SMSI Oui ! Certification ? Peut être…

Gérer concrètement ses risques avec l'ISO 27001

« L'homme honorable commence par appliquer ce qu'il veut enseigner » Confucius

solucom
solucom group

23 octobre 2008

Agenda

1. L'ISO 27001 : pour gérer les risques ?
2. Principes et implémentation de l'ISO 27001
3. Pour plus d'information...

L'enjeu : maîtriser les risques pesant sur la sécurité des SI

Contribuer **aux stratégies Métier**…

… en maîtrisant les risques de sécurité de l'information de façon **globale** et **transverse** …

… en **rationalisant** l'organisation et les ressources sécurité…

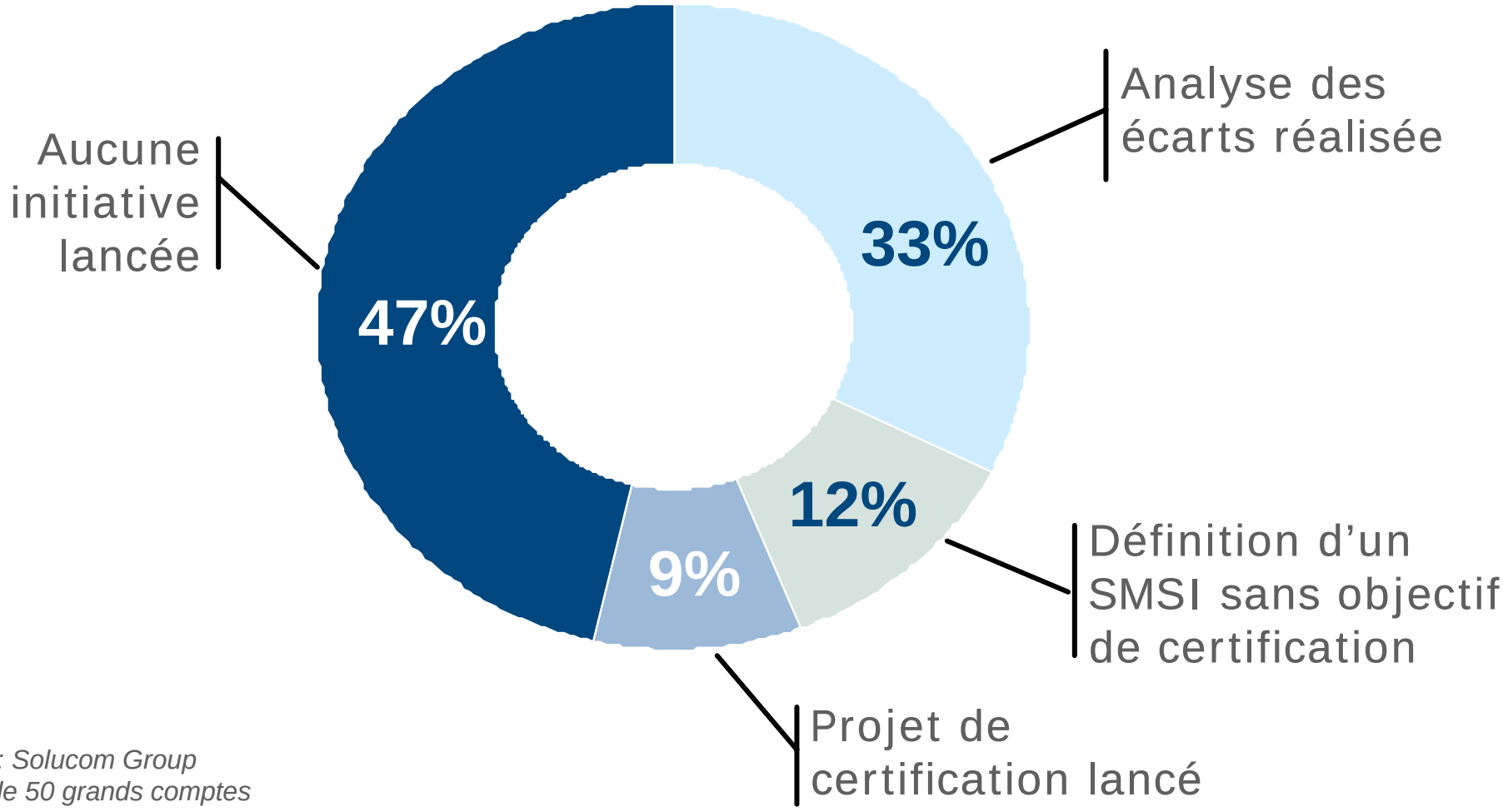
… et en s'inscrivant dans une **dynamique de progrès**

