

Les visages
de la sécurité
Au-delà des apparences



Conférences
Expositions



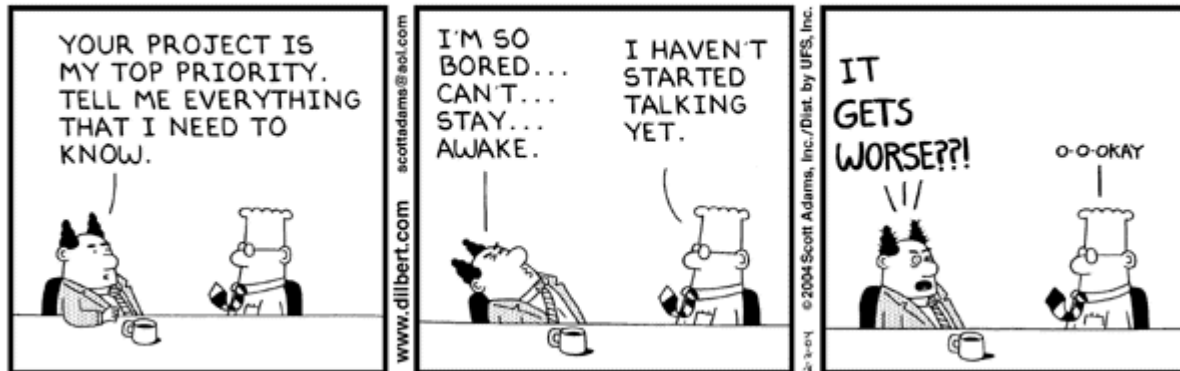
RSI 2010

Rendez-vous de la **sécurité**
de **l'information**

PROCESSUS DE CERTIFICATION ISO 27001 : UN CAS VÉCU PAR GARDIEN VIRTUEL

Dilbert

by Scott Adams

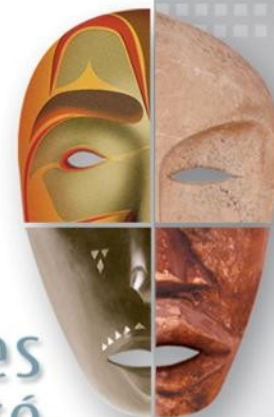


© UFS, Inc.



Qui est Gardien Virtuel?

- Entreprise de services-conseils spécialisée dans la sécurité de l'information.
- Mission: Augmenter la confidentialité, l'intégrité et la disponibilité de vos systèmes d'information.
- Bureau chef situé à Laval.
- 20 employés dont 8 au département de R&D
- Président : Patrick Boucher, CISSP, CEH, CISA, CGEIT et ITIL. M. Boucher possède au-delà de 15 années d'expérience en sécurité.



La gouvernance c'est...

- Assurer que la direction dans laquelle nous allons est celle que nous souhaitons!
- Comment savoir que nous arrivons à destination sans l'avoir préalablement défini?
- Voici des synonymes: Gouverner, Gérer, Organiser, Diriger, Encadrer, Encourager

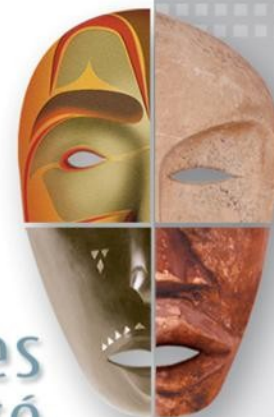
Connaissez-vous cet adage?

« La vie laisse passer les gens qui savent où ils vont »



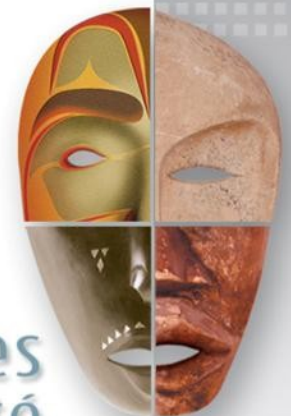
Quiz: Devinez l'ISO!

