ALEXANDRE **FERNANDEZ-TORO**

Préface de **Hervé Schauer**

# Management de la sécurité de l'information

## Implémentation ISO 27001 et ISO 27002

## Mise en place d'un SMSI et audit de certification

 ISBN : 978-2-212-12697-6

EYROLLES

# Préface

J'observe et je m'implique dans la sécurité des systèmes d'information (SSI) depuis plus de 20 ans, et notamment, depuis 1989, à la tête de ma société de conseil en sécurité HSC. La norme ISO 27001 est la révolution qui manquait à ce secteur souffrant cruellement d'une opacité entre les mondes de la direction et celui de la technique. Pendant 15 ans, j'ai accompagné mes clients dans leur démarche souvent fastidieuse pour justifier des investissements pourtant indispensables à la protection du patrimoine informationnel de leur organisation. L'ISO 27001 est à mes yeux le ciment qu'il manquait pour sortir la SSI de sa bulle.

Cette norme est une bouffée d'oxygène dans un environnement de plus en plus sous pression : systèmes d'information à croissance et interconnexion exponentielle, sentiment d'insécurité générale due à un contexte géopolitique difficile, mondialisation des échanges et concurrence féroce, pression réglementaire – SoX, Bâle II, Cour des comptes, etc.

La série des normes ISO 27001 est là pour répondre et anticiper ces besoins pour la sécurité de l'information dans un cadre global.

L'ISO 27001 applique à la sécurité des systèmes d'information les principes de la qualité. Cela permet de gérer la sécurité dans le temps, ce qui a tant manqué jusqu'à présent dans les entreprises, et de s'intégrer dans un tout performant et concurrentiel.

La mise en œuvre de l'ISO 27001 est celle d'un processus : le système de management de la sécurité de l'information (SMSI). Cela n'est pas difficile ; cependant, tout métier a besoin de temps pour s'approprier une telle évolution. Ce livre pratique est là pour que chacun puisse dès à présent maîtriser, mettre en œuvre concrètement et auditer son SMSI, et ainsi progresser en même temps que son employeur.

Il est rédigé par le francophone incontestablement le plus expérimenté dans le domaine. Alliant à sa compétence d'informaticien des qualités pédagogiques qui lui sont reconnues par les stagiaires qui l'ont suivi, Alexandre Fernandez-Toro possède le don de conter les histoires, d'illustrer notre formation de références culturelles et ainsi permettre à ses étudiants d'appréhender facilement les concepts les plus pointus.

Ce sont toutes ces qualités professionnelles et pédagogiques que vous retrouverez dans cet ouvrage. Un condensé d'expériences sur le terrain (mise en œuvre, audit) alliées à la richesse des échanges avec les centaines de stagiaires que nous avons eu le plaisir de préparer à la certification.

Bonne lecture !
Hervé Schauer

# Table des matières

## Partie II – Normes de la série ISO 27000

## Partie III – Implémenter un SMSI

## Partie IV – Audit des SMSI

# Avant-propos

À l'heure où l'ensemble de l'activité économique migre vers le tout numérique, la sécurité des systèmes d'information est devenue un enjeu crucial. Les solutions techniques et organisationnelles existent pour assurer la sécurité, mais elles sont trop souvent déployées indépendamment les unes des autres, sans aucune cohérence d'ensemble. Cela conduit à une sécurité partielle et désorganisée.

La norme ISO 27001 est précisément l'outil qui manquait pour sécuriser le système d'information de façon cohérente. Malheureusement, beaucoup d'acteurs pensent encore que pour implémenter la norme, il suffit de rédiger « de la procédure » et de procéder à une simple analyse des risques… ce qui est tout à fait réducteur.

## À qui s'adresse cet ouvrage ?

Ce livre s'adresse aux professionnels souhaitant comprendre la norme et voulant savoir très concrètement comment mettre en place un système de management de la sécurité de l'information (SMSI) conforme aux exigences de l'ISO 27001. Par ailleurs, il permet à ceux qui souhaitent obtenir une certification ISO 27001 de se préparer au mieux à cet audit, encore trop souvent mal vécu.

## Structure de l'ouvrage

La compréhension et l'application des normes ISO 27001 et ISO 27002 constituent la base de cet ouvrage, enrichi en conséquence de retours d'expérience lors de missions de conseil à l'implémentation. Notez que cet ouvrage ne remplace pas les normes. Aussi l'achat du texte des normes ISO évoquées ici est-il indispensable à toute personne souhaitant implémenter un SMSI.

Cet ouvrage est articulé en quatre parties.