Une réponse : installer une vraie
Gouvernance de la Sécurité de l'Information

Un outil : L'ISO 27001

Les initiatives ISO 27001 dans les grands comptes

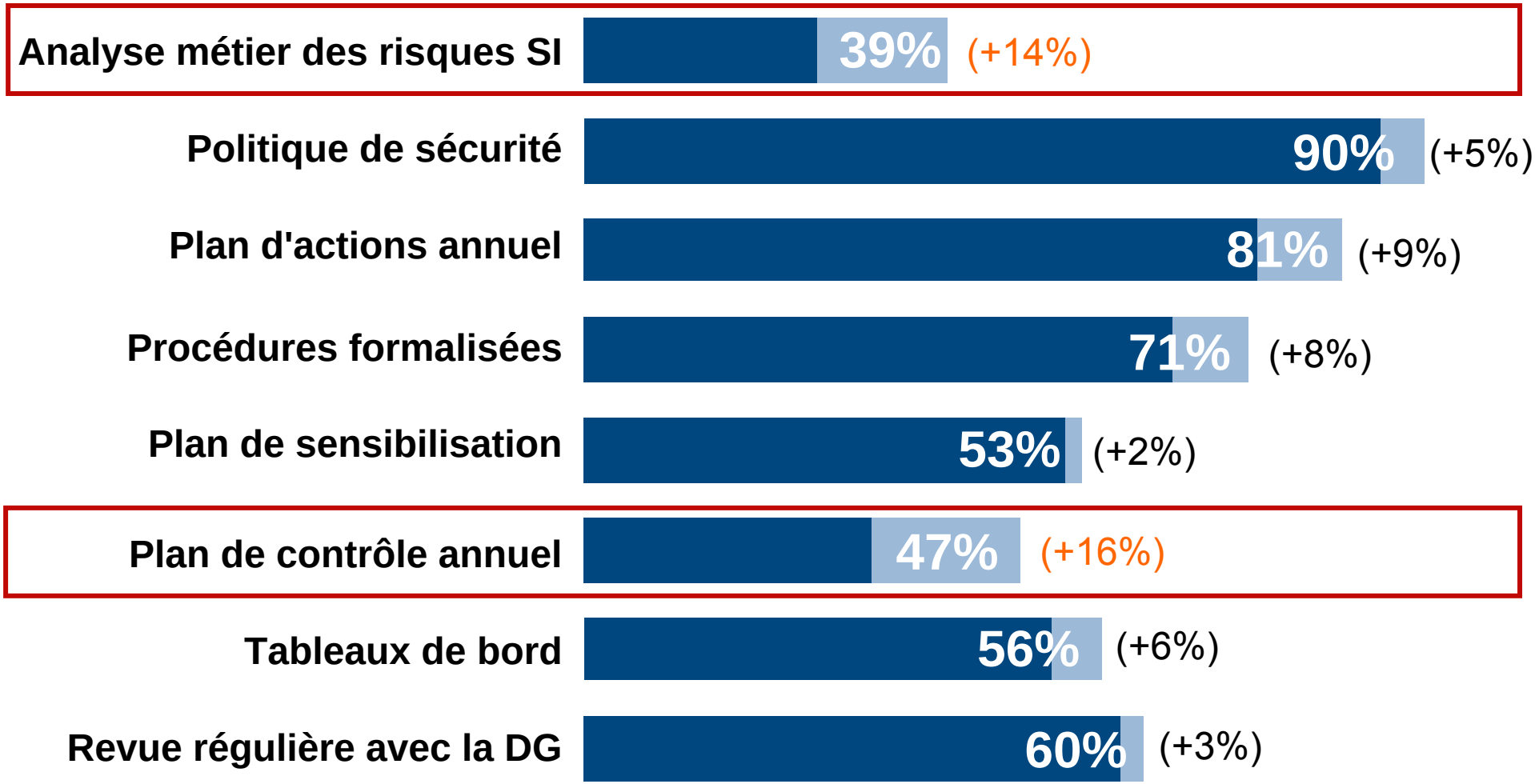
Un mouvement d'adoption réellement enclenché