- ISO 27001
 - Exigences pour les SMSI
- ISO 27002
 - Guides des pratiques (objectifs et recommandations)
- ISO 27003
 - Implantation du SMSI
- ISO 27004
 - Guide de métrique; méthode pour mesurer les critères d'efficacité
- ISO 27005
 - Guide pour la gestion du risque
- ISO 27006
 - Guide pour les auditeurs et certification
- ISO 27007
 - Guide des audits SMSI
- ISO 27799
 - Directives pour utilisation dans le secteur de la santé



Clauses obligatoires de l'ISO 27001

- Clause 4 – SMSI
 - Clause 4.2.1 : Mise en place
 - Clause 4.2.2 : Implantation et opération
 - Clause 4.2.3 : Contrôle et revue
 - Clause 4.2.4 : Maintien et améliorations
- Clause 5 – Responsabilités de la direction
- Clause 6 – Audit interne
- Clause 7 – Revue de direction du SMSI
- Clause 8 – Amélioration continue



Structure de la norme ISO 27002

- **Thèmes** : 11
- **Objectifs** : 39
- **Mesures** : 133
- **Préconisations** : 737



Voyons un exemple concret ensemble...



Un exemple sorti du 27002

- **Thèmes (11):**
 - A9. Sécurité physique et environnementale
- **Objectifs (39):**
 - A9.2. Sécurité du matériel: Empêcher la perte, l'endommagement, le vol ou la compromission des biens et l'interruption des activités de l'organisme.
- **Mesures (133):**
 - A9.2.3. Sécurité du câblage: Protéger les câbles électriques, ou de télécommunication transportant des données, contre toute interception ou dommage.
- **Préconisation (737):**
 - A) Enterrer les câbles si possible
 - B) Éviter qu'ils traversent des zones publiques...
 - C) Séparer les câbles électriques de ceux de télécommunication
 - Etc.



PDCA – 9001 vs. 27001 vs. 14001

- PDCA = Plan, Do, Check, Act → Planifier, Déployer, Contrôler, Agir
- Tous les ISO comptent sur l'amélioration continue du « système »
- ISO 9001 – Système de gestion de la qualité
- ISO 27001 – Système de gestion de la sécurité
- ISO 14001 – Système de gestion de l'environnement



Notre cas vécu : le processus

- Il y a SIX étapes principales :
 - Planification
 - Déploiement
 - Contrôle
 - Action
 - Certification
 - Maintien



Étape 1: La planification

- Nous avons commencé par la lecture de TOUS les documents
- Définition des rôles et responsabilités
- État des lieux – Entreprise en SI avec des bonnes pratiques et procédures déjà en place
- Analyse des écarts – Plusieurs documents et validations manquantes
- Création de la déclaration d'applicabilité du ISO 27002



Étape 1: La planification (suite)

- Simplement commencer – par étapes!
- Gardez en tête l'amélioration continue
- Notre PCA avait 5 lignes ainsi qu'un simple guide d'installation
- Rassurez-vous! Maintenant, redondance à plusieurs sites et documentation complète.



Étape 2: Le déploiement

- Mise en oeuvre de:
 - Gestion des incidents
 - Maîtrise des documents
 - Formation et sensibilisation
 - Gestion du changement
 - Plusieurs autres nouveaux processus – Documenter ce qu'on fait est un nouveau concept pour plusieurs (des heures et des heures de plaisir!!)



Étape 2: Le déploiement (suite)

- Les consultants en sécurité vont vouloir faire les choses « trop parfaitement » :
 - C'est trop!
- Le responsable de la mise en place veut bien faire son travail :
 - C'est beaucoup de pression!
- L'important est d'avoir un plan, de mettre des efforts pour le faire progresser et de conserver les preuves de ces efforts.



Étape 2: Le déploiement (suite)

- Lors de notre déploiement, nous avons constaté que :
 - Des éléments de notre politique n'étaient pas clairs
 - Notre gestion documentaire posait problème
 - La gestion des actifs est plus facile à dire qu'à faire



Étape 3: Le contrôle

- Le 30 décembre à 3hrs du matin, notre auditeur travaillait encore afin de remettre son plan avant la fin de l'année!
- L'objectif de l'année 1 est de mettre en place le système et de le faire valider par la firme responsable (ici, la firme SGS S.A.)
- À l'année 2, nous avons amélioré les pratiques et automatisé le plus d'éléments possibles (rapport des KPI)
- Pour la prochaine année, nous envisageons bien améliorer la formation fournie aux nouveaux employés.