La première présente les systèmes de management ainsi que les normes ISO 27001 et ISO 27002, qui sont au cœur du sujet. La deuxième partie présente les normes les plus intéressantes de la famille 27000. Dans la troisième partie, il est

expliqué comment implémenter un SMSI. Cet ouvrage finit, dans une quatrième partie, par détailler le processus de certification et fournit une aide à la préparation de l'audit.

## Dans cette nouvelle édition

Depuis la première édition de cet ouvrage, la percée de l'ISO 27001 s'est confirmée en entreprise, même si les certifications ne progressent que doucement.

La parution de nombreuses normes dans la famille 27000 est un événement majeur dans la gestion des risques en sécurité de l'information. Ce sont, en fait, tous les aspects les plus importants de la sécurité des systèmes d'information qui sont maintenant normalisés par l'ISO.

Enfin, le nombre de SMSI installés (qu'ils soient certifiés ou pas) nous donne aujourd'hui suffisamment de recul pour savoir quelle est la valeur réelle de la certification.

Cette nouvelle édition ne pouvait ignorer ces trois points.

## Remerciements

Je tiens à remercier Pierre Manier, mon vieux maître, et Gérard Florin, mon professeur au CNAM. Je remercie également Caline Villacres pour sa lecture attentive de mon livre et la pertinence de ses remarques. Je remercie enfin Hervé Schauer, référence incontestée de la sécurité des systèmes d'information, sans qui je n'aurais jamais pu écrire ce livre. Par sa personnalité visionnaire et percutante, il œuvre depuis près de vingt ans à rendre à la sécurité de l'information ses lettres de noblesse dans les entreprises de notre pays.

Chapitre 1

# Les systèmes de management

Les systèmes de management de la sécurité de l'information (SMSI) sont avant tout des *systèmes de management*, c'est-à-dire qu'ils appliquent à la sécurité de l'information les recettes déjà éprouvées dans d'autres domaines, notamment la qualité. En ce sens, ils présentent exactement les mêmes caractéristiques que tous les autres systèmes de management. Ce premier chapitre rappelle les principes de base de ces systèmes et constitue une première approche des SMSI.

## Qu'est-ce qu'un système de management ?

Le principe de système de management n'est pas nouveau. Il concerne historiquement le monde de la qualité, surtout dans le domaine des services et de l'industrie. Qui n'a jamais vu un papier à en-tête avec un petit logo « certifié ISO 9001 » ? Qui n'a jamais croisé une camionnette affichant fièrement un autocollant « Société certifiée ISO 9001 » ? La norme ISO 9001 précise les exigences auxquelles il faut répondre pour mettre en place un système de management de la qualité (SMQ).

Comment définir un système de management ? La norme ISO 9000 (à ne pas confondre avec l'ISO 9001 que nous venons d'évoquer) apporte une réponse à cette question en définissant les principes de la qualité. C'est ainsi que dans la rubrique intitulée « Système de management », il est dit qu'un système de management est un système permettant :

- d'établir une politique ;
- d'établir des objectifs ;
- d'atteindre ces objectifs.

La définition est tellement générique qu'il est difficile d'en comprendre clairement le sens. Une définition un peu plus empirique pourra nous éclairer.

Nous pouvons ainsi dire qu'un système de management est un ensemble de mesures organisationnelles et techniques visant à atteindre un objectif et, une fois celui-ci atteint, à s'y tenir, voire à le dépasser.

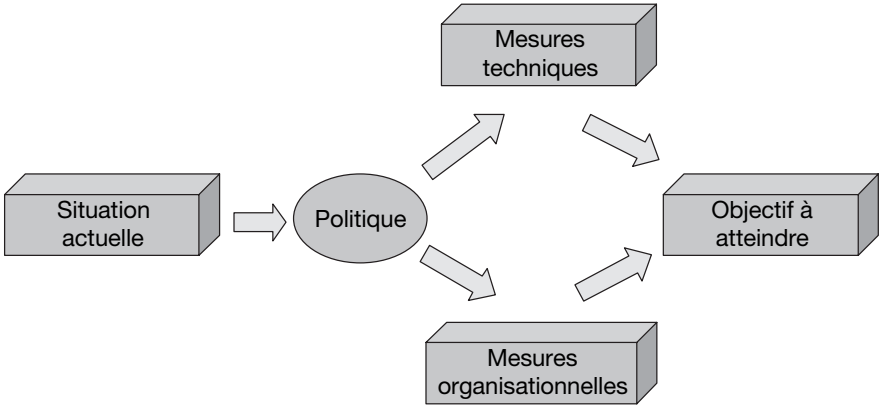


*Figure 1-1 : Vision empirique d'un système de management*

## Principaux systèmes de management

Les systèmes de management ne se cantonnent pas uniquement à la qualité. Ils concernent des domaines très variés comme l'environnement, les services informatiques, la sécurité de l'information, la sécurité alimentaire ou encore la santé. Le tableau ci-après donne un aperçu non exhaustif des principaux référentiels de systèmes de management.