Source: Solucom Group
Panel de 50 grands comptes
Septembre 2008

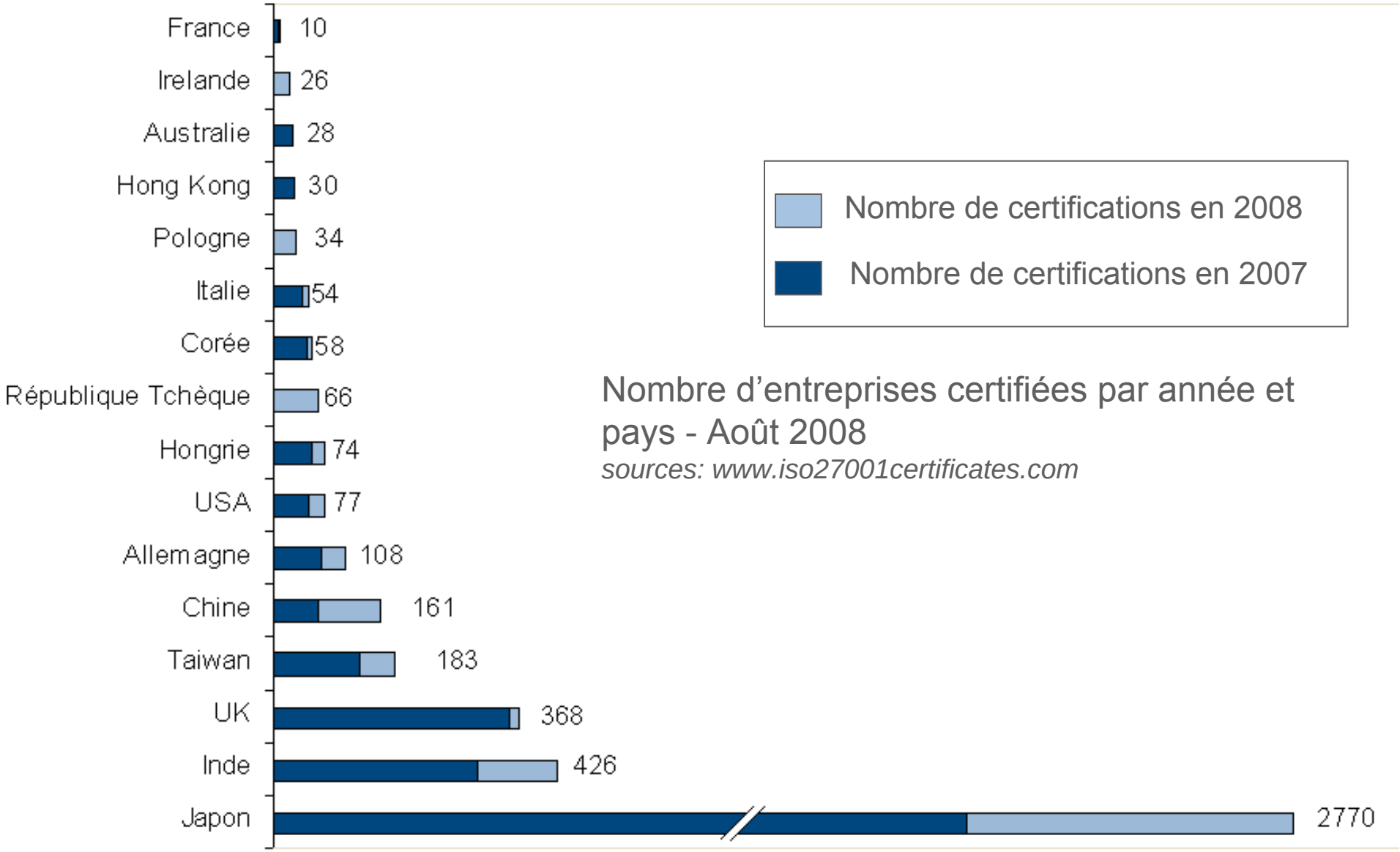
L'adoption des principes de l'ISO 27001 dans les grands comptes

Une norme qui insiste « là où le bât blesse »



Source : Solucom Group
Panel de 50 grands comptes - Septembre 2008

Un mouvement de certification ISO 27001 qui reste timide en France



Nombre d'entreprises certifiées par année et pays - Août 2008

sources: www.iso27001certificates.com

L'ISO 27001 pour gérer les risques ?

