

A L E X A N D R E F E R N A N D E Z - T O R O

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

© Groupe Eyrolles, 2012, 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

Avant-propos	1
--------------------	---

Partie I – Les systèmes de management de la sécurité de l'information

Chapitre 1 – Les systèmes de management	5
Qu'est-ce qu'un système de management ?	5
Principaux systèmes de management	6
Propriétés des systèmes de management	7
<i>Large spectre de métiers et de compétences</i>	7
<i>Un projet fédérateur et mobilisateur</i>	8
<i>Importance de l'écrit</i>	8
<i>Auditabilité</i>	9
Apports des systèmes de management	9
<i>Premier apport : l'adoption de bonnes pratiques</i>	9
<i>Deuxième apport : l'augmentation de la fiabilité</i>	10
<i>Troisième apport : la confiance</i>	10
Le modèle PDCA	11
Sécurité de l'information	13
Historique des normes	15
Chapitre 2 – La norme ISO 27001	17
Premier constat	17
Objectifs généraux	17
Structure de la norme	19
Phase Plan du SMSI	21
<i>Étape 1 : définir le périmètre et la politique</i>	21
<i>Étape 2 : apprécier les risques</i>	23
1. Identifier les actifs	24
2. Identifier les personnes responsables	25
3. Identifier les vulnérabilités	25

4. Identifier les menaces	25
5. Identifier les impacts	25
6. Évaluer la vraisemblance	26
7. Estimer les niveaux de risque	26
Étape 3 : traiter le risque et identifier le risque résiduel	26
Accepter le risque	27
Éviter le risque	27
Transférer le risque	28
Réduire le risque	28
Identifier les risques résiduels	29
Étape 4 : sélectionner les mesures de sécurité	30
Phase Do du SMSI	32
Plan de traitement des risques	32
Déployer les mesures de sécurité	33
Générer des indicateurs	34
Former et sensibiliser le personnel	34
Formation	35
Sensibilisation	35
Gérer le SMSI au quotidien	36
Détection et réaction rapide aux incidents	36
Phase Check du SMSI	37
Les audits internes	38
Le contrôle interne	39
Les revues	40
La revue de direction	40
Revue ponctuelles	41
Phase Act du SMSI	41
Actions correctives	42
Actions préventives	42
Actions d'amélioration	42
Chapitre 3 – La norme ISO 27002	45
Deux approches de la sécurité	45
Les formalisateurs	45
Les techniciens	46
Une complémentarité nécessaire	47
Présentation de la norme	48
Structure générale	48
Chapitres de l'ISO 27002	50
Chapitre 5 – Politique de sécurité	50
Chapitre 6 – Organisation de la sécurité de l'information	50

Chapitre 7 – Gestion des biens	50
Chapitre 8 – Sécurité liée aux ressources humaines.	51
Chapitre 9 – Sécurité physique et environnementale.	51
Chapitre 10 – Gestion de l'exploitation et des télécommunications	51
Chapitre 11 – Contrôle d'accès	52
Chapitre 12 – Acquisition, développement et maintenance des systèmes d'information.	53
Chapitre 13 – Gestion des incidents liés à la sécurité de l'information	54
Chapitre 14 – Gestion du plan de continuité de l'activité	54
Chapitre 15 – Conformité.	54
<i>Utilisation de la norme</i>	54
Chapitre 4 – Comparaison et usages des deux normes	55
Quelques comparaisons	55
<i>Sur la forme</i>	55
<i>Sur le fond</i>	56
Interaction entre les normes	57
L'ISO 27001 a-t-elle besoin de l'ISO 27002 ?	58
L'ISO 27002 a-t-elle besoin de l'ISO 27001 ?	58
<i>Deux normes complémentaires</i>	59
Usages de l'ISO 27001	59
<i>Adopter de bonnes pratiques</i>	59
<i>Diminuer le coût lié aux audits</i>	61
<i>Fournir la confiance aux clients</i>	63
<i>Autres motivations</i>	63
Usages de l'ISO 27002	65
<i>Tableaux de bord</i>	65
<i>Consolidation de tableaux de bord</i>	66
<i>Consolidation d'audits</i>	67
<i>Politiques de sécurité</i>	68
<i>Exigences de sécurité</i>	69

