

Livre Blanc

ISO 27000

Le nouveau nirvana de la sécurité ?



Plan



Do



Check



Act



gouvernance & technologies

Livre blanc rédigé par Gérôme Billois et Tristan Savalle, Consultants Seniors et Lead Auditors ISO 27001, sous le pilotage de Laurent Bellefin, Directeur des Opérations Sécurité de Solucom.

Copyright Solucom - Tous droits réservés
ISBN : 2-9525584-2-6

Tous droits réservés. Ce document ne peut être reproduit et/ou diffusé en tout ou partie sans l'autorisation de Solucom.

Les informations contenues dans ce document sont susceptibles d'être modifiées sans préavis par Solucom. Elles sont données uniquement à titre indicatif, et Solucom ne saurait être tenu pour responsable de l'usage qui en sera fait.

Les marques et noms déposés qui sont cités dans ce document appartiennent à leurs propriétaires respectifs.



Cabinet de conseil en gouvernance et technologies, le groupe Solucom rassemble plus de 500 consultants. Dans le domaine de la sécurité, Solucom accompagne les grandes entreprises dans la mise en place de leur politique de maîtrise des risques SI et dans le design de leurs architectures de sécurité. Notre équipe Sécurité, forte de 120 consultants, est ainsi amenée à :

- cartographier les risques encourus par le SI et conduire des audits,
- formaliser les politiques et les organisations de management de la sécurité,
- élaborer des plans de continuité d'activité,
- concevoir et optimiser les processus et les solutions de gestion des identités et des habilitations.

www.solucom.fr

« L'ISO 27000, nouveau nirvana de la sécurité ? »



Laurent Bellefin

Directeur des Opérations Sécurité
laurent.bellefin@solucom.fr

La sécurité de l'information est plus que jamais sur le devant de la scène. Les systèmes d'information prennent une place toujours plus essentielle dans les processus métiers des entreprises et des administrations. Parallèlement, les menaces et la pression réglementaire ne cessent de s'accroître. La sécurité de l'information est donc maintenant devenue l'un des piliers incontournables de toute bonne gouvernance des SI.

Pourtant les démarches actuelles restent souvent parcellaires et artisanales. Les standards BS 7799, relayés par la suite par la norme ISO 17799, ont bien tenté de formaliser les meilleures pratiques dans le domaine. Mais l'ISO 17799, si elle donne une « check-list » des mesures de sécurité qu'il faut couvrir, ne permet pas de les sélectionner en fonction d'un contexte donné ou de dimensionner l'effort à consentir.

Avec la publication progressive des normes de la famille ISO 27000, et plus particulièrement de son pilier fondateur l'ISO 27001, une étape majeure a été franchie.

L'ISO 27001 crée pour les RSSI l'opportunité de mettre en œuvre un véritable système de management de la sécurité de l'information efficace et s'auto-améliorant avec le temps. Elle est appelée à devenir une référence internationale reconnue, utilisée par tous les auditeurs SI. Elle sera très probablement incontournable dans certains secteurs d'activité, à l'instar de ce qu'a pu être la norme ISO 9000 dans le domaine de la qualité, en s'imposant comme une « garantie de confiance » pour les clients et partenaires d'une entreprise ou d'une institution.

Chaque entreprise va donc devoir, à court ou moyen terme, se positionner sur l'usage qu'elle souhaite faire de cette norme.

Pour alimenter ces réflexions, Solucom publie ce livre blanc consacré à la famille ISO 27000. S'appuyant sur nos premiers retours d'expérience, et sur l'analyse de nos consultants certifiés Lead Auditors ISO 27001, il donne notre propre lecture des normes ISO 27000, en clarifie les principes et les apports mais aussi les limites.

J'espère que ce livre blanc contribuera efficacement à vos réflexions et à vos projets.

ISO 27000, une famille nombreuse...

Fruits de plusieurs années de réflexion au niveau international, les normes ISO 27000 apportent une aide indéniable dans la définition, la construction et la déclinaison d'un système de management de la sécurité de l'information efficace.

Une nouvelle famille de normes

Issue des réflexions de groupes de travail internationaux dédiés au domaine de la sécurité de l'information, la famille des normes ISO 27000 est progressivement publiée depuis 2005.

Nous pouvons distinguer trois types de normes dans cette grande famille.

Des normes certifiantes

Elles décrivent les exigences devant être respectées si l'on souhaite viser la certification et ainsi obtenir une reconnaissance externe.

L'ISO 27001, norme de définition et de mise en place du Système de Management de la Sécurité de l'Information (SMSI), publiée en 2005, est le pilier du système. Elle s'inspire largement des travaux de l'organisme de normalisation British Standard et de sa norme BS 7799-2 qui était déjà « certifiante » et largement diffusée au Royaume-Uni et en Asie.

L'ISO 27006, qui définit les exigences s'appliquant aux organismes accrédités pour prononcer eux-mêmes la certification, entre aussi dans cette catégorie.

Des normes de recommandations

Ces normes proposent des bonnes pratiques à suivre pour définir le système de management et sélectionner les mesures de sécurité.

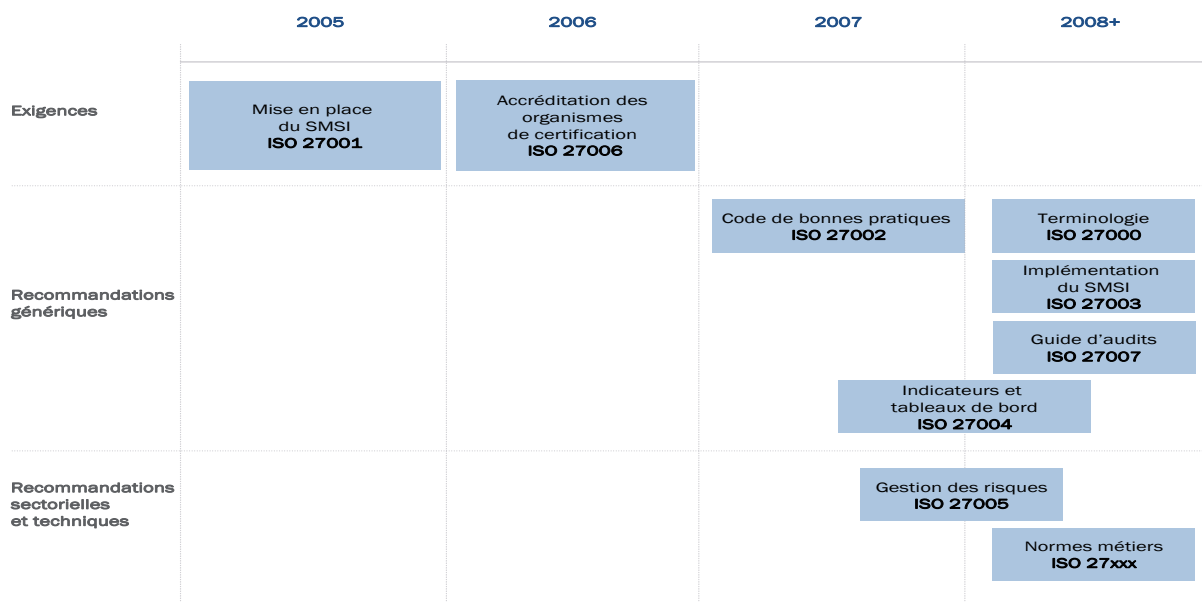
La plus connue est la norme ISO 27002 (ancienne ISO 17799) qui décrit les mesures de sécurité en 39 objectifs et 133 mesures.