La famille des normes ISO 2700x (septembre 2008)

Norme	Titre	Statut
27000	Définitions et vocabulaire	Draft
27001	Exigences d'un SMSI	Publiée
27002	Guides de bonnes pratiques de sécurité de l'information	Publiée
27003	Guide d'implémentation d'un SMSI	Draft
27004	Indicateurs et tableaux de bord	Draft
27005	Gestion des risques	Publiée
27006	Exigences pour les organismes d'audit et de certification	Publiée
27007	Guide pour l'audit d'un SMSI	Draft
WLA SCS	Standard SMSI spécifique au secteur du jeu (World Lottery Association)	Publiée

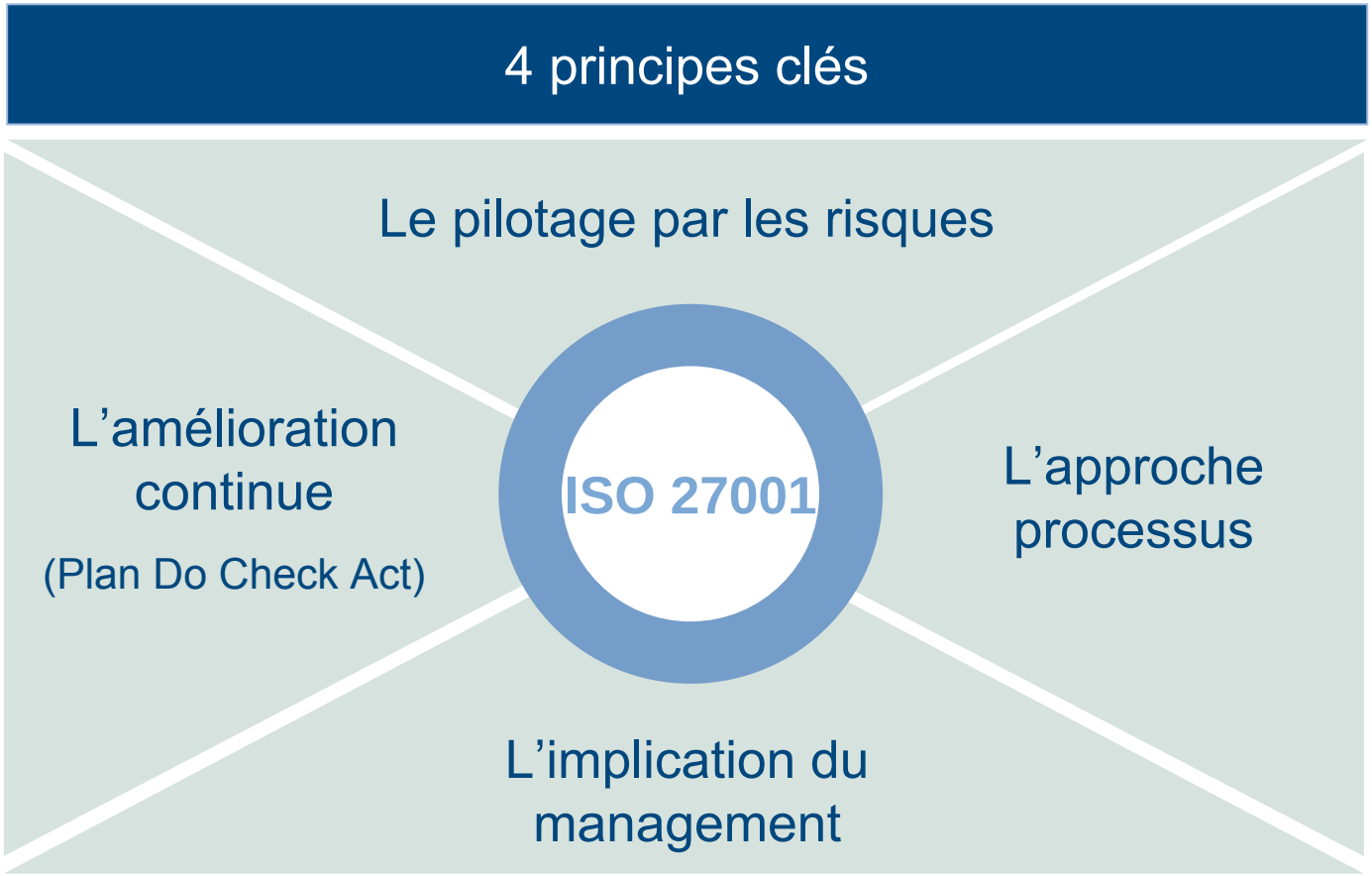
Norme	Titre	Statut
27011	Guide pour le secteur des télécommunication	Draft
27012	Guide pour le secteur financier	Proposée
27013	Guide pour le secteur de l'industrie	Proposée
27015	Guide pour l'accréditation	Proposée
27016	Audits et revues	Proposée
27031	Continuité d'activité	Draft
27032	Cybersécurité (Internet)	Draft
27033-x	Sécurité des réseaux	Draft
27034-1	Guide pour la sécurité applicative	Draft
27035	Gestion des incidents de sécurité	Draft
27799	Déclinaison de l'ISO 27002 pour le secteur de la santé	Publiée