Partie II – Normes de la série ISO 27000

Chapitre 5 – La série des normes ISO 27000	73
Conseils généraux	73
<i>Comment lire cette partie ?</i>	73
<i>Implémentation et audit de SMSI</i>	73
Principales normes	74

Normes justifiant un chapitre dans cet ouvrage	.74
Normes ne justifiant pas un chapitre	.75
ISO 27000	.75
ISO 27006	.76
Normes sectorielles	.78
Chapitre 6 – ISO 27003 – Implémentation d'un SMSI	.79
Introduction	.79
Structure de la norme	.80
<i>Sur la forme</i>	.80
<i>Obtention de l'approbation du management</i>	.81
<i>Définition du périmètre et de la politique</i>	.81
<i>Analyse des exigences en sécurité de l'information</i>	.81
<i>Appréciation des risques et plan de traitement des risques</i>	.82
<i>Conception du SMSI</i>	.82
<i>Annexes</i>	.84
Points positifs	.84
Points négatifs	.85
Conclusion	.86
Chapitre 7 – ISO 27004 – Indicateurs du SMSI	.87
L'essentiel de la norme	.87
<i>Aspect organisationnel</i>	.87
<i>Aspect méthodologique</i>	.88
<i>Annexes</i>	.91
Conclusion	.91
Chapitre 8 – ISO 27005 – Appréciation des risques	.93
La norme ISO 27005	.93
<i>Pourquoi cette norme ?</i>	.93
<i>Structure de la norme</i>	.94
Début de la norme : notions préliminaires	.94
Chapitre 7 : établissement du contexte	.94
Chapitre 8 : identification et évaluation du risque	.95
Chapitres suivants : traitement, acceptation, communication, surveillance	.97
Les annexes de la norme	.98
<i>Conclusion sur l'ISO 27005</i>	.99

Chapitre 9 – ISO 27007 – Audit des SMSI	101
Introduction	101
Présentation de la norme	102
<i>Structure</i>	102
<i>Spécificités pour les SMSI</i>	102
<i>Annexe</i>	103
Conclusion	104
Chapitre 10 – ISO 27008 – Revue des mesures de sécurité	105
Introduction	105
Présentation de la norme	106
<i>Contexte</i>	106
<i>Généralités</i>	106
<i>Méthodes de revue</i>	107
<i>Déroulement de la revue</i>	108
Préparation	108
Plan	108
Conduite des revues et analyse des résultats	109
<i>Annexes</i>	110
Conclusion	111
<i>Points négatifs</i>	111
<i>Points positifs</i>	111
Chapitre 11 – ISO 27035– Gestion des incidents de sécurité	113
Exemple de gestion d'incident	113
<i>Phase où l'on subit l'incident</i>	114
La déferlante des alertes	114
La réactivité inégale des personnes concernées	115
Les initiatives individuelles désordonnées	115
Questions fondamentales	116
<i>Phase de lutte contre l'incident</i>	117
<i>Phase de retour à la normale</i>	119
<i>En synthèse</i>	120
La norme ISO 27035	120
<i>Généralités</i>	120
<i>Structure de la norme</i>	121
Chapitre introductif	121
Planification	122
Détection et signalement	122

Appréciation de l'incident	123
Phase de réaction	123
Retour d'expérience	125
Annexes	125
<i>Points forts</i>	126
<i>Points à améliorer</i>	126
<i>Conclusion</i>	127

