ISO 27004

Information security management Measurements

Métrage et métriques d'un SMSI

Brouillon n°3 du 7 janvier 2006

Clusif
Groupe de travail ISO27000
21 avril 2006

Hervé Schauer
<Herve.Schauer@hsc.fr>

Sommaire

- Introduction
- Vocabulaire
- Métrage dans le SMSI
- Modèle de sécurité de l'information du métrage
- Métrage du modèle de sécurité de l'information
- Conclusion

Introduction

- Norme ISO 27001 insiste sur l'importance
  - Des mesures : 0.2 d) ; 4.2.2 d) ; 4.2.3 c) ; 4.3.1 g) ; 7.2 f) : 7.3 e)
    - *Measures, measurement*
  - Des indicateurs : 4.2.3 a) 4)
- Phase Check du PDCA
  - Mesure de performance du SMSI : 0.2 ; 4.2.3 b) ; 4.2.3 c)
- Titre du document : *Information security management - measurements*
- Noir : ce qui vient de la norme
- Rouge : la référence dans la norme ISO27004
- Gris : ce qui vient de moi

Vocabulaire

- **Attribut** *Attribute* 3.1 ISO 15939 : *Software Measurement Process*
  - Propriété ou caractéristique d'une **entité**
  - Distinguée quantitativement ou qualitativement
  - Par des moyens humains ou automatiques
- **Entité** *Entity* 3.7 ISO 15939
  - Objet devant être défini par le métrage (la mesure) de ses **attributs**
  - Tangible ou intangible
    - Définitions d'attribut et d'entité se mordent la queue

Vocabulaire

- **Metrique** ou **Unité** *Measure* 3.13 ISO 15939
  - Variable à laquelle une valeur est assignée
    - Variable et pas attribut
- **Metrique de base** ou **Unité de base** *Base measure* 3.2 ISO 15939
  - Type de métrique et échelle pour mesurer un attribut
- **Métrique combinée ou dérivée** *Derived measure* 3.4 ISO 15939
  - Une métrique définie par une fonction de plusieurs métriques de base

Vocabulaire

- **Métrage** ou **Capacité** ou **Mesurage** *Measurement* 3.15
  - Ce qui permet d'obtenir la valeur d'un attribut d'une entité en utilisant un type de métrique
    - Evaluation ou estimation d'un attribut
    - Metrage = le fait de mesurer, Mesurage = *measuring*
- **Type** ou **classe de métrage** *Form of measurement* 3.8
  - Ensemble d'opérations pour déterminer la valeur du métrage
    - Méthode de mesure
    - Fonction de calcul
    - Modèle analytique
- **Indicateur** *Information security indicator* 3.10
  - Ajout d'un critère d'interprétation au métrage
  - Note : Evaluation ou estimation d'un attribut

Vocabulaire

- **Méthode de métrage** *measurement method* 3.17
  - Séquence logique d'opérations exprimées génériquement pour entreprendre la description du métrage
- **Unité de métrage** ou **de mesure** *unit of measurement* 3.21
  - Quantité particulière, définie et adoptée par convention, avec laquelle les autres quantités de même nature sont comparées pour exprimer la magnitude relative à cette quantité
    - Etalon de référence pour faire des mesures
- *Metrics* **metriques**
  - Jamais utilisé dans la partie normative du document
    - Sauf dans la figure au 5.1 : *attribute* ➔ *measure* ➔ *metric* ➔ *indicator*
  - Utilisé sans arrêt dans les annexes informatives
  - Pas défini dans le document