Agenda

1. L'ISO 27001 : pour gérer les risques ?
2. Principes et implémentation de l'ISO 27001
3. Pour plus d'information...

Un SMSI reposant sur 4 principes clés…

L'ISO 27001 propose un modèle répondant aux enjeux d'une gouvernance optimisée et pérenne de la sécurité de l'information :
le **Système de Management de la Sécurité de l'Information (SMSI)**



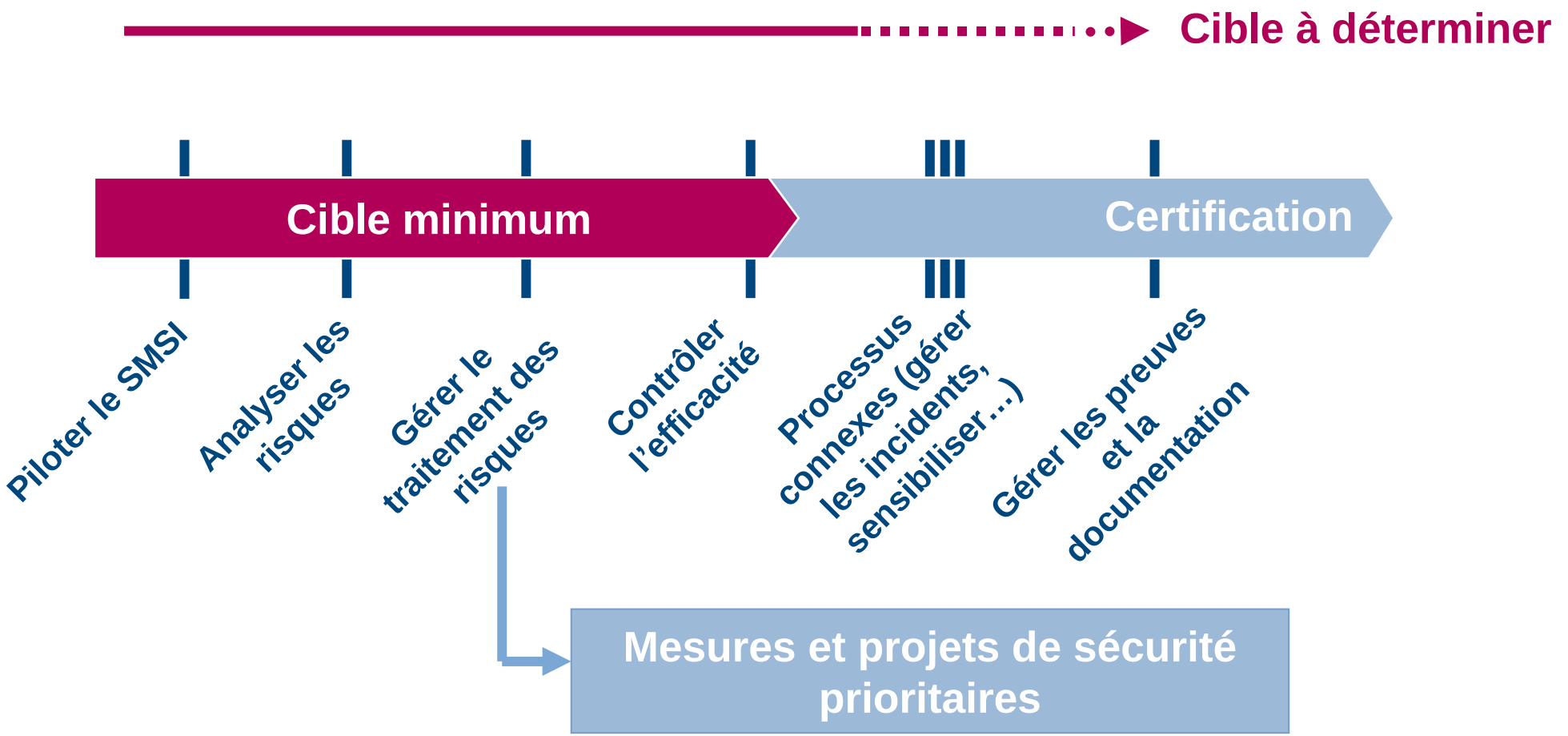
…impliquant la formalisation de 7 processus essentiels…