Les normes ISO 27003 (guide de mise en œuvre), ISO 27004 (mesure de l'efficacité) et ISO 27005 (analyse de risques) actuellement en phase de conception apporteront des conseils sur la mise en œuvre du SMSI.

Des normes sectorielles et techniques

L'ISO prépare aussi des « SMSI sectoriels » en sélectionnant et en adaptant les contrôles devant être mis en œuvre pour certains types d'organismes. Un des secteurs les plus avancés est celui des télécommunications avec le projet de norme ISO 27011. La santé n'est pas en reste avec le projet de norme ISO 27799.

La liste des normes ISO 27000 est loin d'être stabilisée, et les réflexions se poursuivent sur des thèmes comme la sécurité des réseaux ou la continuité d'activité par exemple (cf. annexe).



ISO 27001 : les clefs du SMSI

La norme ISO 27001 pose les bases du système de management de la sécurité de l'information. Adoptant une approche par processus, la norme met en lumière les meilleures pratiques de sécurité et surtout les organise dans le temps.

Le système de management de la sécurité de l'information

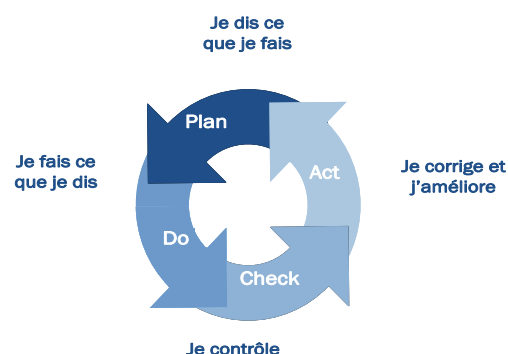
Clef de voûte de l'initiative 27000, la norme ISO 27001 décrit les exigences nécessaires à la mise en œuvre du Système de Management de la Sécurité de l'Information (SMSI).

Le SMSI est défini par l'ensemble des ressources mises en place pour organiser et gérer au quotidien la sécurité de l'information. Plus concrètement, il englobe l'ensemble des documents définissant les règles et processus de sécurité, l'organisation associée (RSSI, correspondants sécurité, exploitants, instances de décision...) ainsi que les infrastructures techniques de sécurité.

Le SMSI constitue donc un dispositif global de gouvernance de la sécurité de l'information. Il est important de noter qu'il est toujours défini pour un périmètre bien déterminé : toute l'entreprise, un métier ou un processus particulier, une application, un centre de production...

Des principes issus de la qualité

Comme les systèmes de management de la qualité (ISO 9000) et de l'environnement (ISO 14000), un SMSI ISO 27001 repose sur le cycle de progrès PDCA : Plan, Do, Check, Act, également appelé Roue de Deming.



Ce cycle vise une amélioration continue reposant sur une logique simple : dire ce que l'on fait, faire ce que l'on a dit, puis contrôler et corriger ce qui ne va pas.

Le SMSI va également s'appuyer sur d'autres principes issus des normes ISO 9000 :

- Un engagement concret du management : le management joue un rôle prépondérant et explicite dans la validation et le fonctionnement du SMSI.
- Une approche par processus : la norme préconise en effet que toutes les activités liées au SMSI soient conçues et formalisées sous la forme de processus. Les porteurs et acteurs des différentes actions contribuant à la sécurité doivent donc être identifiés tout comme l'enchaînement des actions à mener pour chaque processus de sécurité.

Tout le cycle de vie du SMSI (PDCA) doit lui-même être vu comme un processus englobant l'ensemble du dispositif. La norme ISO 27001 décrit grâce à ce processus les différentes étapes de la mise en place et du fonctionnement de la gouvernance de la sécurité de l'information.

Plusieurs niveaux d'exigence

Le corps de la norme ISO 27001 est consacré à la création et au maintien du SMSI. Si certains sujets sont mis fortement en avant comme la formation et la sensibilisation, l'organisation, la gestion des ressources, la gestion des incidents ou les plans d'audits, toutes les mesures de sécurité évoquées dans l'ISO 27002 ne sont pas traitées en détail.

Cela étant, la norme ISO 27001 propose dans son annexe A une liste des 133 mesures de l'ISO 27002 organisées selon les 39 objectifs de la même norme. Cette annexe sera utilisée pour élaborer le plan de traitement des risques (cf. ci-après) et ainsi déterminer les chantiers nécessaires pour garantir l'atteinte du niveau de sécurité souhaité.

1 - PLAN : CONCEVOIR LE SMSI

La phase PLAN consiste à poser les bases du SMSI qui vont encadrer l'exécution des phases avales.

- Définition du périmètre du SMSI : par exemple un site, un processus, une direction ou toute l'entreprise.
- Définition de la politique du SMSI regroupant les objectifs de sécurité, les principales contraintes légales, réglementaires et contractuelles que rencontre l'organisation, les liens avec la gestion des risques de l'entreprise (si elle existe), les critères d'acceptation des risques. Cette politique concrétise également l'implication de la direction de l'entreprise et doit donc être validée par elle.
- Élaboration ou sélection d'une méthodologie d'analyse des risques de sécurité de l'information
- Conduite d'une analyse de risques complète sur le périmètre, afin de comprendre les enjeux métiers à prendre en compte et les risques présents dus à l'existant. L'analyse de risques se termine par l'identification des mesures de sécurité macroscopiques à mettre en œuvre (plan d'actions) et par l'acceptation par le management des risques résiduels. Le management peut bien sûr aussi décider de transférer certains risques à des tiers par exemple à travers des assurances.
- Rédaction de la déclaration d'applicabilité (Statement of Applicability – SoA). Ce document, nécessaire uniquement pour la certification, permet de préciser les mesures de sécurité qui seront implémentées ou rejetées en fonction des objectifs recherchés. Les mesures sont reprises de l'ISO 27002, mais il est possible d'en rajouter ou de les adapter au besoin. Le fait d'écarter une mesure de sécurité doit être justifié dans cette déclaration.

