

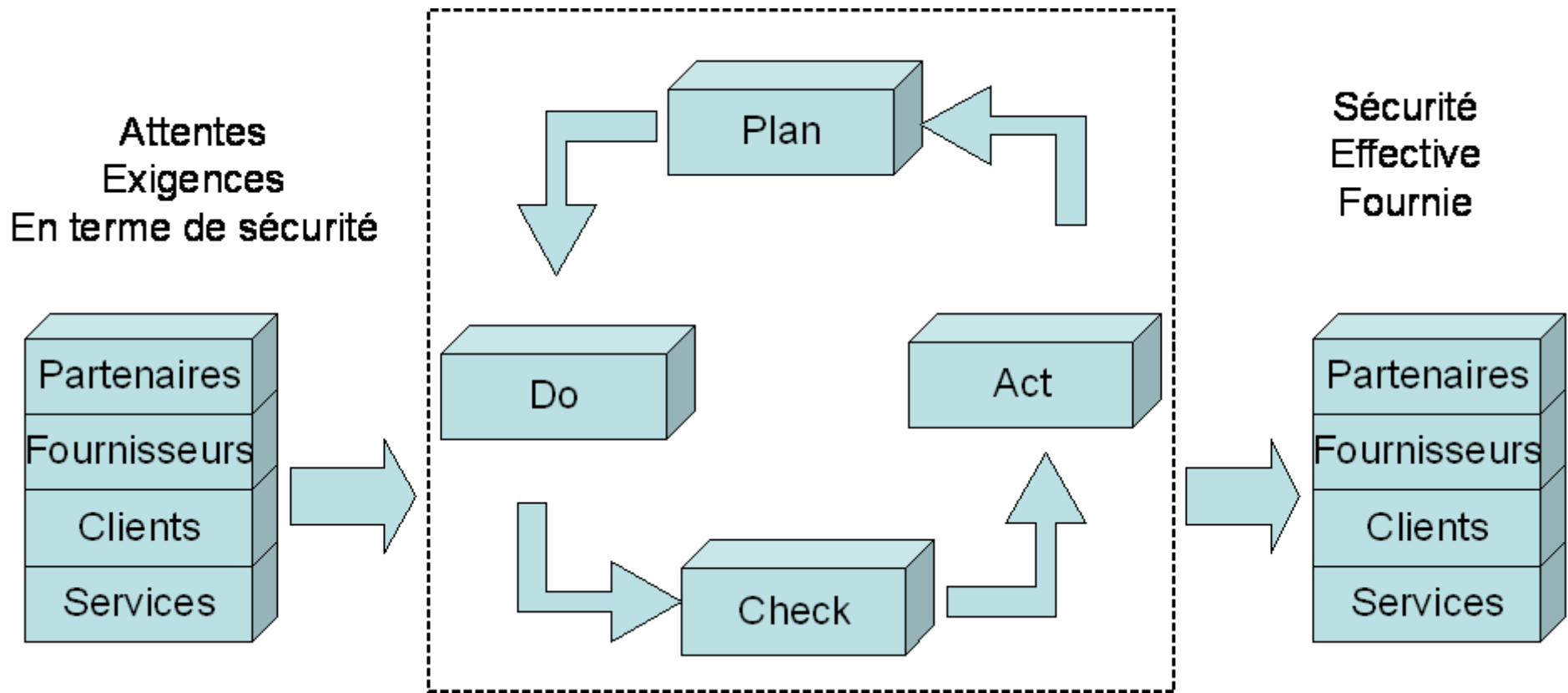


Comment choisir les indicateurs ISO 27001

Alexandre Fernandez
<Alexandre.Fernandez@hsc.fr>

ISO 27001

Système de Management de la Sécurité de l'Information



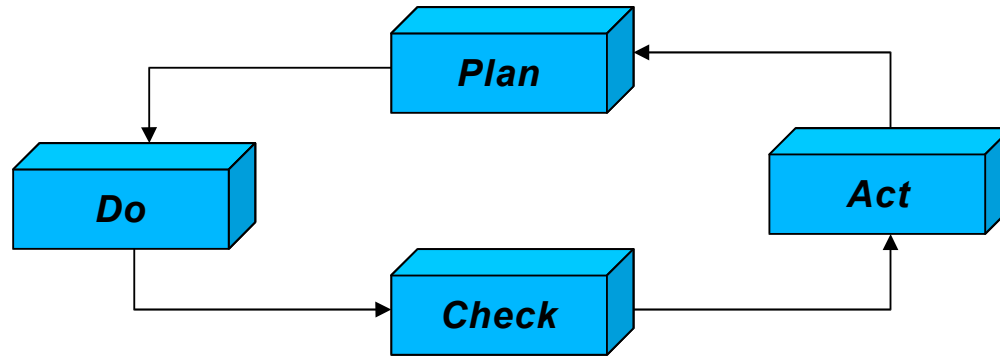
- ISO 17799
 - Catalogue de mesures de sécurité
 - Politique de sécurité
 - Organisation de la sécurité de l'information
 - Gestion des biens
 - Sécurité des ressources humaines
 - Sécurité physique
 - Procédures opérationnelles et communication
 - Contrôle d'accès
 - Acquisition, développement et maintenance de systèmes d'information
 - Gestion des incidents de sécurité
 - Plan de continuité de l'activité
 - Conformité aux réglementations