7 processus essentiels

Chaque processus s'applique à lui même le principe d'amélioration continue

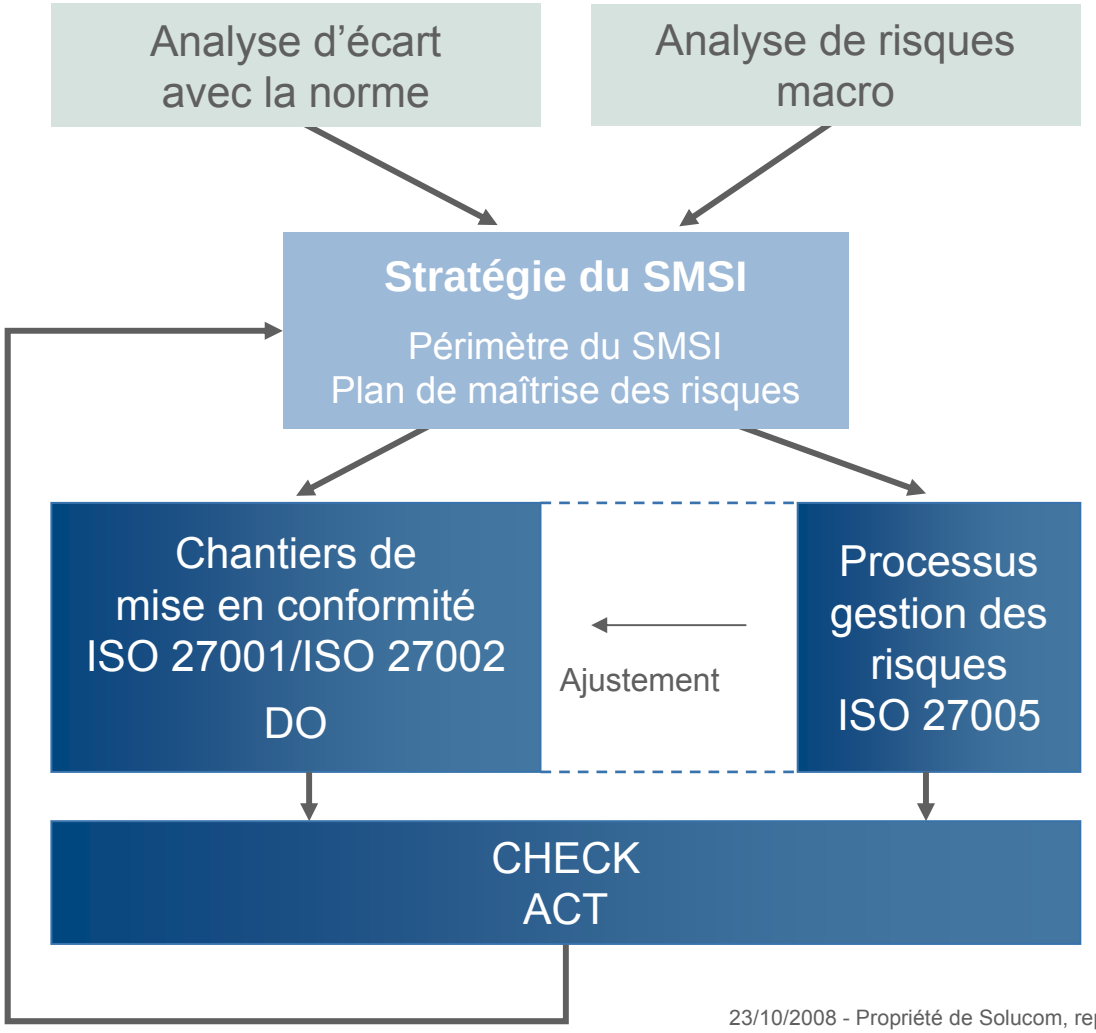
1. Piloter le SMSI
2. Analyser les risques
3. Gérer le traitement des risques
4. Contrôler l'efficacité
5. Gérer les incidents et les vulnérabilités
6. Former et sensibiliser
7. Gérer la documentation et les preuves