2 - DO : IMPLÉMENTER ET OPÉRER LE SMSI

La phase DO consiste à mettre en place les mesures que l'analyse de risques a identifiées comme nécessaires.

La mise en place des mesures peut prendre de nombreuses formes :

- Le lancement de projets concrets : par exemple la mise en place d'un Plan de Continuité d'Activité ou la mise en œuvre d'un système de gestion des habilitations des tiers, accompagnées des documents adéquats : procédures, dossiers techniques...
- La mise en conformité des mesures déjà existantes : documentation, contrôle...

Cette phase s'appuie fortement sur le plan de traitement des risques, c'est-à-dire le plan d'actions détaillé issu de l'analyse de risques. Il identifie les porteurs de chaque action, les budgets, les plannings, les priorités, etc.

Certaines mesures sont rendues directement nécessaires par la norme, comme la préparation des contrôles d'efficacité du SMSI (indicateurs, tableaux de bord...), la sensibilisation/formation des utilisateurs, les procédures de gestion du SMSI (gestion de la documentation, gestion des ressources du SMSI, détection des événements et gestion des incidents de sécurité...).

4 - ACT : AMÉLIORER LE SMSI

La phase ACT, consiste à prendre en compte les écarts et problèmes observés pendant la phase CHECK et à proposer les actions nécessaires pour les corriger (actions correctrices) et anticiper des problèmes futurs (actions préventives).

Cette phase permet également de terminer le cycle de Deming en préparant le cycle suivant.

La norme insiste sur l'élaboration d'un plan d'actions correctrices, destiné à corriger des dysfonctionnements avérés du SMSI. Ces dysfonctionnements peuvent être liés :

- Aux imperfections du SMSI lui-même, par exemple l'absence de certaines preuves ou des écarts entre les contrôles demandés et les contrôles réalisés ou la mise à jour de procédures non pertinentes.
- A l'inefficacité des mesures de sécurité permettant la protection du patrimoine de l'entreprise, par exemple des dispositifs de sécurité qui n'auraient pas fonctionné (attaques...) ou qui ne prendraient pas en compte de nouvelles menaces.

Dans le cadre du modèle d'amélioration continue PDCA, il s'agit également de proposer un plan d'actions préventives qui a pour objectif d'empêcher des dysfonctionnements futurs (mise en place de contrôles supplémentaires par exemple).



3 - CHECK : CONTRÔLER LE SMSI

La phase CHECK consiste à vérifier le fonctionnement du SMSI en détectant les éléments de non-conformité ou de faiblesse du SMSI et en préconisant des améliorations quand cela est pertinent.

Ces vérifications se font à travers :

- Des plans de contrôles internes ;
- L'analyse des résultats des audits ponctuels ;
- L'analyse des résultats des procédures de remontée d'incidents et de problèmes ;
- La publication d'indicateurs d'efficacité et de suivi du SMSI.

La phase CHECK inclut systématiquement une revue managériale du SMSI permettant ainsi de resituer le SMSI par rapport aux objectifs et aux enjeux et contraintes (légales, contractuelles...) de l'entreprise et si nécessaire, de demander la mise à jour de l'analyse de risques et du plan de traitement des risques.

La pertinence de cette phase dépend de la qualité des preuves (ou enregistrements) conservées lors du déroulement des différents processus du SMSI. La gestion de ces enregistrements est donc un pan important du SMSI, tant sur la production des preuves (comptes-rendus de réunion, rapport d'audits, PV de contrôles, listes de vérification, journaux...) que sur la conservation et la restitution de ces preuves.

UNE NORME QUI INSISTE « LÀ OÙ LE BÂT BLESSE »

Sans avoir attendu la norme ISO 27001, les grandes entreprises ou administrations ont déjà posé les bases de leur gouvernance de la sécurité. Pour autant, certains aspects essentiels soulignés à juste titre par la norme restent encore très peu implémentés.

S'aligner sur les risques

La majorité des politiques de sécurité formalisées dans le passé énonce déjà le principe d'une démarche sécurité alignée avec les risques encourus par l'entreprise. Pourtant, rares sont encore les cas où le RSSI dispose d'une vraie « cartographie des risques » globale et d'un plan d'actions justifié par ces risques.

Souvent, les mesures de sécurité sont décidées et mises en œuvre directement par les équipes de la DSI ou sont choisies en fonction de « l'état de l'art » sans forcément sélectionner de manière objective les mesures réellement les plus pertinentes. Les analyses de risques, quand elles existent, sont limitées tant en périmètre (un projet, une infrastructure sensible), qu'en terme de pertinence (faible implication des métiers).

L'ISO 27001 rend nécessaire la conduite d'une analyse de risques dès la phase PLAN. La méthodologie d'analyse n'est pas imposée mais doit être définie au préalable et répondre à certaines contraintes : identification des processus et actifs critiques, identification des propriétaires, analyse des impacts, identification des menaces et des vulnérabilités, puis description et pondération des risques.

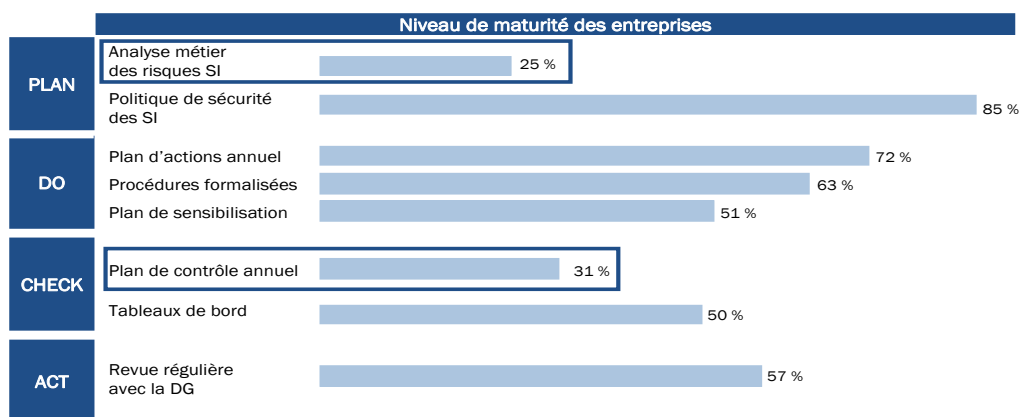
« La norme ISO 27001 impose la conduite d'une analyse de risques puis la définition d'un plan de traitement de ces risques dont l'application est strictement contrôlée. »

Adopter une démarche qualité

Les politiques actuelles intègrent aussi très souvent des règles concernant la formalisation des procédures de sécurité, la réalisation de contrôles ou l'enregistrement des journaux. Mais elles ne décrivent pas précisément les processus et moyens qui vont permettre de réaliser effectivement ces actions.

