



HERVÉ SCHAUER CONSULTANTS

Cabinet de Consultants en Sécurité Informatique depuis 1989

Spécialisé sur Unix, Windows, TCP/IP et Internet

# Usages de l'ISO 27001 dans les entreprises

**Paris**

**15 février 2008**

**Hervé Schauer**

<Herve.Schauer@hsc.fr>

- Usages constatés de l'ISO 27001
  - Pour l'ISO 27002 (ISO 17799) sans ISO 27001
  - Pour son organisation de la SSI
  - Pour clarifier la conformité
  - Parce que c'est tendance et cela apporte la confiance
  - A cause d'ISO 20000-1
  - Signature électronique
  - Pour une certification dans longtemps
- Usages à venir
  - Pour une partie prenante qui l'impose
  - Pour ses atouts réglementaires
  - Pour l'intérêt financier

**Les transparents seront  
disponibles sur  
[www.hsc.fr](http://www.hsc.fr)**

- Conclusion

- Sans ISO 27001
- Utilisation des mesures de sécurité comme bonnes pratiques
- Utilisation sans réflexion, analyse ou discernement
- Utilisation sans appréciation des risques ou indépendamment
  
- Latence des utilisateurs à découvrir ISO 27001
- « Politiques de sécurité » recopiant bêtement ISO 27002
- Effet néfaste de l'ISO 27799
- Effet des textes publiés avant 11/05 mentionnant « BS7799 »

- ISO 27001 **bon moyen de s'organiser / structurant**
  - Amélioration continue
  - Audits internes
  - Appréciation des risques
  - Traitement des incidents
  - Indicateurs, ...
  - Facilite le dialogue et la communication avec
    - Les métiers, les utilisateurs
    - La production / la DSI
    - Les auditeurs
- Usage pour soi en tant que RSSI

- Effet **conformité** grandissant
- RSSI qui passent leur temps à recevoir les auditeurs
- ISO 27001 dénominateur commun de toutes les conformités SSI
- Mutualisation vis-à-vis des auditeurs
  - Seconde partie
  - SoX
  - Commission bancaire, Bâle II
  - Cours des comptes
  - ...

- Tendance
  - « Grands » qui adoptent la démarche
- Tendance  $\Rightarrow$  Confiance  $\Rightarrow$  Croissance
- Pas encore jusqu'à la certification
  - Certification n'apporte pas nécessairement / pas encore la confiance
- Dynamique positive
- Confiance entre les parties parce que utilisation d'un référentiel commun
  - Adoption par les sociétés de conseil et les SSII
    - Confiance client/fournisseur en SSI
  - Adoption internationale
    - Compréhension mutuelle

- ISO 20000-1 définit les processus ITIL en version PDCA
- ITIL populaire dans les DSI
- Certification ISO 20000-1 : moyen de preuve d'adoption des bonnes pratiques
- DSI motivés, car positif pour leur carrière personnelle
- ISO 20000-1  $\Rightarrow$  ISO 27001 pour la cohérence
  - Processus « Gestion de la Sécurité »  $\Rightarrow$  Processus SMSI
- Levier pour les RSSI

- Prestataires de services de confiance
- Professions réglementées
- Inspiration ISO 27001
  - Certification
  - PDCA
  - Audit
  - etc

- Certification pas un objectif officiel ou affiché, mais envisagé par certains
  - ISO 27001 nécessaire pour cela
- Auto-satisfaction du travail accompli
  - Flatte l'égo du RSSI
- Certification : seule garantie d'avoir un SMSI
  - Renverse l'habituel « Après moi le déluge »
  - Maturité passe par la certification
- Intérêt marketing

## Pour une partie prenante

- Partie prenante qui impose la certification ISO 27001
  - Manipulation de données sensibles par le tiers
    - Futurs modèles
    - Base de données nominatives
- Facilité de rédaction dans les appels d'offre
  - « Le prestataire devra être certifié ISO 27001 sur le périmètre considéré et intégrer nos données hébergées dans les actifs sensibles »
- Meilleure transparence
- Facilite les audits externes

- Pour mieux respecter la loi (extraits non-exhaustifs) :

## Plan

- Identifier les législations en vigueur (5.2.1.c) (A.15.1.1)
- Définir une politique de sécurité tenant compte des exigences légales (4.2.1.b.2)
- Utiliser une méthodologie d'appréciation du risque adaptée aux exigences légales (4.2.1.c.1)
- Sélectionner les mesures de sécurité pour respecter les obligations légales (4.2.1.g) (3.16)

## Do

- Appliquer la législation en matière de données nominatives (A.15.1.4)
- Collecter les preuves suite à un incident de sécurité conformément aux dispositions légales (A.13.2.3)

- Pour mieux respecter la loi (suite) :

## Check

- Maîtriser les enregistrements conformément à la loi (4.3.3)
- Réexaminer l'appréciation des risques en tenant compte des modifications apportées à la législation (4.2.3.d.6)
- Vérifier la conformité à la législation applicable lors des audits internes (6.a)
- Vérifier lors de la revue de direction les changements législatifs (7.3.c.4)

- Pour la **clarté des rôles et responsabilités**
  - Politique du SMSI ou politique de sécurité = **doctrine**
    - 2 à 4 pages de vision **réellement approuvées par le comité de direction**
  - Facilite l'engagement de la direction qui est **indispensable**
  - Engagement formel de la direction lors de l'appréciation des risques sur le plan de traitement des risques
  - Engagement devant être renouvelé formellement un fois par an
  - ➔ Possibilité de délégation de responsabilité plus claire
  - Direction générale ➔ RSSI
    - Plus exhaustive et mieux bornée