*Tableau 1-1 : Différents référentiels de systèmes de management*

| Référentiel | Domaine |
|---|---|
| ISO 9001 | Qualité |
| ISO 14001 | Environnement |
| ISO 27001 | Sécurité de l'information |
| ISO 20000 | Services informatiques |
| ISO 22000 | Sécurité alimentaire |
| OHSAS 18001 | Santé/Sécurité du personnel |

Nous constatons que la majorité de ces référentiels sont normalisés par l'ISO (Organisation internationale de normalisation). Cependant, d'autres organismes privés ou nationaux peuvent proposer leurs propres référentiels. La dernière ligne de cette liste montre, en effet, que l'ISO n'a pas le monopole des systèmes de management, puisque la norme relative à la sécurité du personnel au travail (OHSAS 18001) n'est pas spécifiée par l'ISO.

## Propriétés des systèmes de management

Continuons à nous intéresser aux systèmes de management en général, en faisant abstraction (pour le moment) de la sécurité de l'information. Parmi les nombreuses propriétés partagées par ces systèmes, quatre d'entre elles nous intéressent plus particulièrement pour la suite.

### Large spectre de métiers et de compétences

Quel que soit leur périmètre (du plus petit au plus ambitieux), les systèmes de management impliquent un nombre important de métiers et de compétences. Aussi, même si le périmètre ne couvre qu'une toute petite partie de l'activité de l'entreprise, il nécessite la participation de différents corps de métiers.

> **Exemple**
>
> Considérons une société implantée sur un seul site, développant et fabriquant des équipements électroménagers. Elle a mis en place un système de management dont le périmètre ne couvre que les activités de recherche et développement (R&D), ce qui représente un petit périmètre. Dans ces conditions, il paraît logique que seules les personnes travaillant dans le laboratoire de R&D soient concernées. Ce n'est pourtant pas le cas.
>
> – Le service de R&D est hébergé dans les locaux de l'entreprise. Il consomme de l'eau, de l'électricité, de l'air conditionné et tout autre type de servitudes. Les personnes des services généraux sont donc concernées, même indirectement.
>
> – Le service de R&D utilise les ressources informatiques qui sont mises à sa disposition : serveurs, réseau, postes de travail, etc. Les informaticiens sont donc aussi concernés par le système de management.
>
> – Toutes ces personnes (informaticiens, techniciens des services généraux, chercheurs) sont des employés ou des sous-traitants de la société, il est donc logique que le service du personnel soit impliqué dans le système de management.
>
> – Enfin, chaque fois que le service de R&D achète des biens ou des services, cela concerne également la comptabilité et les finances.

Par conséquent, la mise en place d'un système de management est nécessairement un projet transversal, couvrant de nombreux services de l'entreprise. Ne pas en tenir compte peut avoir de graves conséquences lors de la mise en place d'un tel système.

## Un projet fédérateur et mobilisateur

À l'approche transversale que nous venons d'évoquer s'ajoute une approche verticale. Concrètement, cela signifie qu'un système de management implique toute la hiérarchie de l'entreprise. Bien sûr, cela commence par les plus hauts responsables, qui sont à l'initiative du système et qui se doivent de montrer l'exemple. Les cadres et employés ont également leur part de responsabilité dans la mise en œuvre et l'exploitation de ces systèmes de management. Mais l'on oublie aussi trop facilement les personnes travaillant à l'accueil et les techniciens de surface, car elles interagissent également de près ou de loin avec le système.

> **Exemple**
>
> Généralement, les personnes concernées par les systèmes de management sont :
>
> – les membres de la direction générale ;
>
> – les principaux responsables des services concernés ;
>
> – tous les cadres et employés directement impliqués dans les activités couvertes par le système de management ;
>
> – tous les cadres ou employés indirectement impliqués par le système de management.

## Importance de l'écrit

On ne peut pas concevoir un système de management sans passer par l'écrit. La formalisation des politiques et des procédures de l'entreprise est indispensable. Or, la transmission de la connaissance dans l'entreprise se fait encore très souvent par tradition orale (les anciens employés expliquant aux nouveaux les procédures en situation, par l'exemple). Les systèmes de management imposent de passer à la tradition écrite.