La norme ISO 27001 propose en revanche d'intégrer ces éléments comme des fondements incontournables de la démarche sécurité :

- 1) Des processus de sécurité bien identifiés et formalisés (analyse de risques, gestion des incidents, sensibilisation, contrôles...).
- 2) Le contrôle systématique des éléments mis en œuvre via le SMSI.
- 3) La gestion efficace de la documentation (création et mises à jour).
- 4) La gestion stricte des enregistrements pour permettre le contrôle des mesures de sécurité mises en place (par exemple : traces de tous les accès à un local sécurisé). Notons que cet élément s'avère de plus en plus incontournable du fait des nouvelles réglementations légales (Sarbanes-Oxley Act, LSF) ou sectorielles (Bâle II ou MiFID dans le milieu bancaire, Solvency II...).



Source : Solucom / Panel de 50 grandes entreprises ou administrations - Septembre 2007

POURQUOI ET COMMENT ADOPTER L'ISO 27001 ?

Par rapport aux démarches actuelles de sécurité, la norme ISO 27001 a des apports indéniables. Comment valoriser ces apports ? Et jusqu'où aller dans son application ?

Pourquoi adopter l'ISO 27001 ?

L'ISO 27001 propose des principes pertinents qui amènent un plus réel aux démarches d'amélioration de la sécurité. Elle apporte en effet :

- Une meilleure maîtrise des risques qui pèsent réellement sur les activités de l'entreprise.
- La garantie de mieux dimensionner le budget sécurité et surtout de l'affecter aux mesures les plus pertinentes.
- Une association plus systématique des acteurs métiers et du management aux décisions, et donc une meilleure acceptation des contraintes amenées par les mesures de sécurité.
- Un pilotage plus efficace du traitement des risques.
- La facilitation d'autres démarches liées à la sécurité de l'information, comme par exemple la mise en conformité à Bâle II, à Sarbanes-Oxley ou aux lois informatique et libertés.
- La garantie de mieux répondre aux attentes des « auditeurs » qui vont maintenant utiliser cette norme comme référence.

L'utilisation de l'ISO 27001 va par ailleurs renforcer la confiance du management dans la démarche entreprise par le RSSI et sa crédibilité. Elle offrira au RSSI un support plus efficace pour obtenir les moyens dont il a besoin pour mener ses actions.

« Les apports de la norme ISO 27001 par rapport aux pratiques actuelles la rendent incontournable pour toute bonne gouvernance du SI. »

Plusieurs approches face aux normes

La norme ISO 27001 peut, comme tout guide, être utilisée comme un recueil de bonnes idées dans lequel on peut piocher. Mais elle ne donnera sa pleine efficacité que si les principes fondateurs qu'elle propose sont effectivement mis en œuvre.

La question qui se pose alors, est de savoir jusqu'où aller dans la mise en œuvre de ces principes, avec deux grandes options possibles :

1. Construire un ou plusieurs SMSI avec une véritable démarche de progrès PDCA, mais sans chercher la certification à court terme.
2. Chercher à obtenir rapidement une certification officielle et tirer ainsi parti au maximum de ce que la norme peut apporter. Dans ce cas, comme nous le verrons plus loin, mieux vaut se fixer un périmètre raisonnable au départ.

En tout état de cause, le projet d'adoption de l'ISO 27001 devra trouver sa place au cœur de la gouvernance SI de l'entreprise. Il peut être porté par le RSSI, avec l'aide des équipes Qualité et des Risk Managers, mais doit être sponsorisé par la Direction. Il associera systématiquement les métiers liés au périmètre concerné et bien entendu les acteurs de la DSI, qui sont concernés au premier chef.

Le chapitre suivant de ce livre blanc, « Mettre en œuvre le SMSI », explique comment passer d'une gouvernance de sécurité « classique » à un ou plusieurs véritable(s) SMSI fonctionnel(s).

Le chapitre « La certification ISO 27001 » aborde la problématique de la certification de ce(s) SMSI fonctionnel(s), en cherchant à isoler les étapes supplémentaires qu'il faudra franchir pour pouvoir non seulement prétendre à être certifié, mais surtout le rester.

Mettre en œuvre un SMSI

La norme ISO 27001 arrive alors que les entreprises et les administrations ont déjà pour la plupart mis en place des premiers éléments de gouvernance de la sécurité et ont engagé de nombreux chantiers d'amélioration. La décision d'appliquer les principes de l'ISO 27001 remet-elle en cause tout l'existant ? Comment entamer ce projet ISO 27001 ?

Donner rapidement...

Si l'on prend l'ISO 27001 au pied de la lettre, la première étape à mener est l'analyse de risques.

Pour conduire cette action, le choix du « niveau de granularité » est lourd de conséquences. Identifier tous les risques en analysant chaque micro processus de l'entreprise est une tâche de longue haleine. Se placer à un niveau très macroscopique permet d'aller beaucoup plus vite, mais donne des résultats beaucoup moins précis.

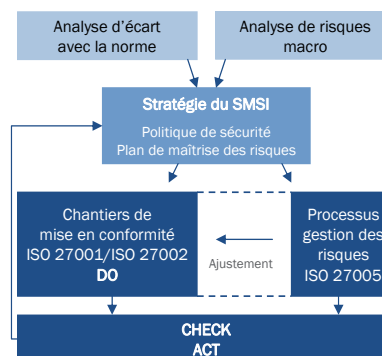
Pour traiter ce dilemme et lancer la « boucle PDCA » dans un délai raisonnable, nous préconisons de mener en parallèle :

- L'identification macroscopique des besoins de sécurité, réalisée sur la base d'interviews des principaux responsables métiers et de la Direction Générale.
- Une analyse des écarts entre les pratiques existantes et les principes et règles de la norme (i.e. les chapitres 4 à 8 de l'ISO 27001 et les 133 mesures de sécurité de l'ISO 27002), réalisée sur la base d'interviews du RSSI et des responsables SI (exploitants, architectes, chefs de projets...), d'une revue documentaire et de visites de sites.