- Pour les preuves et les enregistrements
  - Système de management  $\Rightarrow$  preuves et enregistrement formels
  - Génération d'indicateurs pour mesurer l'efficacité
  - Audits internes
  - Réunions de réexamen régulières
  - Application de mesures correctives
  - Revue annuelle par la direction générale
  - $\rightarrow$  Constitution des dossiers de preuves et de préjudice plus facile
  - $\rightarrow$  Contestation ce ceux-ci plus difficile
  - $\rightarrow$  Meilleure préparation et anticipation des conflits

- ISO 27001 : Norme homologuée en France depuis 12/07
  - [http://www.standarmedia.com/std/gen\\_glo.asp?PageLetter=N&Page=1](http://www.standarmedia.com/std/gen_glo.asp?PageLetter=N&Page=1)

*Norme homologuée :*

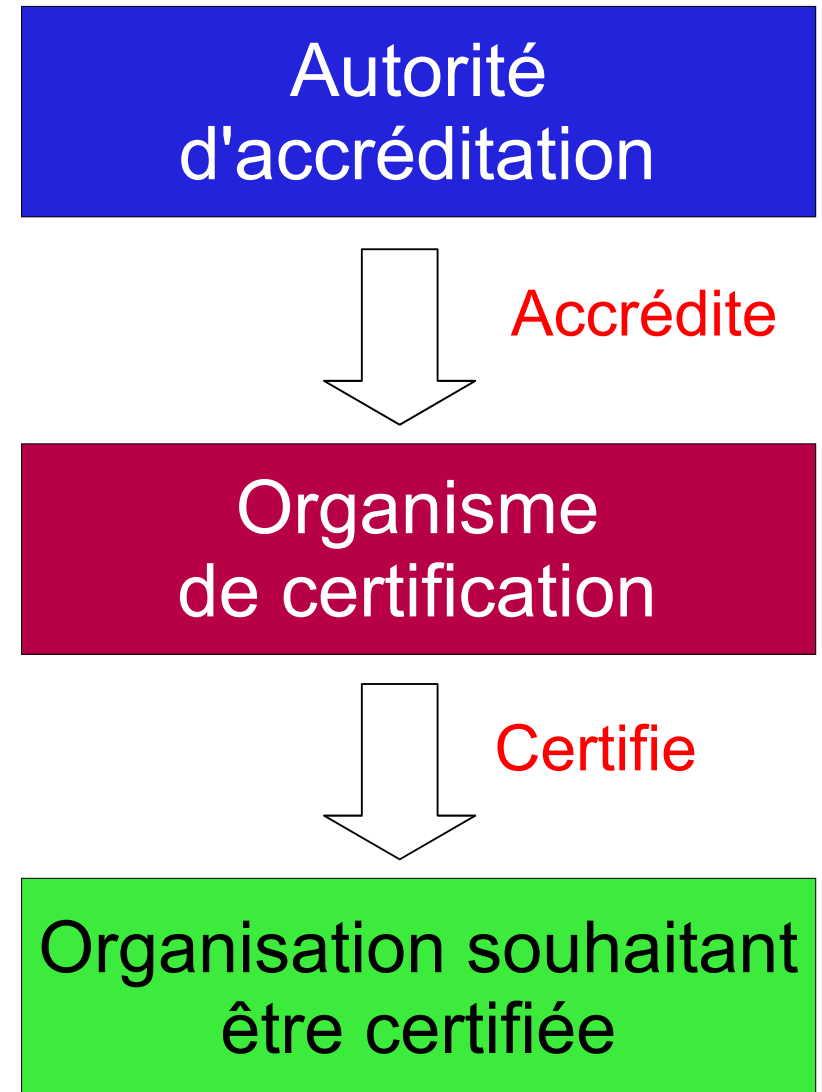
*Norme française ayant fait l'objet de la procédure officielle d'approbation et de publication prévue par le décret 84-74 modifié, fixant le statut de la normalisation et par la directive relative à l'établissement des normes du 7 novembre 1994 du ministre chargé de l'industrie.*

*Elle peut servir de référence dans une réglementation, un marché public, une marque NF.*

*L'homologation confère à la norme son caractère officiel et national.*

*Une norme homologuée peut être rendue obligatoire à l'appui d'une réglementation notamment dans les domaines de la sécurité, de la santé et de l'environnement.*

- Par la certification
  - Tierce partie indépendante certifie que vous appliquez la norme
  - Cela prouve que vous avez fait ce que vous avez dit et réciproquement que vous dites ce que vous faites
  - Reconnaissance internationale par l'accréditation des certificateurs par les organismes d'état
  - → **Présomption de fiabilité devant les tribunaux**
  - → **Renversement de la preuve**



- Réduction substantielle des primes d'assurance
  - Même avant l'obtention de la certification
- Mutualisation des audits seconde partie

- Usage encore limité
- Utilisation pour des raisons variées
- Intérêt individuel encore primordial

## Questions ?

[Herve.Schauer@hsc.fr](mailto:Herve.Schauer@hsc.fr) [www.hsc.fr](http://www.hsc.fr)



### ISO 27001 a son club !

Paris, Toulouse, Rennes, ...

*En projet* : Lyon, Nice, ..

Mutualisation ITIL/itSMF

[www.club-27001.fr](http://www.club-27001.fr)