- Apports du tandem ISO 27001 + ISO 17799
 - Adopter de bonnes pratiques
 - Montrer pattes blanches aux parties prenantes
 - Certification ISO 27001

- Indicateurs
 - Sous-entendus dans la norme BS 7799-2:2002
 - Explicites dans l'ISO 27001
 - La norme ISO 27001 insiste sur l'importance des indicateurs
 - 4.2.2 d)
 - 4.2.3 4)
 - 7.2 f)

- Pourquoi faire?
 - Identifier les écarts
 - Spécifié / Constaté
 - Mesurer l'efficacité du SMSI
 - Comparer différents services / succursales / BU / etc...
 - Communiquer
 - Piloter
 - Déclencher des actions
 - Sur franchissement de seuil
- Ne sert pas à mesurer le niveau de sécurité de l'entreprise

- Quelques idées reçues
 - Indicateurs servent à comparer plusieurs SMSI : **faux**
 - Indicateurs sont un standard : **faux**
- Quelques précisions
 - Indicateurs spécifiques à chaque organisme
 - Pas deux entreprises avec les mêmes indicateurs



- SMSI \Rightarrow modèle PDCA \Rightarrow Mesures de sécurité
- Donc, contrôler l'efficacité d'un SMSI revient à
 - Contrôler l'efficacité du modèle PDCA
 - Qui revient à contrôler l'efficacité des mesures de sécurité mises en oeuvre

- Pour chaque mesure de sécurité du SMSI
 - Répondre **systematiquement** à trois questions **fondamentales** :
- Première question
 - Quel fait
 - Concret
 - Mesurable
 - Si possible vérifiable
 - Permettra de savoir si la mesure de sécurité est
 - Appliquée
 - Efficace

- Deuxième question
 - Ce fait est-il mesurable **facilement** ?
- Troisième question
 - Comment obtenir **concrètement** la mesure ?
- Pour trouver un indicateur, il faut avoir répondu aux trois questions

- Les indicateurs ne doivent concerner que les mesures de sécurité mises en oeuvre dans le SMSI
- Chercher au moins un indicateur par mesure de sécurité mise en oeuvre dans le SMSI
- Ne pas s'obstiner si aucun indicateur n'est trouvé
 - Pas d'indicateur est préférable à un indicateur inapproprié
 - Travail inutile, coût, mauvaise perception du SMSI

- Erreurs à éviter
 - Indicateur ne correspondant pas à une mesure de sécurité du SMSI
 - Indicateur ne mesurant pas l'efficacité d'une mesure de sécurité du SMSI
 - Indicateur sélectionné sans réflexion préalable
 - Récupération d'informations de rapports déjà existants
 - Recopie d'indicateurs trouvés sur Internet ou ceux utilisés dans une autre société, prise en exemple

- Des réservoirs d'indicateurs sont découverts lors de l'identification des indicateurs
- Réservoir d'indicateur
 - Entité qui fournit une partie importante des indicateurs
 - Service, personne, application, etc
- Exemples
 - Ressources humaines; RSSI; DSI
 - Rapports du support ou *helpdesk*
 - Logiciel antivirus
 - Système de gestion des données de sécurité (journaux systèmes et applicatifs)

- Raison d'être des indicateurs
 - Donner une image **fiable** de l'efficacité et de l'adéquation du SMSI
- **Fiabilité** vient du latin *fides*, qui veut dire **confiance**, donc
 - La fiabilité de l'image que l'on a du SMSI dépend de la confiance que l'on a sur les indicateurs
 - Pour faire confiance au SMSI, il faut faire confiance aux indicateurs
- Conséquence
 - La confiance que l'on a sur les indicateurs est un point clé dans le SMSI

- Risques portant sur les indicateurs
 - Choix : Un indicateur mal choisi ne donne pas une image fiable du SMSI
 - Retard : Il se peut que les gens oublient de :
 - Fournir l'indicateur
 - Plus grave : comptabiliser les éléments qui permettent de produire l'indicateur
 - Erreur accidentelle : dans la saisie, dans un programme
 - Erreur volontaire : pour cacher un fait gênant, voire compromettant