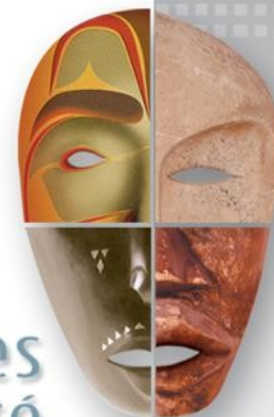
Étape 4: L'action

- Amélioration continue – découvrir et traiter les non-conformités
- Importance de la segmentation des tâches :
 - Même pour une petite équipe à l'époque, ce fut très bénéfique d'avoir une bonne segmentation des tâches
 - *Challenge* entre les membres
 - La bonne personne pour le bon poste a permis de réduire le temps requis de mise en œuvre



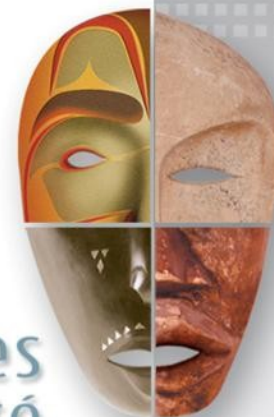
Étape 4: L'action (suite)

- La clé? L'implication de la direction!
- L'auditeur interne valide la mise en place et écrit ses recommandations
- Le comité d'implantation cherche à satisfaire « tout le monde »
- Belle collaboration, aucun conflit, pas (trop) de problèmes d'égo ou de gestion des changements pour nous <OUF!>
 - Implication de chaque membre de l'équipe!



Étape 5: La certification

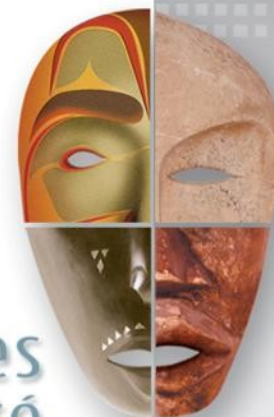
- Choix d'un organisme – expertise ISO 27001 limitée
 - SGS S.A. est une firme suisse basée au Québec pouvant communiquer en français
- Préparation des documents pour l'audit documentaire
 - N'oubliez pas la maîtrise documentaire!
- Audit sur place
 - Grand dérangement et haut niveau de stress du comité d'implantation



Étape 6: Le maintien

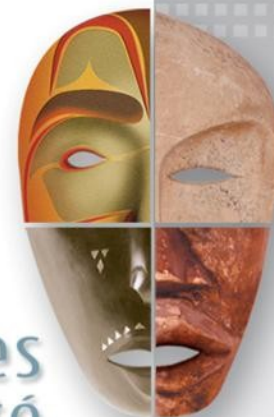
- Pièges à éviter :
 - Si changement de personnel
 - Calendrier sans dates fixes
 - Procédures non-utilisées des gens

- **Un système qui n'est pas adopté par les employés ne survivra pas!**



Étape 6: Le maintien (suite)

- Trucs qui ont fonctionné pour nous :
 - Avoir un endroit central pour les dernières versions des documents
 - Clairement définir les critères de la portée
 - Ne pas laisser de questions sans réponses
 - Participer en tant que gestionnaire et pas seulement « prendre le contrôle »



Les coûts et les délais

- AVANT : septembre 2008
 - GVI possède déjà un bon processus de sécurité
 - Formation ISO 27001 suivie par tous
- PENDANT
 - Mise à contribution de tous les membres de l'équipe
 - Rencontres de coordination régulières
- APRÈS : mars 2009 et +
 - Audit de la SGS S.A.
 - Réception du certificat ISO 27001



Les coûts et les délais (suite)

- Formation: 5,000 \$
 - Salaires des employés affectés au projet: 25,000 \$
 - Certification officielle: 15,000 \$
 - Amélioration de sécurité: 5,000 \$
- TOTAL: 50,000 \$



Les retombées (suite)

- Confiance accrue des clients
- Nous aide à atteindre un degré de maturité plus élevé
- Nous aide à être organisés et plus structurés
- Plus grande confiance envers nous-mêmes
- Être la première firme services-conseils en SI au Canada à générer beaucoup de demandes pour nos services
- Le gouvernement suivra-t-il en ajoutant ce pré-requis à ses appels d'offres comme il l'a fait pour l'ISO 9001 à l'époque?



Questions?



Merci!

- Gardien Virtuel vient de déménager : Prenez note de nos nouvelles coordonnées...



1565, Boul. de l'Avenir, Bureau 110,
Laval, QC, H7S 2N5

Téléphone: 450-933-7774

Courriel: info@gardienvirtuel.ca

URL: www.gardienvirtuel.ca

