

Conférence CLUSIF, 23 Octobre 2008

Très faible nombre de sociétés certifiées ISO 27001 en France

Retour d'expérience de la dernière en date

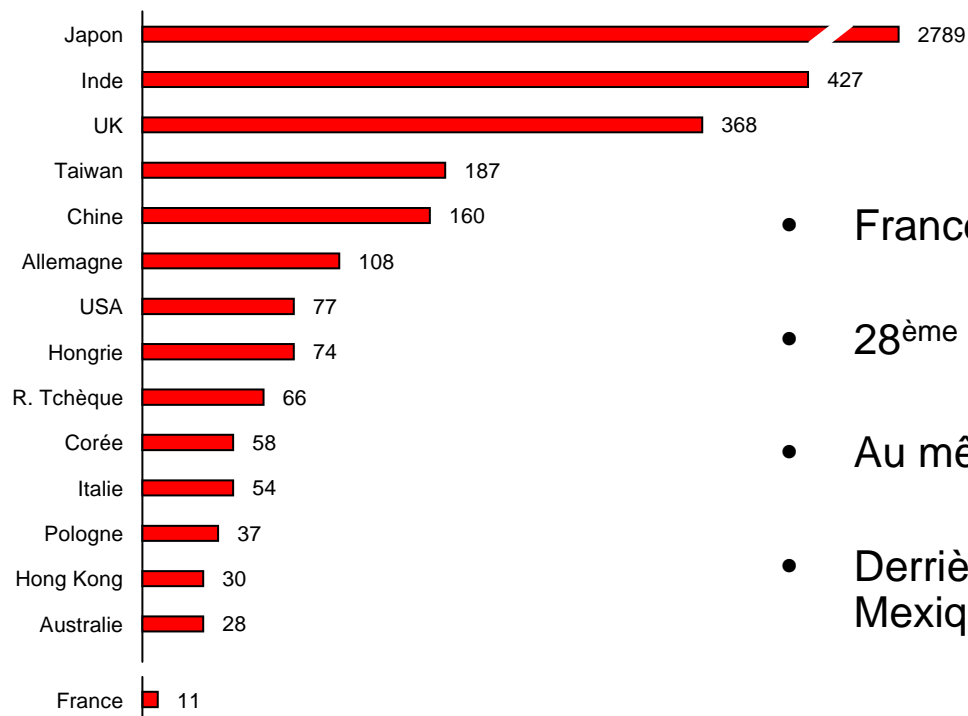


Stéphane Duproz – Directeur Général
stephane.duproz@telecity.com

Seulement 11 certifiés



Nombre de certificats ISO 27001 dans le monde = 4848



- France 10 certifiés + TelecityGroup
- 28^{ème} rang mondial avec 0,22% des certifiés
- Au même niveau que Philippines ou Pakistan
- Derrière Turquie, Roumanie, Thaïlande, Mexique

Source: International Register of ISMS Certificates – version 185, October 2008

Beaucoup de freins, supposés ou réels

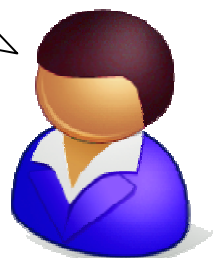


La certification,
ça coûte de
l'argent

Je n'ai pas
de budget
pour ça

Mes équipes
sont sur
d'autres
projets

J'ai des
missions plus
stratégiques



Pas besoin
de prouver
quoi que ce
soit !

Je n'ai
pas de
clients

Un SMSI,
c'est
suffisant

Les méthodes
sont en place,
c'est ça
l'important



Et pourtant les avantages sont là !

Fort gain d'image vers l'extérieur



- Validation des processus de sécurité
 - Qualité de l'organisation existante
 - Gage de maintenance/amélioration



Preuve

- Souvent demandé dans les appels d'offres de services
 - En particulier pour les grands comptes



Approbation

- Avantage concurrentiel
 - Peu d'entreprises certifiées



Avantage

Une très utile validation en interne a) vis à vis de la hiérarchie



- Nécessaire besoin d'une politique de sécurité
 - SMSI obligatoire



Sécurité

- Apporte de la crédibilité dans la politique de sécurité
 - Montre qu'elle est bien menée



Crédibilité

- Permet d'obliger certains à suivre
 - « fait accompli »



Facilité

Une très utile validation en interne a) vis à vis de ses équipes



- Optimise l'efficacité du SMSI, car obligation de
 - Résultat : une fois la certification lancée, il fait réussir
 - Maintenance : une fois la certification obtenue, il faut la garder



Efficacité



Pérennité

- Justification du changement
 - Excellent prétexte à des changements qui seraient difficiles sans l'objectif de la certification