- Comment réduire ces risques ?
 - En automatisant le plus possible la récupération des informations
 - Très difficile
 - Impossible pour de nombreux indicateurs
 - En limitant le plus possible les indicateurs binaires
 - Remplacer les oui/non par des fractions
 - Pas toujours possible
 - En faisant en sorte que numérateur et dénominateur soient remplis par des entités différentes (*segregation of duties*)

- Cumuls ou nombres issus d'un comptage
 - Garder une trace des évènements au fur et à mesure de leur occurrence
 - Par exemple, remplir un formulaire
 - Peut impliquer l'utilisation d'outils
 - Paramétrage d'outils
 - Maintenance évolutive des outils
 - Développement spécifique de certains outils
 - Il faut pouvoir rejouer la génération de l'indicateur

- Pourcentages
 - État d'avancement des actions correctives
 - Proportion de personnes satisfaites ou très satisfaites d'une formation
- Date de révision ou de mise à jour, date d'audit
- Binaire
 - L'audit signalait-il la nécessité d'entreprendre des actions correctives ?
 - Les actions correctives ont-elles été bien faites ?

Exemple de *mauvais* indicateurs

- Binaire
 - Exemple : est-ce que le travail est bien fait (oui/non)
- Fraction ne respectant pas la séparation des rôles (*segregation of duties*)
- Indicateur impossible à trouver
 - Exemple : nombre total d'incidents de sécurité
- Indicateur difficile à obtenir
 - Exemple : coût de la perte de disponibilité

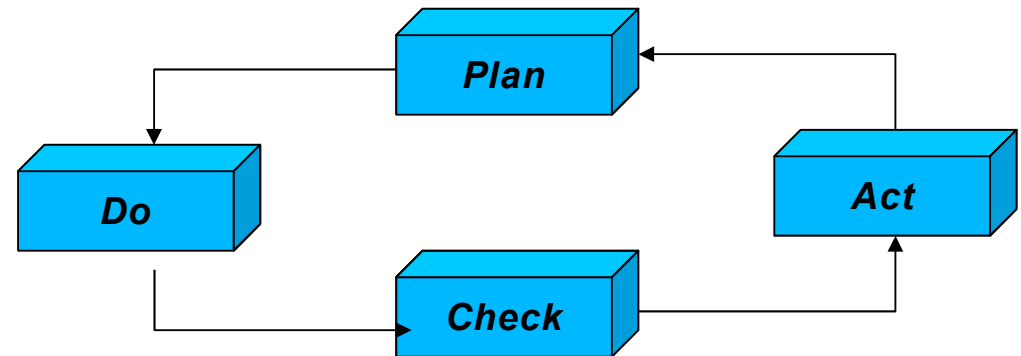
- Vecteur : moyen par lequel le responsable de l'indicateur le transmet au responsable de la consolidation
- Différents types de vecteurs
 - Automatiques
 - Manuels
 - Courriel, formulaire web, formulaire papier
- Différentes formes
 - QCM
 - Tableau Excel
- Les vecteurs doivent être auditables
 - Datés
 - Stockés

- Visualisation synthétique rapide
 - Pour le RSSI
 - Pour le top management
 - Pour le middle-management
 - Pour les actionnaires
 - Pour les auditeurs
- Sensibilisation et aide à la décision
- Conformité SAS 70, Bâle II, ...
- Indicateurs publiés sous la forme de **tableaux de bord**

- Quand
 - A chaque changement important du SMSI
 - A défaut, périodiquement
- Pertinence des indicateurs
 - Vérifier que l'indicateur est en relation avec l'objectif de la mesure de sécurité
 - Valider les éléments qui ont conduit à utiliser tel indicateur sur telle mesure de sécurité
- Cohérence des indicateurs
 - Vérifier la cohérence des indicateurs entre eux

- Fiabilité des indicateurs
 - Reprendre les données ou éléments ayant permis la construction de l'indicateur et le recalculer
 - Valider la façon dont les indicateurs sont obtenus
 - Les procédures sont-elles effectuées correctement ?
 - Aux dates prévues ?
 - Où sont les traces ?

- Phase 1 : Choisir les indicateurs
- Phase 2 : Identifier la source de chaque indicateur
- Phase 3 : Obtenir les indicateurs
- Phase 4 : Transmettre les indicateurs
- Phase 5 : Consolider les indicateurs
- Phase 6 : Utiliser les indicateurs
- Phase 7 : Auditer les indicateurs
- Phase 8 : Agir en conséquence



- Les indicateurs sont indispensables au SMSI
- Leur choix doit faire l'objet d'une réflexion, de pragmatisme et d'une amélioration constante
 - Avoir des indicateurs pour toutes ses mesures de sécurité n'est généralement pas possible
 - Choisir les bons indicateurs est généralement impossible du premier coup
- Le chantier reste ouvert
- La norme 27004 est annoncée