> **Tradition écrite**
>
> Les industriels en général, et le secteur aéronautique en particulier, ont la culture de la tradition écrite depuis longtemps. Les procédures sont écrites et les décisions sont prises lors de commissions, donnant lieu à des comptes rendus. J'ai même vu une entreprise réunir une commission pour décider du changement de place ou non d'une simple prise de courant. Il faut dire que la sensibilité de son activité le justifiait amplement.

> **Tradition orale**
>
> Les sociétés du secteur tertiaire, et notamment les *start-up* d'Internet, ont la réputation de moins formaliser leurs procédures. La transmission de la connaissance se fait le plus souvent par tradition orale.

Naturellement, il ne faut pas exagérer cette division manichéenne entre un secteur industriel, qui serait le bon élève, et un secteur des services qui serait le cancre, dans la mesure où de nombreuses exceptions existent de part et d'autre.

Ce passage de la tradition orale à la tradition écrite est l'une des difficultés majeures dans la mise en place et l'exploitation d'un système de management. Il convient cependant de se garder de tout abus en matière d'écrit, car trop d'écrit tue l'écrit. Ce point fait l'objet d'un développement dans la seconde partie de l'ouvrage.

### Auditabilité

Dans la mesure où l'entreprise qui a mis en place un système de management formalise ses procédures par écrit et consigne les principales décisions dans des comptes rendus, il devient possible à une personne extérieure (un auditeur, par exemple) de venir vérifier que ce qui est pratiqué correspond effectivement à ce qui a été spécifié par écrit.

La conséquence de cette propriété est que l'audit est indissociable des systèmes de management. On ne peut pas considérer l'un sans l'autre. Par conséquent, un système de management implique systématiquement la mise en place d'un processus d'audit.

## Apports des systèmes de management

Les propriétés que nous venons de décrire donnent de bonnes raisons de penser que la mise en place et l'exploitation d'un système de management n'est pas un projet facile à mener. Il faut commencer par fixer des politiques, formaliser les procédures par écrit et mener à bien des audits réguliers. Ces opérations sont loin d'être transparentes. Souvent lourdes à implémenter, leur coût humain et financier n'est pas négligeable. Dans ces conditions, il est légitime de se demander ce qui justifie un tel investissement. Quels bénéfices concrets pouvons-nous en espérer ?

### Premier apport : l'adoption de bonnes pratiques

Les systèmes de management se basent sur des guides de bonnes pratiques dans le domaine qui les concerne (qualité, sécurité, environnement, etc.). Ainsi, celui qui se lance dans la mise en place d'un système de management est quasiment obligé d'adopter ces bonnes pratiques.

> **Exemple**
> Un système de management en sécurité de l'information permettra d'adopter des mesures de sécurité appropriées aux besoins de l'entreprise, en posant les bonnes questions. Quels sont les éléments les plus sensibles de l'entreprise ? Où déployer en priorité les mesures de sécurité ? Comment cloisonner les réseaux ? Comment détecter les incidents ? Comment réagir rapidement aux intrusions ? Comment améliorer les processus ? Et ainsi de suite…

### Deuxième apport : l'augmentation de la fiabilité

L'adoption de bonnes pratiques a pour conséquence directe, à court ou moyen terme, l'augmentation de la fiabilité. Ceci est principalement dû au fait que les systèmes de management imposent la mise en place de mécanismes d'amélioration continue favorisant la capitalisation sur les retours d'expérience.

> **Exemple**
> Considérons une entreprise qui, dans le cadre de son SMSI, a mis en place une procédure de réaction aux incidents de sécurité. Lorsqu'une tentative d'intrusion se produit sur le réseau, les équipes savent ce qu'elles ont à faire et agissent en conséquence pour limiter l'impact de cette attaque. Après coup, l'attaque est analysée et des actions préventives sont entreprises pour éviter qu'une telle agression puisse se reproduire. Sur la durée, cette organisation rend les attaques de plus en plus difficiles à réaliser.

### Troisième apport : la confiance

Il est vrai que le fait d'adopter de bonnes pratiques entraîne (à court ou moyen terme) une augmentation de la fiabilité. Mais ceci n'apporte pas en soi d'avantage commercial particulier. Encore faut-il faire connaître cette amélioration. Pour cela, l'entreprise fait appel à des auditeurs indépendants qui certifieront qu'elle applique effectivement les référentiels qu'elle s'est engagée à adopter (ISO 9001, ISO 27001 ou autre). C'est parce que des auditeurs indépendants certifient que les pratiques sont conformes aux référentiels que les systèmes de management apportent la confiance aux parties prenantes.