... une impulsion décisive

Ce travail initial permet d'identifier les grandes familles de risques et les périmètres du SI sur lesquels les enjeux sont les plus forts. Il permet aussi de détecter les éléments manquants pour disposer d'un SMSI opérationnel et efficient. Le travail ainsi mené permet de définir et de faire valider la « stratégie du SMSI » par la Direction Générale. La stratégie du SMSI consiste à :

- 1) Fixer le périmètre du SMSI.
- 2) Formaliser une politique de sécurité de l'information et une organisation adéquate.
- 3) Définir un plan de maîtrise des risques argumenté identifiant les chantiers prioritaires.



Le plan de maîtrise des risques comporte plusieurs volets :

- Des chantiers de conformité ISO 27001 pour décliner les exigences de la norme (cf. chapitre précédent). Une approche par processus de sécurité sera évidemment très pertinente (gestion des incidents, contrôle...).
- Des chantiers « ISO 27002 » comme par exemple le Plan de Continuité d'Activité, la gestion des identités et des accès (IAM), la gestion contractuelle des tiers...

Phase 1 :
Pour démarrer, il faut « raisonner macro », autant pour l'analyse de risque que pour mesurer les écarts entre l'existant et la norme

Phase 2 :
Mettre en place un processus de gestion des risques permanent

Le processus de gestion des risques, défini par l'ISO 27005, est l'un des processus clés à mettre en place dans le cadre de ce plan de maîtrise des risques. Ce processus permet de préciser et de mettre à jour progressivement la « cartographie des risques » globale. Il permet

aussi d'ajuster les contours et les priorités des chantiers de mise en conformité et de réorienter le SMSI dans la bonne direction si nécessaire. Le processus de gestion des risques prévoira dans la plupart des cas une alimentation régulière de la cartographie des risques sur la base :

- Des analyses de risques réalisées pour chaque projet SI.
- D'un travail progressif d'analyse détaillée des risques pour chaque processus métier.

L'analyse de risques, point focal de la démarche

L'analyse de risques constitue le point de départ d'une démarche ISO 27001. Pour autant, il s'agit d'un exercice complexe et sensible nécessitant un vrai appui de la direction ainsi qu'une méthodologie et un plan de communication bien élaborés. Les difficultés à anticiper incluent :

- La définition des critères d'acceptation des risques (à partir de quel niveau l'entreprise ne peut accepter un risque).
- La définition d'une grille d'impacts, nécessaire pour avoir des résultats homogènes. Cette grille doit être indiscutable : il est toujours difficile de faire admettre à un responsable que le processus dont il a la charge n'est pas le plus critique...
- Les enjeux liés aux périmètres croisés lorsqu'un risque ne concerne pas qu'une seule équipe ou un seul processus métier.
- La norme ne donne par ailleurs aucun guide, ni pour le choix du niveau de granularité à adopter, ni pour la définition et la valorisation des types d'impacts. Seuls le bon sens et l'expertise peuvent permettre de faire des choix pertinents dans ce domaine.

L'ISO 27005 : GESTION DES RISQUES

La norme ISO 27005 est un guide de mise en œuvre du processus de gestion des risques liés à la sécurité de l'information. Elle propose une méthodologie d'appréciation et de traitement des risques et complète ainsi les principes de la norme ISO 27001 qui établit le SMSI en s'appuyant sur l'analyse des risques.

La norme ISO 27005 s'inscrit dans la logique vertueuse du cycle PDCA initiée par la norme ISO 27001 tant par son objectif d'amélioration de la sécurité que par le cycle de vie de la gestion des risques qu'elle propose de mettre en place.

Au-delà des apports méthodologiques qu'elle représente pour la gestion des risques, elle est enrichie d'annexes qui forment un outillage conséquent pour leur appréciation et leur analyse.

Pour autant, l'ISO 27005 ne constitue probablement pas aujourd'hui une base de scénarios de risques suffisamment exhaustive pour être utilisée. L'aide d'une véritable méthodologie d'analyse de risques (comme EBIOS ou MEHARI) et une expertise avancée restent nécessaires en complément.

Construire sur l'existant

Le travail de planification initial et de construction du SMSI ne va pas forcément remettre en cause tout l'existant. Il est possible dans la plupart des cas de s'appuyer sur les éléments pertinents déjà existants, notamment les politiques, les chartes, les directives, mais aussi les procédures opérationnelles. Le schéma ci-dessous explicite les éléments apportés par l'existant et les nouveaux éléments qui seront vraisemblablement à créer.

	Existant	Alignement sur les principes	Certification
PLAN			Définition du périmètre
	Politique générale		
	Directives & chartes		
		Processus du SMSI	
		Analyse de risques	
			Déclaration d'applicabilité (SoA)
DO	Procédures	Approche contrôle / PDCA	Systématisation
		Gestion des actifs	Systématisation
			Gestion documentaire
CHECK & ACT		Plans de contrôles	Audits de conformité
		Mesures de l'efficacité	
			Gestion des preuves

Formaliser le SMSI

L'ISO 27001 n'impose pas de structure documentaire. Le document de politique de sécurité de l'information pourra ainsi très bien regrouper les principes de la politique du SMSI, son périmètre, l'organisation du SMSI et les directives/procédures sur lesquelles la sécurité sera bâtie.

Il pourra aussi être pertinent de consigner ces informations dans le manuel du SMSI, document maître du SMSI décrivant toute l'organisation mise en œuvre.

ISO 27003 : LE GUIDE D'IMPLEMENTATION

Annoncée pour la fin 2008, cette norme sera un guide d'aide à l'implémentation du SMSI.

Les premières versions de travail montrent une volonté forte de donner des conseils précis basés sur les meilleures pratiques rencontrées pour mettre en œuvre un SMSI.

Le document sera structuré en fonction de chaque étape du processus PLAN, DO, CHECK, ACT mais détaillera également la notion même de processus et abordera également les phases amont (facteurs clés de succès, engagement du management...).

La rédaction de cette norme est un travail important et complexe mais si le résultat est à la hauteur des espérances, elle pourrait devenir incontournable pour tous les RSSI.