Partie III – Implémenter un SMSI

Chapitre 12 – Le projet de mise en place du SMSI	131
Nature du projet	131
Chef de projet	132
Projet de mise en place du SMSI	133
<i>Approche séquentielle</i>	133
<i>Approche projet</i>	135
Contraintes	135
Phase 1 : Analyse préalable	135
Phase 2 : Mise en place de la structure de base	137
Phase 3 : Mise en place des processus du SMSI	138
Phase 4 : Démarrage du SMSI	139
Dépendances	140
<i>Principales erreurs à éviter</i>	141
<i>Coût et suivi du projet</i>	143
Éléments du projet de SMSI	145
Chapitre 13. Politique et périmètre du SMSI	147
La pierre angulaire du SMSI	147
Le périmètre	148
<i>Contraintes normatives sur le périmètre</i>	148
<i>Exemple de périmètre</i>	149
<i>Différentes stratégies</i>	150
Périmètre orienté entreprise	150
Périmètre orienté site	151
Périmètre orienté service	152
Alignement avec d'autres systèmes de management	152
Stratégie progressive	153
La politique	154
<i>Deux types de politiques</i>	154

<i>Contraintes normatives sur la politique du SMSI</i>	155
<i>Exemple de politique du SMSI</i>	156
Sur la forme	157
Éléments du sous-projet de politique et de périmètre	157
Chapitre 14 – Gouvernance de la sécurité	159
Besoin de gouvernance	159
Modèles de gouvernance	160
<i>Modèle empirique</i>	160
<i>Modèle Cobit</i>	161
<i>Le processus DS5 de Cobit</i>	163
Exigences de la norme en matière de gouvernance	164
Intégrer la sécurité dans la gouvernance de l'entreprise	165
<i>Instances les plus communes dans l'entreprise</i>	166
<i>Erreurs à éviter</i>	167
<i>Exemple</i>	167
<i>Formalisation de la gouvernance</i>	170
Éléments du sous-projet de gouvernance	171
Chapitre 15 – Documentation	173
Exigence normative	173
Documents exigés	176
<i>Documents explicitement exigés</i>	176
<i>Documents implicitement nécessaires</i>	177
Recommandations générales	177
<i>Erreurs les plus courantes</i>	178
<i>Recommandations</i>	180
Rubriques	180
Partir des faits	183
Rédiger en style laconique	184
Approche projet	184
Éléments du sous-projet de documentation	185
Chapitre 16 – Audit interne et suivi des actions	187
Audit interne	187
<i>Exigence normative</i>	187
<i>L'état d'esprit de l'audit interne</i>	188
<i>Programmation des audits internes</i>	189
<i>Déroulement des audits internes</i>	191

Comment mettre en place l'audit interne ?	193
<i>Dans une PME</i>	193
Le « tout en interne »	193
Stratégie d'externalisation	194
Stratégie hybride	194
<i>Dans les grandes structures sans audit interne</i>	194
Créer une structure indépendante	194
Rattachement à une structure existante	194
<i>Dans les grandes structures avec audit interne</i>	195
<i>Guide d'audit</i>	196
Suivi des actions	197
Éléments du sous-projet d'audit et de suivi d'actions	199
Chapitre 17 – Appréciation des risques	201
Processus de gestion du risque	201
Différentes méthodes	202
Différentes approches	203
<i>Une appréciation des risques existe déjà</i>	203
<i>Démarche « canonique »</i>	204
<i>Démarche « pragmatique »</i>	204
Difficultés courantes de l'appréciation des risques	207
<i>Commencer l'appréciation</i>	207
<i>Inventaire des actifs</i>	208
Se servir autant que possible de l'existant	208
Différents niveaux d'actifs	209
Nombre d'actifs	209
Granularités variables	210
Identifier les actifs sensibles	210
<i>Valoriser les actifs</i>	211
<i>Estimer le risque</i>	212
<i>Mesures de sécurité</i>	213
<i>Établir des niveaux de risque</i>	214
<i>Définir les risques acceptables</i>	216
Étude de cas d'appréciation de risques	217
<i>Oubli d'un risque</i>	218
Éléments du sous-projet de gestion des risques	219
Chapitre 18 – Sélection des mesures de sécurité	221
Importance de la déclaration d'applicabilité (SoA)	221

