les phrases composées d'un sujet, d'un verbe et d'un complément.

**Exemple**

A la phrase « Un dispositif permettant de contrôler finement les échanges entre les réseaux internes et externes doit être installé afin de ne laisser passer que les protocoles nécessaires entre les sources et destinations préétablies », Il faudra lui préférer : « Les flux réseau doivent être filtrés par un pare-feu ».

Comme il s'agit d'une politique, et donc de règles à appliquer, le document doit être rédigé au mode impératif. Quant aux interdictions, elles doivent être clairement énoncées.

**Exemple**

A la phrase « L'utilisation d'applications proposées par des fournisseurs sur Internet, et proposant des services d'échange de fichiers, de prise de contrôle à distance, la messagerie, ou tout autre type de service clé en main doit être validé au préalable par la DSI », il faut lui préférer « Il est interdit d'utiliser un service du *cloud* non validé par la DSI ».

Les articles de la politique doivent être brefs, et ils doivent tous être numérotés. Le but de cette numérotation est de pouvoir opposer un numéro d'article bien précis à toute personne ne respectant pas la règle.

**Exemple**

Il est plus simple de rappeler à un utilisateur récalcitrant que l'article 4.3.5 de la PSSI stipule sans équivoque que « 4.3.5. Toute installation d'une liaison Internet non validée par la DSI est strictement interdite », plutôt que de dire que quelque part dans la PSSI il y a une phrase interdisant cette pratique.

Le niveau de détail des exigences doit être soigneusement choisi. Il faut être suffisamment générique pour rester applicable dans le temps, indépendamment des évolutions technologiques et de contexte, mais suffisamment précis pour que l'interprétation soit claire et non équivoque.

**Exemple**

Il est peu prudent d'écrire « Les liaisons chiffrées pour les tunnels doivent être protégées par le protocole TLS v1.1 ». La version sûre de ce protocole ne manquera pas d'évoluer. De plus, rien ne prouve que l'usage même du protocole TLS soit indiqué pour tous les cas de figure. Il est donc préférable de formuler l'exigence de la façon suivante : « Tout tunnel doit être protégé par un protocole de chiffrement adapté, reconnu et à jour ».

Il faut aussi éviter les explications inutiles. Une politique n'a pas pour but de faire comprendre un enjeu de sécurité. Elle a pour but de dire clairement ce qui est autorisé et ce qui est interdit. Si, par ailleurs, il y a un besoin de pédagogie, rien n'empêche le RSSI de compléter la politique par des actions de sensibilisation appropriées.

**Exemple**

L'explication suivante est parfaitement inutile dans une PSSI : « Les pirates utilisent des dictionnaires précalculés pour essayer de casser les mots de passe. Si votre mot de passe correspond à un mot du dictionnaire, il sera nécessairement compromis. Il ne faut donc pas choisir un mot de passe figurant dans le dictionnaire. » Il suffit de dire « Les mots de passe doivent être complexes et ne jamais figurer dans le dictionnaire ».

Un dernier point à signaler est que la PSSI doit correspondre à la réalité ou, tout du moins, à une réalité raisonnablement atteignable. Exiger de l'authentification forte à tous les niveaux, ou imposer partout des mots de passe de vingt caractères, renouvelés tous les trois mois n'a aucun sens car ces exigences ne seront jamais respectées. En revanche, exiger que tous les systèmes d'exploitation des infrastructures les plus exposées sur Internet soient à jour est un objectif salutaire et parfaitement atteignable. On peut poser cette règle dans la PSSI, même si elle n'est pas encore tout à fait satisfaite dans un premier temps.

Terminons cette partie sur la PSSI en précisant que le document doit être signé par la direction générale. Ainsi, le RSSI pourra opposer la PSSI à toute personne de l'entreprise, quelle que soit la direction dans laquelle elle travaille, et quel que soit son niveau hiérarchique.

## Répartir les rôles et responsabilités en matière de sécurité

Pour répartir les rôles et les responsabilités, l'implémenteur doit commencer par se demander quelles sont les fonctions dans l'entreprise pour lesquelles il y a des responsabilités (de quelque nature qu'elles soient) en matière de sécurité des SI. On sera étonné du nombre important de fonctions concernées. Naturellement, la première fonction à laquelle on pense est le RSSI. Par nature, il consacre tout son temps à la sécurité de l'information. Très rapidement, on pensera aussi aux principaux responsables de la DSI (responsable de la production, responsable des études, etc.). Pour chacune de ces fonctions, il faudra formaliser les responsabilités dans le domaine de la sécurité. Passons en revue ces principales fonctions :

- **Le DSI :** on ne pense pas forcément au DSI en premier. Pourtant, c'est bien lui qui fournit l'essentiel des moyens au RSSI. C'est aussi lui qui le soutient dans son action en tranchant en sa faveur chaque fois que cela est nécessaire (du moins, dans un monde parfait).
- **Le RSSI :** toutes les missions du RSSI sont liées à la sécurité de l'information. Il suffit donc de lire sa fiche de poste pour énumérer ses responsabilités. Généralement, le RSSI est chargé de définir la PSSI, il est responsable du bon fonctionnement des mesures de sécurité, il définit et met en œuvre des plans d'action pour sécuriser le SI, il procède à l'appréciation des risques et en déduit un plan de traitement des risques, il coordonne les actions en cas d'incident de sécurité, il assure une veille technologique et une veille en vulnérabilité, et il sensibilise le personnel aux questions de sécurité.