Dans la plupart des cas, les procédures de sécurité devront être complétées par une description des processus de sécurité. Ces processus précisent les règles applicables par une vision « organisationnelle » des rôles et responsabilités. L'essentiel, c'est que tous les éléments qui composent le SMSI soient clairement identifiés. Si certains documents ne s'appliquent que partiellement au SMSI, cela doit être indiqué explicitement. C'est notamment le rôle de la Déclaration d'Applicabilité (SoA) qui, même si elle n'est pas impérative en dehors d'une certification officielle, constitue un document très pertinent pour bâtir le SMSI.

Mesurer l'efficacité du SMSI

Pour garantir l'efficacité du SMSI, il faut se doter de moyens de mesure représentatifs et cohérents. A travers la publication de tableaux de bord de sécurité, les porteurs du SMSI vont pouvoir à la fois mesurer cette efficacité, et communiquer vers les acteurs impliqués.

L'ISO 27004 ET LES INDICATEURS

Actuellement au stade final de normalisation, la norme ISO 27004 décrit les mécanismes de de conception et de mesure des indicateurs de suivi du SMSI.

Cette norme, très complète, contient beaucoup d'informations sur ce qu'est une mesure, comment les collecter et calculer les différents indicateurs issus de ces données. Suivant ensuite les différentes phases de la vie du SMSI (Plan, Do, Check, Act), la norme précise les actions qui devraient être conduites à chaque étape pour ce qui concerne les indicateurs.

En annexe, la norme propose des fiches de description des indicateurs et également de nombreux exemples d'indicateurs avec les modes de calcul associés.

Un bon indicateur est un compromis entre pertinence, complexité et pérennité. Pour construire des tableaux de bord, il faut à la fois :

- Reprendre et consolider les éléments qui existent déjà (souvent de nombreux indicateurs techniques issus des équipes d'exploitation).
- Mais aussi construire des éléments de haut-niveau représentatifs du SMSI dans son ensemble.

On retrouvera donc dans les indicateurs des éléments de mesure de chaque phase et notamment :

- De l'analyse de risques (PLAN) et du plan de traitement des risques (DO).
- De suivi des chantiers ISO 27001 et ISO 27002 (DO).
- Des contrôles et audits (CHECK).
- De suivi des actions correctrices et des recommandations des audits (ACT).

Trois pièges à éviter :

- Des indicateurs trop nombreux (au-delà d'une vingtaine).
- Des indicateurs sans identification d'objectifs à atteindre, donc difficiles à interpréter.
- Une industrialisation trop rapide : il vaut mieux valider que les indicateurs produits sont les bons avant d'industrialiser complètement.

ISO 27000 et contrôle interne

La mise en œuvre des normes ISO 27000 implique un renforcement du contrôle interne.

Ce renforcement est d'ailleurs mis en avant par toutes les démarches de gestion des risques qui considèrent que seul un processus contrôlé régulièrement peut être considéré comme maîtrisé. La plupart des nouvelles réglementations ont pour conséquence un renforcement du contrôle interne.

L'une des tâches essentielles de la phase CHECK consiste donc à élaborer et à mettre en œuvre un plan de contrôle qui définit l'ensemble des contrôles réalisés pour évaluer le niveau de maîtrise des processus de sécurité et l'efficacité du SMSI.

Il combine des contrôles de premier niveau, réalisés par les acteurs opérationnels, des contrôles de second niveau, réalisés par des acteurs tels que le RSSI, ou encore des contrôles périodiques ou audits réalisés par des tiers indépendants, comme par exemple les équipes internes d'inspection.

Chaque mesure mise en œuvre doit en théorie faire l'objet d'un contrôle régulier. De manière plus pragmatique, c'est l'analyse des risques qui doit permettre de définir les points de contrôles prioritaires ainsi que l'effort à consacrer pour chaque type de contrôle.

COBIT, ITIL et ISO 27000

La plupart des DSI ont engagé des démarches de mise en application des référentiels de gouvernance des SI, les plus souvent cités étant COBIT, ITIL et CMMI. Se pose donc la question de la cohérence et de l'articulation de ces démarches avec l'ISO 27000.

Sans entrer en concurrence, ces différentes normes peuvent se compléter et permettre des économies d'échelle. Par exemple la mise en place de démarches CMMI et ITIL facilite la mise en œuvre des mesures de l'ISO 27002. Le COBIT, avec son approche de gestion des risques, est également une aide pour viser l'ISO 27001. Il envisage des types de risques plus larges que l'ISO 27000 (risques affectant l'efficacité, la fiabilité ou l'efficience du SI, en plus des critères plus orientés vers la sécurité tels que la confidentialité, l'intégrité, la disponibilité ou la conformité) mais les démarches restent fondamentalement proches.

En règle générale, on peut considérer que les normes ISO 27000 constituent un approfondissement sur les thèmes de la sécurité de l'information et de la gestion des risques, qui sont évoqués de manière plus succincte dans les autres référentiels.

Il faut d'ailleurs noter que la norme ISO 20000, issue d'ITIL, « pointe » maintenant directement sur la norme ISO 27001 pour ce qui concerne le processus de gestion de la sécurité du SI.

LES OUTILS POUR GÉRER LE SMSI

Il existe différents kits sur le marché pour aider à la mise en place et au suivi d'un SMSI.

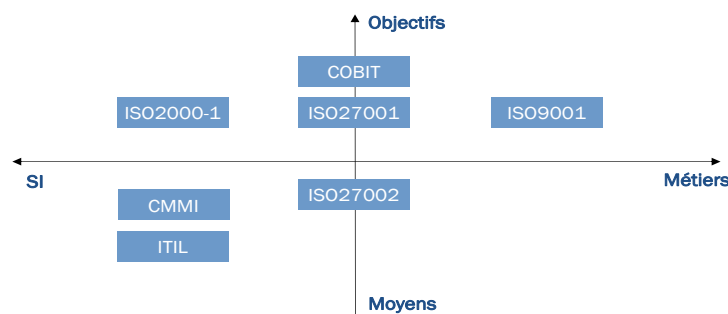
Ces kits permettent de simplifier le travail en proposant des modèles et des procédures standards (par exemple la gestion documentaire).

Attention cependant, l'aide apportée peut parfois se révéler contraignante, voire inadaptée car trop générique (par exemple pour l'analyse de risques).

L'expérience montre que beaucoup d'entreprises certifiées ont préféré se baser sur des outils « maison » basés sur les suites bureautiques classiques.