Nous touchons enfin à la raison d'être des systèmes de management : ils fournissent la confiance envers les parties prenantes. Qu'entendons-nous par *parties prenantes* ? Il s'agit de toute personne, groupe ou instance envers laquelle l'entreprise doit rendre des comptes. Les parties prenantes les plus classiques sont les suivantes :

1. **Les actionnaires :** en tant que propriétaires, ils sont directement concernés par les résultats de l'entreprise.
2. **Les autorités de tutelle :** les administrations doivent rendre des comptes à leurs autorités de tutelle, qui fixent leurs missions.
3. **Les clients :** ils sont la partie prenante par excellence, puisque l'entreprise ne peut vivre sans eux.
4. **Les fournisseurs :** même si la relation client-fournisseur place souvent ceux-ci en situation d'infériorité, l'entreprise a des responsabilités envers eux.
5. **Les partenaires :** les relations de partenariat sont devenues indispensables pour le développement de l'entreprise. Si les partenaires n'ont pas confiance, ils ne collaboreront pas.
6. **Les banques et les assurances :** l'entreprise ne peut pas vivre sans leur confiance.

7. **Le personnel :** son adhésion est capitale pour le bon fonctionnement de l'entreprise.
8. **L'opinion publique :** elle a un pouvoir de sanction très important, dont les conséquences peuvent se révéler désastreuses pour l'entreprise.

> **Vocabulaire : parties prenantes, *stakeholders*, *interested parties***
> La traduction usuelle de « partie prenante » en anglais est *stakeholder*, terme souvent employé tel quel en français. Par ailleurs, la norme ISO 27001, qui sera présentée dans la suite de cet ouvrage, parle également de *interested parties*. Il faut donc considérer les termes partie prenante, *stakeholder* et *interested parties* comme ayant le même sens.

Sans la pression des parties prenantes, les systèmes de management n'existeraient pas. Ils sont mis en place à cause des parties prenantes, pour les parties prenantes, parce qu'elles exigent qu'on leur fournisse de la confiance.

Pourquoi la confiance est-elle si importante ? Tout simplement, parce que qui dit confiance dit business. Cette formule quelque peu commerciale est pourtant essentielle.

> **Exemple**
> Considérons une entreprise qui souhaite rendre plus attractif son site web, devenu trop vieillot. Elle recherche une agence qui se chargera de proposer une nouvelle charte graphique, de développer les nouvelles pages et de les mettre en ligne. Après quelques recherches, l'entreprise trouve une agence. En tant que cliente, elle n'a aucune garantie de la qualité du service qui lui sera rendu par l'agence. D'un autre côté, rien ne garantit à l'agence que l'entreprise payera la facture en fin de prestation. Pourtant, le contrat est passé. Qu'est-ce qui fait que le contrat est signé ? C'est la confiance.

En fait, nous oublions trop souvent que la confiance est le vecteur qui permet toute relation entre un client et un fournisseur. Autant dire qu'il n'y aurait aucune activité économique sans la confiance.

## Le modèle PDCA

Les systèmes de management fonctionnent selon un modèle en quatre temps appelé « PDCA », pour P*lan*, D*o*, C*heck*, A*ct*.

1. **Phase P*lan* :** dire ce que l'on va faire dans un domaine particulier (qualité, environnement, sécurité, etc.).
2. **Phase D*o* :** faire ce que l'on a dit dans ce domaine.
3. **Phase *Check* :** vérifier qu'il n'y a pas d'écart entre ce que l'on a dit et ce que l'on a fait.
4. **Phase *Act* :** entreprendre des actions correctives pour régler tout écart qui aurait été constaté précédemment.

**Vocabulaire : *Plan, Do, Check, Act* (PDCA)**
Les termes français pour nommer le modèle PDCA pourraient être « Planification », « Action », « Vérification » et « Correction ». Malheureusement, force est de constater que la terminologie française n'est pas du tout utilisée. Aussi parlerons-nous dorénavant du modèle *Plan, Do, Check, Act* ou PDCA.

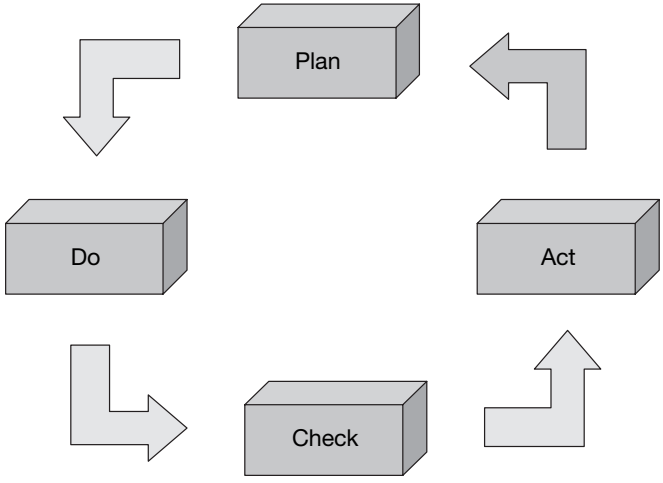


*Figure 1-2 : Le modèle PDCA*

Ce modèle présente deux propriétés principales : il est cyclique et fractal.