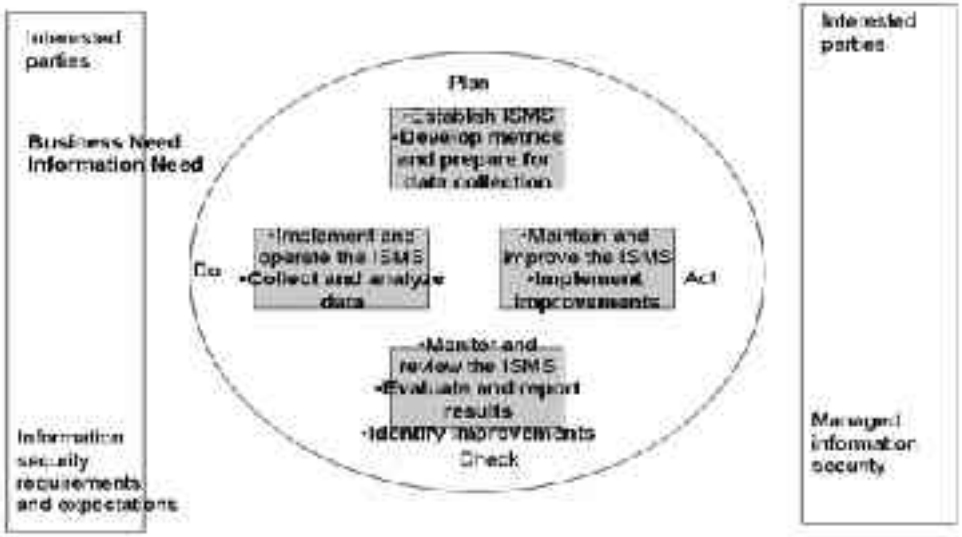
Métrage dans le SMSI

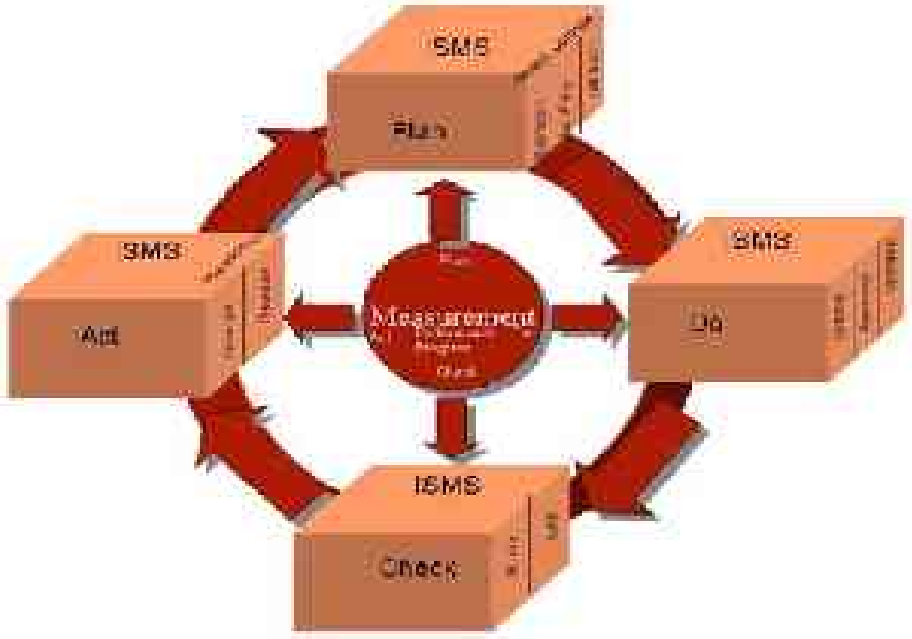
- Objectifs 4)
  - Evaluer l'efficacité de mise en oeuvre des mesure de sécurité
  - Evaluer le SMSI et son amélioration permanente
  - Fournir un état pour guider les revues du management, faciliter les améliorations, et fournir des traces pour les audits
  - Communiquer sur l'importance de la sécurité en interne
  - Servir à l'analyse de risque et au traitement du risque

Métrage dans le SMSI

- Par rapport au PDCA 4)
- Plan
  - 4.2.2.d) Définir comment mesurer l'efficacité des mesures de sécurité
- Do et Check
  - 4.2.3.c) Evaluer l'efficacité des mesure de sécurité
- Act
  - 4.3.1.g) Décrire comment évaluer l'efficacité des mesures de sécurité
- Plusieurs propositions dans la norme pour clarifier cet aspect
  - Schémas difficilement lisibles
  - A réintégrer dans une mise à jour de l'ISO 27001 pour rester cohérent