Quelles mesures sélectionner ?	222
<i>Mesures obligatoires par transitivité</i>	223
<i>Mesures obligatoires par le contexte</i>	224
<i>Groupes cohérents de mesures</i>	225
Méthodologie : modèle PDCA et cohérence	225
<i>Conformité au modèle PDCA</i>	225
<i>Cohérence générale</i>	226
Éléments du sous-projet SoA	226
Chapitre 19 – Formation et sensibilisation	229
Exigence normative	229
La formation	230
<i>Points importants</i>	230
<i>Besoins en formation</i>	230
Pendant la construction du SMSI	231
Pendant l'exploitation du SMSI	232
La sensibilisation	233
<i>Différentes formes de sensibilisation</i>	233
<i>Questions abordées</i>	235
<i>Exemple de programme de sensibilisation</i>	236
<i>Points importants</i>	237
Éléments du sous-projet formation	237
Éléments du sous-projet de sensibilisation	239
Chapitre 20 – Indicateurs du SMSI	241
Exigence de la norme	241
Comment choisir les indicateurs pour un SMSI ?	242
<i>Questions fondamentales</i>	242
<i>Principales erreurs à éviter</i>	243
<i>Différents types d'indicateurs</i>	245
Principaux indicateurs à mettre en place dans un SMSI	246
<i>Critères pour choisir les indicateurs</i>	246
<i>Exemples d'indicateurs</i>	248
Éléments du sous-projet indicateurs	250

Partie IV – Audit des SMSI

Chapitre 21 – Le principe de la certification	255
La certification	255
<i>Obtenir le certificat ISO 27001</i>	255
Audit initial	255
Audit complémentaire	256
<i>Conserver le certificat</i>	257
Audit de surveillance	257
Audit de renouvellement	259
Les organismes de certification	259
<i>Cadre réglementaire</i>	259
Réglementation	260
Contrôle	261
<i>Relations contractuelles avec l'audité</i>	264
Chapitre 22 – Les audits	267
Principes de base	267
<i>Deux façons de considérer les audits</i>	267
<i>Principes de l'audit</i>	268
<i>Différents types d'audits</i>	269
Audits de base	269
Audits particuliers	270
Programme d'audits	270
Déroulement d'un audit	272
1. <i>Premier contact</i>	272
2. <i>Revue de documentation</i>	273
3. <i>Plan d'audit</i>	273
4. <i>Réunion d'ouverture</i>	276
5. <i>Activités d'audit</i>	276
6. <i>Réunion de clôture</i>	277
7. <i>Après l'audit</i>	277
Le rapport d'audit	277
Validation	279
La notion de non-conformité	279
<i>Différents types de non-conformités</i>	279
<i>Critères de qualification</i>	280
<i>Séquence de gestion d'une non-conformité</i>	281
<i>Procédure de contestation</i>	285

Chapitre 23 – Se préparer à l’audit de certification	287
Avant l’audit de certification	287
<i>Audit à blanc</i>	287
<i>Informier</i>	288
<i>Préparer les documents</i>	290
Critères d’audit	290
Documentation de base	290
Manuel sécurité	291
Cahier de l’audité	292
<i>Prévoir les questions d’intendance</i>	293
Pendant l’audit	295
<i>Revue de documentation</i>	295
<i>Réunion d’ouverture</i>	296
<i>Activités d’audit</i>	296
Obtention de l’information	296
Recoupements et mise en perspective	297
Débriefing du soir	297
<i>Réunion de clôture</i>	298
Après l’audit	299
Quelques conseils	300
<i>Facteurs anxioènes pour l’audité</i>	300
<i>Éléments susceptibles d’indisposer l’auditeur</i>	301
<i>Erreurs à éviter</i>	302
<i>Points sur lesquels il faut rester ferme</i>	303
Chapitre 24 – La vraie valeur de la certification	305
Quelle est la valeur réelle de la certification ?	305
<i>Absurdité de la question</i>	306
<i>Pertinence de la question</i>	306
Les différents profils de certifications	306
<i>Cas n° 1 : les sociétés cherchant la conformité avant tout</i>	307
<i>Cas n° 2 : les sociétés maîtrisant déjà la sécurité</i>	307
<i>Cas n° 3 : les sociétés découvrant la sécurité avec l’ISO 27001</i>	307
Les questions à se poser	308
<i>Le périmètre de la certification</i>	308
Périmètre flou	308
Périmètre inadéquat	309
Périmètre trop restreint	309
Périmètre trop ambitieux	310

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.