- **Caractère cyclique** – C'est ce cycle P*lan*, D*o*, C*heck*, A*ct* qui permet d'atteindre les objectifs (de sécurité, de qualité, d'environnement ou autre) fixés par le management. En revanche, que se passe-t-il une fois que l'objectif a été atteint ? Un nouveau cycle doit être entrepris. C'est pour cela que l'on peut voir une flèche (figure 1-2, en haut à droite) entre la phase A*ct* et la phase P*lan*. Cette flèche grisée permet à l'entreprise non seulement d'atteindre ses objectifs, mais aussi de s'y tenir dans la durée. Un système de management est donc un processus qui tourne indéfiniment. Ce point est trop souvent sous-estimé lors de la mise en place d'un SMSI.
- **Caractère fractal** – Une fractale est une figure géométrique qui garde les mêmes propriétés, quelle que soit l'échelle à laquelle on l'observe. Le principe est le même avec les systèmes de management : quelle que soit l'échelle à laquelle on l'observe, on doit retrouver le modèle P*lan*, D*o*, C*heck*, A*ct*.

**Exemple : SMSI observé à l'échelle globale**
Considérons un système de management de la sécurité de l'information dans son ensemble. La mise en place d'un SMSI nécessite de produire un certain nombre de documents de politique et d'identifier les actions à entreprendre pour se prémunir contre les actes de malveillance. C'est la phase *Plan*. Ensuite, il faut mettre en œuvre les mesures de sécurité

identifiées précédemment. C'est la phase *Do*. L'audit interne permettra de vérifier que ce qui est mis en place est conforme aux politiques et aux procédures. C'est la phase *Check*. Enfin, des actions corrigeront ces écarts. C'est la phase *Act*.

**Exemple : SMSI observé à l'échelle d'un processus**

Changeons à présent d'échelle pour ne considérer que ce qui concerne le cloisonnement des réseaux de niveaux de sensibilité différents (c'est-à-dire les DMZ ou zones démilitarisées). La phase *Plan* implique qu'il faut une politique de flux réseau conduisant à l'élaboration d'une matrice de flux. La phase *Do* consistera à configurer les pare-feux et les routeurs afin de ne laisser passer que les protocoles nécessaires (TCP, UDP, ports, protocoles) entre les différents segments du réseau. La phase *Check* consistera à vérifier périodiquement que les règles des pare-feux et des routeurs correspondent bien à ce qui est spécifié dans la matrice de flux. Enfin, la phase *Act* reviendra à corriger tout écart entre les deux.

Ainsi, non seulement le modèle PDCA s'applique à l'échelle globale du système de management, mais on le retrouve également au niveau de chacun des processus du système.

## Sécurité de l'information

Nous avons parlé jusqu'à présent de la partie SM (système de management) du SMSI. Parlons désormais de la partie SI (sécurité de l'information). La sécurité est au centre de cet ouvrage. Quel sens donnons-nous à ce mot ?

Commençons par préciser qu'il est question ici de *sécurité de l'information* au sens large du terme, c'est-à-dire que nous ne parlons pas seulement de *sécurité informatique*. Nous nous intéressons à l'information sous toutes ses formes, indépendamment de son support : logiciel, matériel, mais aussi humain, papier, savoir-faire, etc. Naturellement, en tant que support privilégié de l'information, l'informatique occupera une part importante, mais réduire le SMSI à son côté strictement informatique serait une erreur.

Sécurité ou sûreté ? On comprend souvent le mot *sécurité* comme la discipline consistant à se protéger contre les actes de malveillance. Pourtant, il n'est pas illégitime de comprendre ce mot comme l'ensemble des moyens déployés pour protéger les personnes contre les accidents. En effet, lorsque nous entrons dans une voiture, nous attachons notre ceinture de sécurité. Cette ceinture ne nous protège pas contre les actes de malveillance, elle nous protège contre les accidents de la route. Dans ce cas, ne serait-il pas plus pertinent de parler plutôt de *sûreté* pour désigner la protection contre les actes de malveillance ? Après tout, nous parlons bien de sûreté de l'État pour se protéger contre l'espionnage ou le terrorisme. Certes, mais *sûreté* est aussi un terme à double sens. Prenons par exemple la sûreté de fonctionnement : il s'agit du mécanisme qui fait que, même lorsqu'un dispositif tombe en panne, il fonctionne toujours (serveurs DNS en *round-robin*, routeurs redondants avec un protocole HSRP, etc.). Alors quel terme faut-il choisir, puisque sûreté et sécurité sont tous les deux polysémiques ?