Métrage dans le SMSI



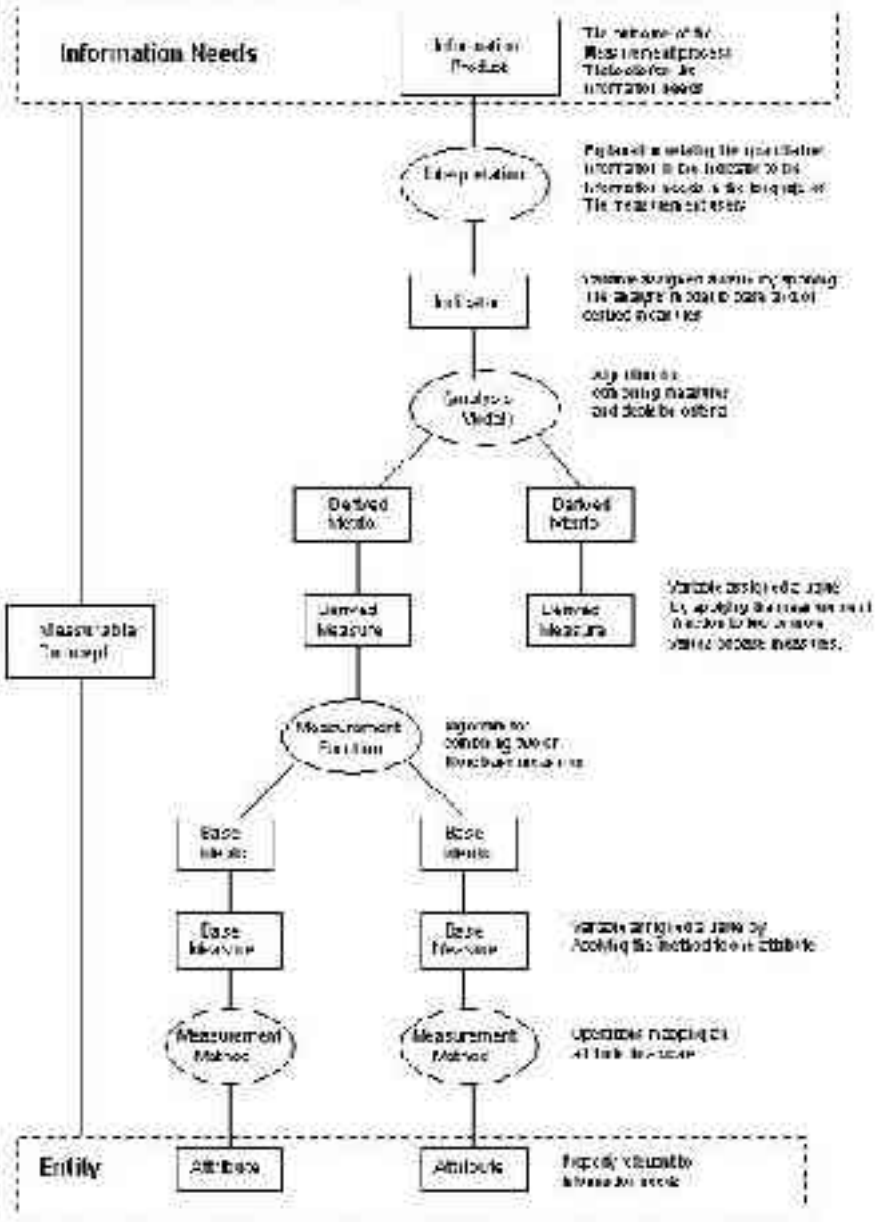


Modèle de sécurité du métrage

- Modèle de sécurité de l'information (ISM) du métrage 5.1
  - Identifier les attributs
  - Sélectionner les attributs
  - En déduire des indicateurs
- Identifier la méthode 5.2
  - d'obtention des attributs
- Identifier la fréquence 5.3
- Document très détaillé sur des exemples génériques
- Manque de méthode opérationelle
- Ne pas confondre *ISMS* avec *MISM* : *Measurements Information Security Model* et ISMM : *Information Security Model Measurement* utilisés dans la suite du document

Modèle de sécurité du métrage

- Trois types de métriques (*measures*) : 5.1
  - Métrique de base (*base measure*)
  - Métrique combinée (d*erived measure*)
  - Indicateur (*indicator*)



Métrages du modèle de sécurité

- Définition et sélection des métrages du SMSI 6
  - Indicateurs devront être analysés (*assessed*)
  - Etapes du métrage du SMSI
    - Processus de définition
    - Développement des métrage applicables
    - Implémentation du programme de métrage
    - Révision des métrages
- Types de métrage du SMSI 6.1
  - Métrage de performance (*performance measurements*) : efficacité
  - Métrage de progrès (*progress measurements*) : changements dans la protection de l'information

Métrages du modèle de sécurité

- Métrage du modèle de sécurité de l'information dans la phase *Plan* 6.2
- Critères de validation du métrage de l'ISM 6.2.1
- Sélection des métrages de l'ISM 6.2.2
  - SoA (du SMSI ?) doit contenir
    - Objectifs des indicateurs
    - Métrage du modèle de sécurité de l'information
    - Raison de leur sélection
  - Pas dit dans l'ISO27001, SoA pas défini
- Identifier les objets à mesurer 6.2.3
  - Objet (*object*) pas défini et sert à définir entité (*entity*)
  - *business objects*

Métrage du modèle de sécurité

- Identifier le critère 6.2.4
  - Identifier le critère d'identification de l'objet
  - Métrage donne une valeur qui réprésente un attribut de l'objet
  - Critère : comme un mètre-étalon (*yardstick*) utilisé pour mesurer la longueur
    - Pas de référence à unité de métrage défini au début
- Identifier, selectionner et documenter le métrage de l'ISM 6.2.5
- Documenter le plan d'implémentation des métriques 6.2.6

Exploitation, amélioration, ...

- Exploitation des métrages du modèle de sécurité de l'information 7
- Amélioration du ISMM 8
- Engagement du management 9

Annexes

- Format des indicateurs Annex A
- Exemples de *security metrics* Annex B
- Technique de métrage à base de scénarios issus de l'analyse de risque Annex C

Conclusion

- Pas encore toujours très clair
- Pas cohérent
  - Entre paragraphes
  - Dans le vocabulaire
- Pas un document en développement de croissance
  - Assemblage de sources variées à rendre utilisables
- Etat de l'art pourrait être plus simple, plus court, et plus opérationnel ?
- Contribution ?
- Ré-écriture ?