Les éléments importants à prévoir sont :

- Un fichier de suivi des exigences des §4 à 8 de la norme ISO 27001.
- Un modèle de SoA que l'on utilisera dans un premier temps comme un fichier de suivi des chantiers.
- Des modèles de procédures (gestion documentaire, mesures de protections, etc.).



La certification ISO 27001

La certification du SMSI par un organisme externe apporte une reconnaissance publique et internationale. Cette certification nécessite cependant des efforts importants qui doivent donc être justifiés par un réel besoin métier.

La certification garantit de manière indépendante que le SMSI est conforme aux exigences spécifiées, qu'il est capable de réaliser de manière fiable les objectifs déclarés et qu'il est mis en œuvre de manière efficace. Ses apports sont notamment :

1. Vis-à-vis des clients, des fournisseurs et des partenaires :
 - La réponse à des demandes explicites des clients lors d'émission d'appels d'offres requérant la certification.
 - La maîtrise des coûts avec la réduction du nombre d'audits mandatés par des tiers.
 - Le renforcement de l'image de marque de la société.
2. Pour l'entreprise, la capacité de mobiliser ses équipes derrière un projet commun et visible, dans un objectif de planning déterminé, et d'accélérer ainsi la démarche d'amélioration de la sécurité.

Mais viser la certification reste une cible ambitieuse nécessitant un bon niveau de maturité. C'est un projet à part entière nécessitant un haut niveau de sponsoring. C'est aussi un engagement dans la durée, aussi bien dans la fourniture de moyens que dans l'amélioration continue. À la vue des efforts nécessaires, la certification doit répondre à une demande explicite des métiers et de la direction de la société.

La certification dans le monde

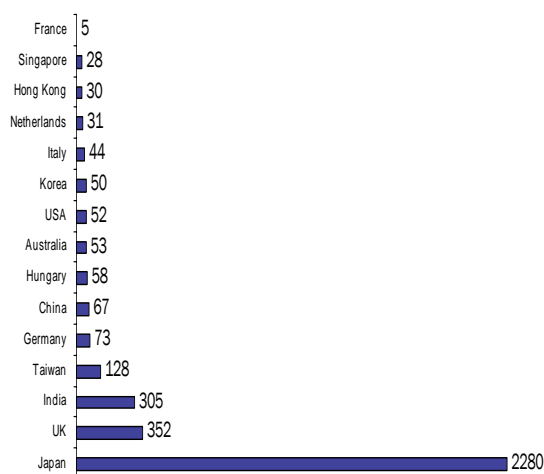
Aujourd'hui, le niveau d'adoption de la certification ISO 27001 est très hétérogène d'un pays à l'autre. Certains sont très en avance, en particulier le Japon. D'autres (États-Unis, Inde...) sont en train de rattraper leur retard suite à la publication de l'ISO 27001 comme norme internationale. Fin août 2007, 2 323 certifications ISO 27001 ont été prononcées dans le monde.

En France, quelques sociétés ont obtenu la certification. Agissant principalement sur le domaine des technologies de l'information, ces sociétés ont certifié des processus particuliers proches de leur cœur de métier.

COMMENT ÉVALUER LE CERTIFICAT D'UN PARTENAIRE ?

L'obtention de la certification et son utilisation lors d'échanges commerciaux sont soumises à des règles assez strictes définies par l'ISO. Cependant la certification ne garantit pas forcément la sécurité du partenaire et de ses infrastructures. En effet la norme impose uniquement la présence et le bon fonctionnement du SMSI. Il est donc important de vérifier les critères suivants pour bien évaluer l'apport de la certification :

- Le périmètre du certificat, qui détaille quels processus de l'entreprise sont couverts par le SMSI.
- La déclaration d'applicabilité (SoA), qui précise quels contrôles (issus ou non de la norme ISO 27002) ont été sélectionnés et mis en œuvre.
- La date de certification, qui indique la pérennité de la démarche chez le partenaire. Ce critère est à relativiser au vu de la récente publication de la norme, mais il est important que le SMSI ait au moins réalisé une fois le cycle PDCA.



Entreprises certifiées par pays

Source : <http://www.iso27001certificates.com/08/2007>

La certification, une démarche encadrée et normalisée

Pour obtenir la certification, il est nécessaire de faire auditer son SMSI par un organisme de certification externe. La certification du SMSI ISO 27001 suit le même processus que celle des autres systèmes de management tels que l'ISO 9001 et l'ISO 14001 (système de management environnemental). Les normes génériques d'audit sont complétées par des textes spécifiques au SMSI, en particulier la norme ISO 27006.

L'organisation souhaitant se faire certifier va tout d'abord contracter avec un organisme de certification. Ce contrat d'une durée de 3 ans va encadrer l'ensemble du cycle de la certification. L'organisme de certification va mandater des auditeurs certifiés pour réaliser les contrôles. Plusieurs types d'audits sont formellement identifiés : l'audit initial couvrant la totalité du périmètre, des audits de surveillance sur un périmètre plus restreint et l'audit de renouvellement.

La durée de l'audit est déterminée par la norme ISO 27006 et varie suivant le nombre et la taille des sites, le nombre de personnes dans le périmètre et la complexité du SI. À titre d'exemple, il faut compter un peu moins de 30 jours d'audit pour une société de 10 000 employés.

« La vérification de la documentation et des enregistrements est au centre de la démarche de certification. Elle exige donc un niveau de maturité élevé sur ces points ! »

Réalisation de l'audit de certification

Suite à cette phase de contractualisation, l'audit certifiant est initié. Une première phase de vérification documentaire est réalisée avant d'enchaîner sur les visites de sites. Lors de cette opération, les auditeurs réalisent un ensemble de contrôles, techniques et organisationnels, pour vérifier que le SMSI « tourne », que les principes sélectionnés ont bien été mis en œuvre et que le système est pérenne.

La majorité des contrôles organisationnels nécessitent la fourniture de preuves concrètes (compte-rendu de réunion, documents approuvés, listes de personnes ayant suivi les formations...). Les contrôles plus techniques sont vérifiés concrètement avec l'auditeur par la réalisation d'opérations sur les systèmes (affichage des habilitations, vérification des correctifs,...). De plus, certains contrôles par des interviews spontanées d'employés sont possibles.

Suite à l'audit, les auditeurs font parvenir leurs recommandations à l'organisme de certification qui approuve les résultats et peut délivrer le certificat officiel. En cas de désaccord avec les résultats, il est possible de poser des recours.

ISO 9001 ET ISO 27001 : QUELS AXES D'OPTIMISATION ?