**Vocabulaire : *safety* et *security***
La situation est un peu plus claire en anglais puisque nous retrouvons les mots *safety* et *security*. Le premier désigne la sécurité physique des personnes alors que le second désigne la protection contre la malveillance.

Pour lever cette équivoque entre sécurité et sûreté, nous choisirons le mot *sécurité* pour désigner tout ce qui peut avoir des conséquences (positives ou négatives) en matière de confidentialité, de disponibilité ou d'intégrité de l'information.

Nous avons vu précédemment que la norme traitant des SMSI est l'ISO 27001. Cette dernière insiste sur les notions de *confidentialité*, d'*intégrité* et de *disponibilité*. Ces termes sont formellement définis dans la norme ISO 13335-1 :

- **Confidentialité :** l'information ne doit pas être divulguée à toute personne, entité ou processus non autorisé. En clair, cela signifie que l'information n'est consultable que par ceux qui ont le droit d'y accéder (on dit aussi « besoin d'en connaître »).
- **Intégrité :** le caractère correct et complet des actifs doit être préservé. En clair, cela signifie que l'information ne peut être modifiée que par ceux qui en ont le droit.
- **Disponibilité :** l'information doit être rendue accessible et utilisable sur demande par une entité autorisée. Cela veut dire que l'information doit être disponible dans des conditions convenues à l'avance (soit 24h/24, soit aux heures ouvrables, etc.).

Le principal objectif d'un SMSI est de faire en sorte de préserver ces trois propriétés (confidentialité, intégrité et disponibilité) pour les informations les plus sensibles de l'entreprise.

**Exemple**

Le SMSI d'une agence de voyages sur Internet pourra avoir pour missions principales :

– La *disponibilité* : en permettant à ses clients d'acheter un voyage à n'importe quelle heure du jour ou de la nuit.

– L'*intégrité* : en fournissant aux clients une information exacte sur les vols et débiter exactement le prix convenu, ni plus, ni moins.

– La *confidentialité* : en protégeant les données personnelles de ses clients (compte bancaire, historique des achats, etc.) contre tout accès illicite.

Les trois notions présentées ci-dessus ne sont pas les seules. On parle aussi de *traçabilité*, d'*authentification*, d'*imputabilité*, de *non-répudiation*, et de bien d'autres mécanismes de sécurité. Le fait que ces principes ne soient pas au centre du SMSI ne signifie pas qu'ils ne soient pas importants. Ils seront déployés en fonction des besoins de sécurité de l'entreprise.

**Exemple**
Pour parvenir à ses objectifs de disponibilité, d'intégrité et de confidentialité, l'agence de voyages déploiera des mécanismes d'authentification par mot de passe utilisateur et certificat serveur, chiffrement des flux, signature, scellement, etc.

## Historique des normes

Depuis 1995, plusieurs normes concernant directement ou indirectement les SMSI ont été publiées. C'est ainsi que l'on a vu apparaître successivement les normes BS 7799, BS 7799-2, ISO 17799, ISO 27001 et ISO 27002. Leurs nomenclatures sont souvent très proches, ce qui génère une certaine confusion. On remarque notamment la présence récurrente des radicaux 7799 et 2700x. Si on ajoute à ceci, que certains de ces standards sont obsolètes, nous comprenons pourquoi souvent, encore aujourd'hui, les idées ne sont pas toujours très claires dans le domaine. Une brève revue historique permettra de clarifier les choses :