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.

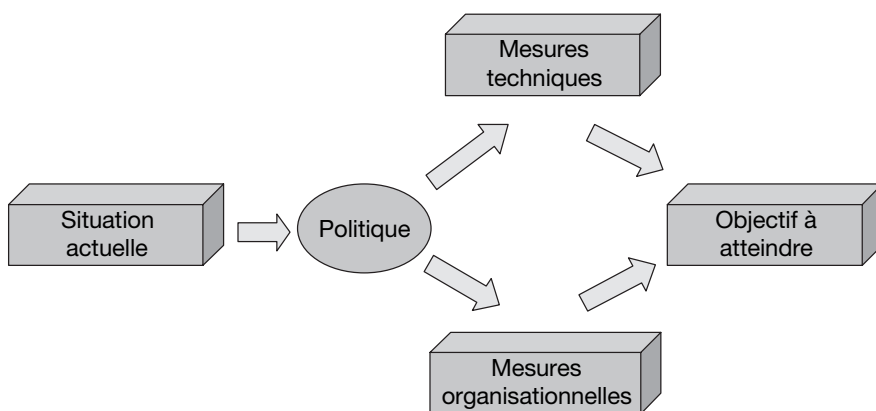


Figure 1-1 : Vision empirique d'un système de management

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 *Plan*, *Do*, *Check*, *Act*.

- 1. Phase Plan** : dire ce que l'on va faire dans un domaine particulier (qualité, environnement, sécurité, etc.).
- 2. Phase Do** : 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.

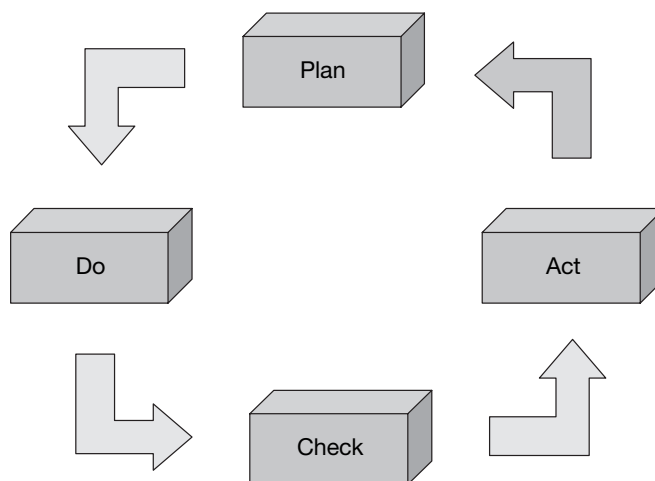


Figure 1-2 : Le modèle PDCA

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

- **Caractère cyclique** – C'est ce cycle *Plan, Do, Check, Act* 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 *Act* et la phase *Plan*. 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 *Plan, Do, Check, Act*.

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.

<i>La politique du SMSI</i>	310
<i>Les signes positifs</i>	311
Un SMSI mature	311
La présence d'autres systèmes de management dans l'entreprise ...	311
Comment distinguer les SMSI des cas n° 1 et des cas n° 2 ?	312
<i>Reconnaître les cas n° 1</i>	312
La documentation	312
La cohérence	312
Les non-conformités	312
Les audit complémentaires	313
<i>Distinguer les cas n° 2</i>	313
La documentation	313
L'absence de non-conformités	313
L'absence d'audits complémentaires	313
<i>La difficulté de vérifier</i>	313
Conclusion	314
 Index	 315