Utilité

- Opportunité d'implication et de progression des équipes



Motivation

- Concrétisation du résultat



Fierté

Le coût marginal reste faible



- Le coût réel est lié à l'étude et l'implémentation du SMSI
 - Le coût financier supplémentaire pour la certification reste faible
 - Il en est de même pour le coût en ressources
 - Le tout dans un processus cadré et contrôlé



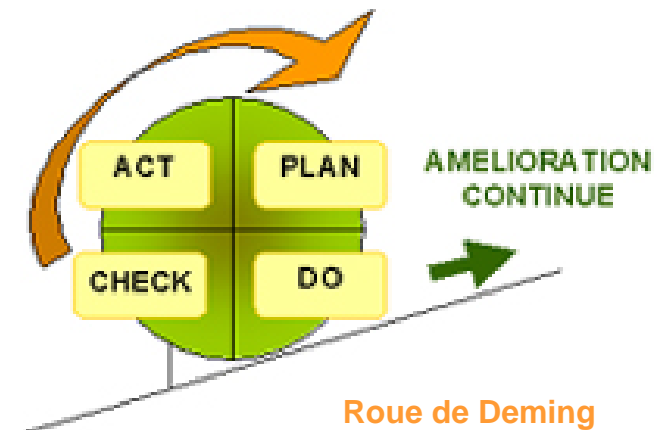
- En revanche, la certification permet d'éviter l'accumulation des audits externes
 - Très consommateurs en ressources
 - Le plus souvent au moment où celles-ci sont très occupées

Retour d'expérience

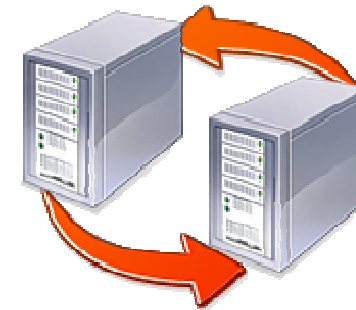
a) pourquoi?



- TelecityGroup opère des centres d'hébergement (datacenters)
 - Hébergement d'infrastructures informatiques
 - Services à Valeur Ajoutée (connectivité, sauvegarde, stockage, ...)
 - 20 sites en Europe (+2 futurs sites annoncés, dont 1 à Paris)
 - 2 sites à Paris (objets de la certification, après 7 autres en Europe) - 35 salariés
- Pourquoi un SMSI ?
 - **Plan** : S'engager, Planifier
 - **Do** : Réaliser, mettre en œuvre
 - **Check** : Vérifier, évaluer
 - **Act** : Agir, réagir, revoir
- Pourquoi aller de SMSI à certification ?
 - Image de marque
 - Facilité pour les Clients
 - « Formalisation du SMSI »



- Travaux de préparation (démarche dupliquée après 7 autres sites certifiés)
 - 4 mois intenses et au moins 100 jours/homme
 - Avoir anticipé au préalable
 - Nommer un chef de projet
 - Tous les Départements impliqués (Opérations, SI, RH, Commercial,...)
 - Confidentialité
 - Intégrité
 - Disponibilité
 - Grands Axes:
 - Mise en conformité des procédures
 - Identification des risques
 - Elaboration du plan de traitement des risques



Retour d'expérience

b) comment? ii) Certification



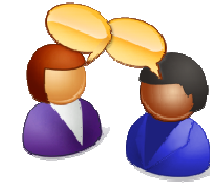
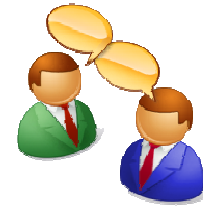
- Audit de certification (sur deux sites en deux jours)
 - Savoir communiquer avec l'auditeur
 - Ne pas se dire que l'Auditeur est là pour piéger, de toute façon il ne faut pas mentir
 - Tout doit être documenté car il va vérifier
 - Se souvenir qu'il ne juge pas la présence de risques, mais leur maîtrise
 - Bien tout expliquer (ce qu'on a fait, ce qu'on fait, ce qu'on va faire)
 - Vision du management est importante
 - Implication nécessaire de l'ensemble du personnel
- Après la certification
 - Informer en interne
 - S'assurer de la continuité des processus
 - Étape suivante: PCI DSS (Payment Card Industry Data Security Standard)



Retour d'expérience c) avec qui?



- Préparation
 - Tout le monde a été informé...
 - ... et impliqué (affectation projets)



- Audit préliminaires
 - Internes par spécialistes sécurité venant de notre maison-mère anglaise, ayant déjà participé à la certification de 7 autres sites: UK, Allemagne, Pays-Bas, Suède.
 - Sans eux, le projet aurait probablement pris 2 fois plus de ressources (temps, hommes, argent)

- Certificateur
 - Lloyd's Register Quality Assurance



Questions ?



Merci de votre attention

A votre disposition, si je peux aider:

stephane.duproz@telecity.com