- **Les responsables de la DSI :** par leur position, les différents responsables de la DSI sont les relais du RSSI pour la production, les développements, les infrastructures, etc. Ils sont donc garants du respect de la PSSI par leurs équipes. Ainsi, doivent-ils relayer auprès de leurs collaborateurs les consignes du RSSI, et exploiter les mesures de sécurité qui sont de leur ressort.
- **Les architectes :** ils ont un rôle clé en sécurité car les solutions qu'ils conçoivent impactent de façon durable les systèmes d'information. La prise en compte de la sécurité dès les phases d'architecture est un point très important. Les architectes se doivent donc de consulter systématiquement le RSSI dans leurs choix et d'appliquer ses directives.
- **Les chefs de projet :** ils doivent intégrer la sécurité le plus en amont possible dans leurs projets. Pour cela, ils sont tenus de consulter la PSSI et de s'assurer que leurs actions sont conformes à ce document. En cas de doute, ils doivent consulter le RSSI.
- **Les développeurs :** ils doivent respecter les consignes de sécurité édictées pour les développements (bonnes pratiques de l'OWASP ou autre référentiel de sécurité). L'usage responsable des données de test fait aussi partie de leurs obligations.
- **Les administrateurs :** qu'ils manipulent des systèmes d'exploitation, des bases de données ou des équipements réseau, les administrateurs sont tenus d'exploiter ces ressources conformément aux consignes de la PSSI. Par ailleurs, ils doivent informer le RSSI en cas d'incident de sécurité. On peut aussi leur demander de signer une charte spécifique.
- **Les techniciens :** qu'il s'agisse de techniciens de proximité ou d'agents de support technique réglant les problèmes des utilisateurs par téléphone, ces personnels bénéficient de privilèges techniques très proches de ceux des administrateurs. Leurs responsabilités en matière de sécurité sont donc très similaires à celles des administrateurs.

En fait, ce sont quasiment toutes les fonctions de la DSI dont il faut se poser la question des responsabilités en matière de sécurité. Mais la sécurité de l'information ne concerne pas que les informaticiens. D'autres collaborateurs sont aussi concernés :

- **La direction générale :** elle fournit au RSSI les moyens humains et financiers pour conduire toutes les actions pertinentes en sécurité. Elle doit aussi prendre connaissance des risques résiduels et les valider. Elle doit enfin valider la PSSI.

- **Les directeurs de service :** ils sont les garants de la bonne application de la PSSI par leurs équipes, et de l'observation de la charte utilisateurs. En tant que propriétaires des risques qui leur incombent, ils doivent les connaître et les accepter. On peut aussi les charger de faire en sorte que leurs équipes conduisent périodiquement les revues de droits sur les applications les plus importantes.
- **Le responsable de la qualité :** si l'organisme a déjà mis en place un ou plusieurs systèmes de management (par exemple les certifications ISO 9001, ISO 14001 ou autres) il est quasiment certain qu'il dispose d'un responsable qualité. Ce dernier est l'acteur idéal pour contrôler tous les aspects purement système de management du SMSI. Il sera plus particulièrement chargé de piloter les audits internes du SMSI, de contrôler le bon suivi des actions correctives et de s'assurer du respect de la gestion de la documentation.
- **Le responsable de l'audit interne :** on peut logiquement lui demander de piloter des audits techniques ou organisationnels sur le système d'information. Il pourra aussi contrôler le suivi des actions suite aux audits précédents.
- **Le gestionnaire des risques :** s'il convient que l'appréciation des risques en sécurité de l'information soit confiée à un spécialise du domaine ou au RSSI, il est parfaitement logique de se rapprocher du gestionnaire des risques, qui pourra apporter son éclairage sur les risques opérationnels.

Enfin, selon les cas, certains métiers seront particulièrement concernés. Notamment, les métiers techniques ainsi que les métiers amenés à manipuler des données sensibles (données à caractère personnel ou secrets industriels et commerciaux).

- **Les informaticiens industriels :** bien que leur action soit focalisée essentiellement sur les automates, ils sont aussi amenés à administrer des systèmes complexes de contrôle/commande. En ce sens, leurs responsabilités sont très proches de celles des administrateurs (système, réseau ou bases de données).
- **Les personnes gérant des données à caractère personnel :** chaque collaborateur amené à manipuler des données à caractère personnel se doit de bien protéger lesdites données en respectant scrupuleusement les procédures établies. Outre la DRH, les métiers concernés sont essentiellement les métiers liés à la relation client, aux interventions client, à la facturation ou au marketing.