…dont l'implémentation doit être priorisée



Donner rapidement une impulsion décisive

Mettre en place une démarche continue de maîtrise des risques



Déterminer rapidement les grandes orientations

Cartographie initiale : Une première analyse de haut niveau

Orientations des grands chantiers et choix du **périmètre**

Cartographie mise à jour : des analyses détaillées sur des périmètres réduits

Ajustement des priorités de mise en œuvre locale des chantiers

Le contrôle : une démarche à industrialiser

Deux objectifs

Évaluer l'efficacité des mesures prises de façon systématique…
… et sensibiliser les opérationnels et les responsables

Points de contrôle

Risques

Politique de sécurité

Démarche de contrôle

Contrôle interne de l'entreprise

Degré 1 Opérationnel (autocontrôle)	**Degré 2** Management & filière de contrôle permanent	**Degré 3** Audits périodiques

Plan de contrôle Sécurité de l'Information

Ajustement / **réalignement** des plans d'actions

Le contrôle : une démarche à industrialiser

3 recommandations

- Identifier les points de contrôles très en amont
  - Dès la formalisation des Politiques de Sécurité pour les points de contrôle globaux
  - Dès la définition des mesures de sécurité dans les projets SI pour les points de contrôles spécifiques à certains périmètres
- Accompagner la mise en œuvre du dispositif de contrôle
  - Mettre en place un accompagnement des opérationnels en conséquence
  - Installer un reporting régulier diffusé aux acteurs impliqués
- Dans la communication, toujours relier les contrôles aux risques associés

Quelques autres points clés

- Bien **définir le périmètre**, et « l'entité de management » associée
  - Le nombre de processus métiers concernés est plus structurant que la taille du périmètre (nombre de sites, nombre d'utilisateurs)
- Prendre en compte la **gestion des « ressources externes »**
  - Gestion du SI
  - Gestion des ressources humaines
  - Gestion des achats…
- S'appuyer sur **l'existant**

- Analyser les risques
- Etablir les conventions de service (auditabilité, indicateurs, preuves, gestion des incidents…)

- **Réévaluer les risques périodiquement** pour faire évoluer le SMSI (par exemple pour prendre en compte de nouvelles réglementations telle que PCI-DSS)
- Et communiquer, **communiquer**….

Conclusion : ce qu'il ne faut pas attendre de la norme !

L'ISO 27001 ne garantit pas
un « bon » niveau de sécurité

Elle ne permet pas de se situer par rapport au marché

Elle ne dit pas comment choisir la « bonne maille » pour réaliser l'analyse des risques

Elle ne garantit pas la pertinence des processus et des solutions de sécurité

Conclusion : les apports de la norme

L'ISO 27001 rationalise et crédibilise la démarche sécurité

Une communication vers le management plus efficace

- Rendre la démarche du RSSI plus crédible et plus lisible
- Obtenir une réelle implication des métiers et contribuer à leur performance

Une meilleure mobilisation des acteurs

- En partageant des objectifs et des périmètres réalistes
- En les impliquant dans le contrôle et la boucle de progrès

Une valeur d'image et de crédibilité externe

- En particulier avec la certification ISO 27001
- Lorsqu'elle répond à un enjeu Métier