L'obtention de la certification ISO 9001 est un avantage indéniable pour entamer une certification ISO 27001. En effet, l'ensemble des éléments sous-jacents nécessaires sont déjà présents : démarche de progrès continu, revue du management, gestion documentaire, suivi des compétences, audit interne...


La réalisation d'audits combinés est un autre axe d'optimisation, elle permet la réduction du nombre de jours d'audits, la mutualisation des efforts et l'alignement des plans d'actions.

Attention cependant, les différents éléments composants les systèmes de gestion doivent être clairement identifiés, aussi bien au niveau des documents internes que des rapports d'audits et de certification.

Les difficultés de la certification

Au-delà des points clés inhérents à la mise en place du SMSI (périmètre, analyse de risques et mesure de l'efficacité), les difficultés rencontrées couramment lors des audits certifiant sont les suivantes :

- La gestion des enregistrements et des preuves demande des efforts importants de formalisation et de communication. C'est sur cette base que les contrôles seront réalisés.
- La connaissance, sur le périmètre concerné, des principes et des règles de sécurité. Les auditeurs ne manqueront pas d'interroger aussi bien des responsables métiers que des employés, voire des prestataires, sur leur connaissance des pratiques de sécurité. Même si un problème sur ce point n'entraînerait qu'une remarque de la part des auditeurs, il est difficile de garantir un sans faute sur ce volet.
- La certification d'un SMSI n'ayant pas encore fait ses preuves. Même si cette pratique n'est pas recommandée, la norme autorise la certification d'un SMSI n'ayant pas encore réalisé un cycle de la boucle PDCA. La certification sera alors plus facile à obtenir mais les audits de renouvellement ne manqueront pas de vérifier que les actions de type CHECK et ACT sont réalisées. Le relâchement « naturel » suite à l'obtention de la certification pourrait alors être fatal.



« Adopter les principes
dès aujourd'hui,
certifier sur opportunité »

Conclusion

La norme ISO/IEC 27001, première brique d'une grande famille de normes internationales consacrées à la sécurité des systèmes d'information, constitue une avancée majeure dans le mouvement de professionnalisation progressive des démarches de sécurité.

Elle formalise des principes essentiels qui vont permettre un alignement progressif de la sécurité de l'information avec les meilleures pratiques de management : pilotage par les risques, formalisation des processus, contrôle, amélioration continue...

Appelée à s'imposer, l'ISO 27000 est aussi pour les RSSI et les DSI un outil de communication efficace permettant d'asseoir la crédibilité et la cohérence des démarches d'amélioration de la sécurité, et de conforter et valoriser ces démarches vis-à-vis du top management. Avec la certification officielle, cette crédibilité deviendra même dans certains secteurs d'activité une reconnaissance externe incontournable.

Il ne faut pourtant pas tout attendre de l'ISO 27000 : en aucun cas les normes n'aident à choisir le bon niveau de granularité et de détail pour conduire les analyses de risques. Elles n'aident pas non plus à sélectionner les mesures de sécurité adaptées au contexte et ne garantissent pas que les processus que vous allez définir seront les plus efficaces pour maîtriser vos risques. Comme dans le domaine de la qualité, les normes fixent des objectifs, proposent une méthodologie, mais seuls le bon sens et l'expertise assurent la pertinence des choix d'implémentation.

Le chemin à parcourir pour s'aligner complètement avec la norme et atteindre la certification ISO 27001 s'avèrera souvent long, coûteux et ambitieux. La certification officielle doit donc être réservée pour le moment aux organisations qui peuvent y trouver un apport direct pour leur cœur de métier.

Mais que cela n'empêche pas chaque entreprise d'appliquer dès maintenant les bons principes des normes, et d'accélérer ainsi leur démarche d'amélioration de la sécurité ! C'est en focalisant dans un premier temps l'attention sur le traitement des risques majeurs que l'on pourra pleinement tirer partie des enseignements des normes tout en se donnant un périmètre de travail raisonnable. Une fois ces risques majeurs maîtrisés, les cycles successifs de la boucle PDCA permettront d'élargir progressivement le périmètre des risques traités pour couvrir à terme l'ensemble du système d'information.

En résumé, appliquons dès aujourd'hui les bons principes de l'ISO 27000, mais visons la certification uniquement lorsque le jeu en vaut la chandelle !

Gérôme Billois,
gerome.billois@solucom.fr

Tristan Savalle
tristan.savalle@solucom.fr

Laurent Bellefin
laurent.bellefin@solucom.fr

Annexe

Etat des normes ISO 27000 au 15/09/07

Norme ISO 2700x	Sujet	Statut	Commentaire
27000	Définitions et vocabulaire	Draft	-
27001	Mise en place d'un SMSI	Publiée	Norme certifiable
27002	Guide de bonnes pratiques de sécurité de l'information	Publiée	Remplace l' ISO 17799 :2005 (133 mesures de sécurité)
27003	Mise en place d'un SMSI	Draft	
27004	Indicateurs et tableaux de bord	Draft	A paraître en 2008
27005	Gestion des risques	Draft	Basée sur la BS 7799-3
27006	Exigences pour les organismes d'audit et de certification des SMSI	Publiée	En complément de l'ISO 17021.
27007	Guide pour l'audit d'un SMSI	Draft	Inspirée de l'ISO 19011:2002 relative à l'audit de SME (environnement) et SMQ (qualité)
27011	Guide pour le secteur des télécommunications	Draft	A paraître à partir de 2010
27012	Guide pour le secteur des finances	Proposée	Non confirmée
27013	Guide pour le secteur de l'industrie	Proposée	Non confirmée
27015	Directives pour l'accréditation	Proposée	Non confirmée
27016	Audits et revues	Proposée	Non confirmée
27031	Continuité d'activité	Draft	Sera basée probablement sur une norme Singapourienne : BC/DR SS507 et sur le British standard : BS 25999
27032	Cybersécurité (Internet)	Proposée	Non confirmée
27033	Sécurité des réseaux informatiques	Draft	Révision de l'ISO 18028, comprenant 7 parties : 27033-1, 27033-2, ..., 27033-7
27034	Sécurité applicative	Draft	-
27799	Guide de bonnes pratiques pour le secteur de la santé	Draft	Equivalent de l'ISO 27002 appliquée au secteur de la santé



Tour Franklin, 100-101 terrasse Boieldieu
92042 Paris La Défense Cedex
Tél : 01 49 03 25 00 Fax : 01 49 03 25 01
www.solucom.fr