- **Les collaborateurs de la R & D :** les personnels travaillant dans les départements de recherche et développement ont la responsabilité de soigner la confidentialité des données qu'ils manipulent. En effet, ces données font partie du capital incorporel de l'entreprise, qui la différencie des concurrents.
- **Le service commercial :** par nature, et quel que soit le secteur économique, les offres commerciales sont strictement secrètes tant qu'elles n'ont pas été soumises aux clients. Toute personne manipulant des informations liées à la préparation des offres commerciales doit suivre les procédures établies pour les garder secrètes.

Maintenant que les fonctions sont bien répertoriées et que l'on a explicitement formalisé leurs responsabilités respectives, il reste à faire l'inventaire des instances au sein desquelles des décisions de sécurité sont prises. Les principales instances sont les suivantes :

- **Le comité de direction :** une fois par an, il valide les risques et le plan de traitement des risques. Occasionnellement, il peut aussi faire un point d'avancement avec le RSSI sur les travaux de sécurisation du SI.
- **Comité de la DSI :** se réunissant de façon régulière, le comité de la DSI permet de faire le point sur tous les projets et les questions d'actualité concernant la DSI. C'est l'occasion pour le RSSI de s'assurer que la sécurité est bien prise en compte. Cela permet d'intégrer la sécurité dans les arbitrages de la DSI.
- **Comité sécurité :** cette instance permet de faire le point sur toutes les actions de sécurité en cours. Il est aussi l'occasion de faire un retour d'expérience sur les incidents de sécurité survenus dans la période. Ce comité sert enfin à décider des plans d'action suite aux audits de sécurité subis dernièrement.
- **Comité sécurité groupe :** les sociétés faisant partie d'un groupe disposent souvent d'un comité de sécurité animé par le RSSI groupe. Le but est double. Il sert d'abord au RSSI groupe à imposer des actions et des procédures homogènes dans toutes les entités. Mais ce comité est aussi très utile pour que chacun partage ses propres expériences. C'est donc une instance d'échange très enrichissante.

- **Comité d'architecture :** de nombreux organismes mettent en œuvre un comité destiné à trancher toutes les questions d'architecture (qu'il s'agisse d'infrastructure ou d'applications). Le RSSI est fondé à intervenir afin de conseiller les architectes sur les choix, et de faire en sorte que les options retenues tiennent compte des contraintes de la sécurité.
- **Autres comités métier :** chaque métier dispose généralement d'un comité qui lui permet de suivre les actions en cours avec le directeur du service. Le RSSI est fondé à « s'inviter » ponctuellement afin de traiter des questions de sécurité spécifiques à ce métier. Cette démarche est salutaire, car elle rapproche le RSSI des utilisateurs.

Nous avons maintenant fait le tour de toutes les fonctions et de toutes les instances où les décisions sont prises dans le domaine de la sécurité. Il reste maintenant à officialiser tout cela. Pour ce faire, l'implémenteur peut rédiger un document de synthèse que l'on peut intituler : « Organisation de la sécurité ».

**Remarque**

Un exemple de document d'organisation de la sécurité est fourni en annexe de cet ouvrage. Le lecteur intéressé est invité à s'y reporter.

Ce document est composé de deux parties. Une première partie récapitule le plus clairement possible toutes les responsabilités en matière de sécurité pour chaque fonction. Une seconde partie rappelle toutes les instances au sein desquelles des décisions sont prises dans le domaine. Pour chaque instance, on précisera les points suivants :

- Dénomination de l'instance.
- Périodicité de tenue.
- Qui en est le président.
- Qui compose cette instance.
- Quelles sont les décisions prises dans le domaine de la sécurité.

Il est important que ce document soit signé par la direction générale pour que chacun se sente responsabilisé dans son domaine.

Dans la mesure du possible, il convient de reporter sur la fiche de poste de chaque collaborateur les missions et responsabilités précisées dans le document « Organisation de la sécurité ». Si cette approche est idéale, elle n'est pas forcément facile à réaliser car, très souvent, modifier les fiches de poste implique la

consultation des représentants du personnel, ce qui est une opération politiquement délicate.

Cette répartition des rôles et responsabilités doit être impérativement complétée par la rédaction d'une charte destinée à tous les collaborateurs de l'entreprise. La charte cadrant l'usage qui doit être fait des moyens informatiques fournis par l'entreprise doit être annexée au règlement intérieur. De cette façon elle devient, de fait, opposable à tout le personnel soumis au règlement intérieur. Comme elle devra être validée par les représentants du personnel, il est important de faire rédiger la charte par un juriste et de la faire approuver par la DRH.

# Traces

Les traces qu'il convient de garder dans le cadre des engagements de la direction sont les suivantes :

- La politique de sécurité des systèmes d'information.
- Le document décrivant les rôles et responsabilités dans la sécurité des systèmes d'information.
- La charte de bon usage des moyens informatiques annexée au règlement intérieur.