Agenda

1. L'ISO 27001 : pour gérer les risques ?
2. Principes et implémentation de l'ISO 27001
3. Pour plus d'information...

Le 18 septembre 2008…

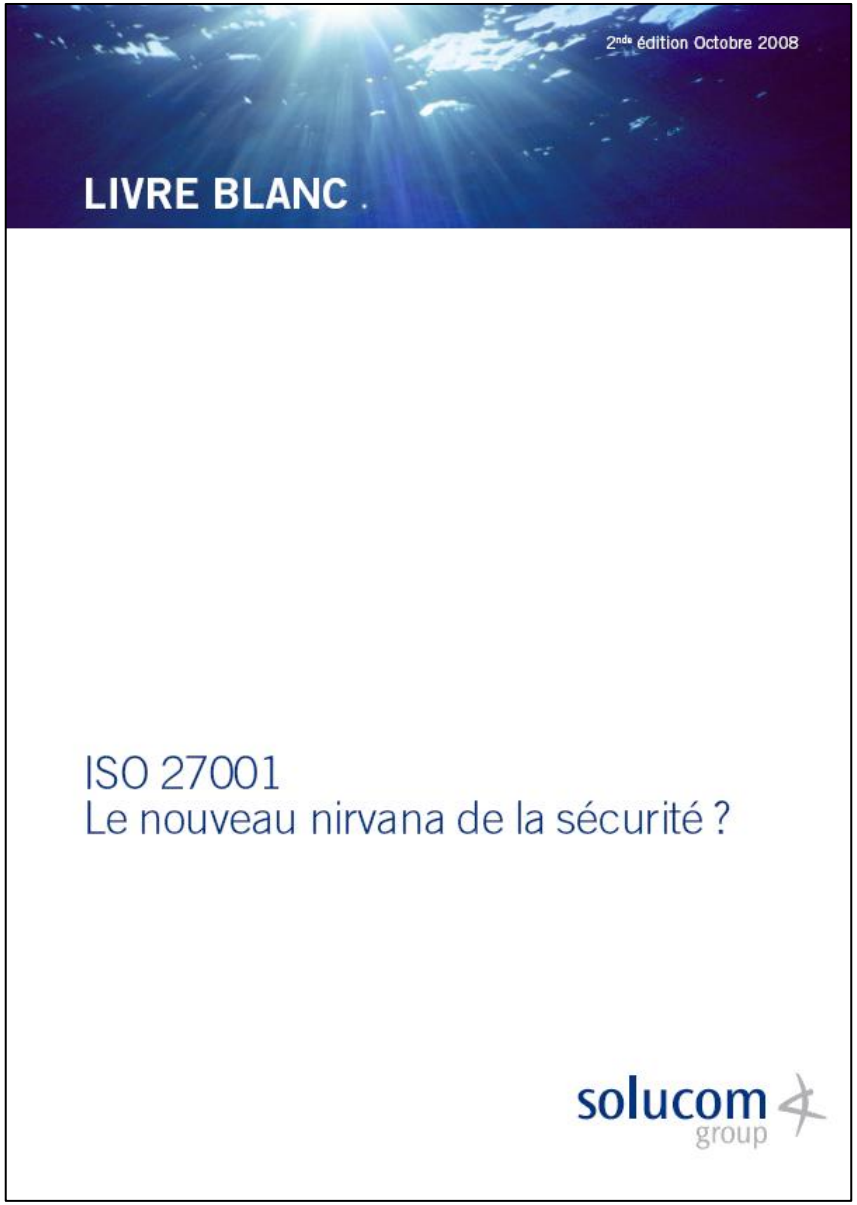
Solucom annonce la certification ISO 27001 de ses prestations d'audit de sécurité des systèmes d'information

« L'homme honorable commence par appliquer ce qu'il veut enseigner » Confucius

Pour plus d'information

Que pouvez vous attendre de la norme ISO 27001 ?

2nde édition de
notre livre blanc
qui vient d'être publié



Des questions ?

LSTI®

Certifié NF ISO/CEI 27001:2005

SOLUCOM – Certificat LSTI/SMSI/11

solucom group

www.solucom.fr
www.solucom-group.fr

Votre contact :

Laurent BELLEFIN

Directeur des opérations sécurité

Tel : +33 (0)1 49 03 25 32

Mobile : +33 (0)6 16 10 20 72

Mail : laurent.bellefin@solucom.fr