- **1995** – La BSI (*British Standards Institution*), qui est l'organisme de normalisation britannique (équivalent de l'AFNOR en France), publie la norme BS 7799. Il s'agit d'un document articulé autour de dix grands chapitres, énumérant les mesures qui peuvent être prises en matière de sécurité de l'information. C'est en fait un catalogue d'une centaine d'entrées. Notons qu'à aucun moment il n'est question de SMSI dans ce document.
- **1998** – La BSI ajoute une seconde partie à cette norme et la nomme BS 7799-2. Le « -2 » ne signifie pas ici « version 2 », mais « deuxième partie ». Cet ajout précise les exigences auxquelles doit répondre un organisme pour mettre en place un SMSI.
- **2000** – La norme BS 7799 de 1995 connaît un tel succès dans le monde que l'ISO l'adopte officiellement sous la référence ISO 17799, en l'enrichissant de quelques mesures de sécurité supplémentaires. On remarque que le radical 7799 a été conservé pour ne pas dérouter les personnes qui s'étaient habituées à la BS 7799. Attention, il ne s'agit que de la première partie de la norme (BS 7799-1), et non de la BS 7799-2. L'ISO 17799 est donc un référentiel qui ne traite pas non plus la question des SMSI.
- **2002** – Parallèlement aux travaux de l'ISO, la BSI poursuit son travail sur la BS 7799-2 et en publie une deuxième version. C'est la BS 7799-2:2002.
- **Juin 2005** – L'ISO sort une nouvelle version de l'ISO 17799, légèrement remaniée et enrichie de nouvelles mesures de sécurité.
- **Octobre 2005** – L'ISO adopte enfin la BS 7799-2 sous la référence ISO 27001:2005. Il s'agit d'une adaptation de la norme britannique, modifiée pour se rapprocher le plus possible de l'ISO 9001 évoquée en début de chapitre. L'ISO 27001 spécifie donc les exigences auxquelles doit répondre un organisme pour mettre en place un SMSI.
- **2007** – Afin de rendre plus cohérentes les nomenclatures entre elles, l'ISO renomme l'ISO 17799 en ISO 27002.

> **Note : BS 7799 ou BS 7799-1 ?**
> Afin d'éviter les confusions, nous utiliserons indifféremment dans cet ouvrage la dénomination de BS 7799 ou BS 7799-1 pour désigner la première partie de la norme BS 7799.

En effet, si sa dénomination officielle est bien BS 7799, il arrivera que nous écrivions BS 7799-1, pour bien faire la différence avec la deuxième partie de cette norme : BS 7799-2.

Le tableau ci-après reprend cet historique.

*Tableau 1-2 : Historique des normes relatives aux SMSI*

| Année | Norme | Traite des SMSI | Remplace la norme |
|---|---|---|---|
| 1995 | BS 7799:1995 | Non | |
| 1998 | BS 7799-2:1998 | Oui | |
| 2000 | ISO 17799:2000 | Non | BS 7799 :1995 |
| 2002 | BS 7799-2:2002 | Oui | BS 7799-2 :1998 |
| 2005 | ISO 17799:2005 | Non | ISO 17799 :2000 |
| 2005 | ISO 27001:2005 | Oui | BS 7799-2 :2002 |
| 2007 | ISO 27002 | Non | ISO 17799 :2005 |

Ce qu'il faut retenir de cet historique est le fait qu'aujourd'hui, nous disposons de deux normes :

- l'**ISO 27001**, qui spécifie des exigences pour les SMSI ;
- l'**ISO 27002**, qui recueille les bonnes pratiques en matière de sécurité de l'information, mais qui ne traite pas des SMSI.

Ces deux normes sont présentées en détail dans les deux chapitres suivants.

**Vocabulaire : SMSI, ISMS, SGSI et SGSSI**

Jusqu'à présent, nous avons cité à plusieurs reprises le sigle SMSI pour désigner les systèmes de management de la sécurité de l'information, mais il en existe d'autres :

**ISMS (*Information Security Management System*)** : c'est le terme anglais pour SMSI. Aussi, tous les documents anglo-saxons utilisent ce sigle. Il est même très fréquent de parler d'ISMS en français.

**SGSI (Système de gestion de la sécurité de l'information)** : ce sigle se retrouve dans certains documents d'origine canadienne. On remarquera que le mot *management* a été traduit par « gestion ».

**SGSSI (Système de gestion de la sécurité des systèmes d'information)** : ce sigle est essentiellement utilisé dans les documents rédigés par la DCSSI (Direction centrale de la sécurité des systèmes d'information), administration dépendant du Premier Ministre, dont une des missions consiste à promouvoir la sécurité des SI.

Tous ces sigles désignent exactement la même chose.

> L'action d'amélioration consiste à faire en sorte que ce soit le service du personnel, seul, qui reçoive l'extrait de casier judiciaire, fournisse le badge à l'employé et fasse le nécessaire pour lui ouvrir un compte sur le réseau. Cela n'augmente pas forcément la conformité du SMSI ou la sécurité du système d'information, mais cela contribue à simplifier le processus.

L'implémenteur doit vérifier que les actions correctives, préventives ou d'amélioration, une fois appliquées, ont bien permis d'atteindre les objectifs fixés. Il informera ensuite toutes les parties concernées du résultat obtenu.

Nous voyons à quel point ces trois types d'actions sont essentielles dans le système de management. Ensemble, elles contribuent effectivement à rendre le SMSI plus fiable et plus efficace dans la durée. Cela renforce indirectement la sécurité du système d'information et, par transitivité, la confiance des parties prenantes.