HERVÉ SCHAUER CONSULTANTS
Cabinet de Consultants en Sécurité Informatique depuis 1989
Spécialisé sur Unix, Windows, TCP/IP et Internet

La conformité et sa dérive par rapport à la gestion des risques

Matinée CNISevent, Paris, 27 avril 2011

Hervé Schauer
<Herve.Schauer@hsc.fr>

Introduction

- Beaucoup d'organismes appliquent des mesures de sécurité à des fins de conformité
- Conformité groupe
- Questionnaires
- Auto-évaluation
- ...

- Celui qui ne ment pas est vite le plus mal noté
  - Simple..., Indicateurs faciles...

- A quoi ça rime ?

Conformité vs Gestion des risques

- Approches conformité
  - SoX
  - ISO 27002
  - ISO 27799
  - Référentiels métiers
  - Hébergeur de données de santé
  - ARJEL
  - PCI-DSS
- Approches gestion des risques
  - RGS
  - ISO 27001
  - ISO27001 + WLA

Conformité

- Législation
  - Application de la loi du 6 janvier 1978 « Informatique et libertés »
    - Personne responsable pénalement : responsable du traitement
    - Personne qui détermine les finalités et les moyens du traitement
    - Article 34 : obligation de moyens → Mettre « tous les moyens en œuvre pour garantir la sécurité »
  - Conformité à la loi pourtant pas la plus développée !
  - Manque d'appréciation des risques juridiques ?

- Législation américaine SoX
  - Interprétation fantaisiste sur la partie sécurité de l'information
  - Disproportion manifeste entre ce qui était demandé à l'un et à l'autre
  - Vache à lait des « *fat four* »

Conformité

- Norme ISO 27002
  - Sisi, en 2011 il a encore des gens qui font de la conformité ISO 27002 et dans plusieurs secteurs !
  - Normalement vocabulaire commun mais détourné pour de la conformité
  - Application de mesures de sécurité non-justifiées
  - Application de mesures de sécurité au mauvais endroit
  - Mauvaise compréhension des coûts
- Norme ISO 27799
  - Appréciation des risques largement faite pour vous
  - Mise en oeuvre de mesures de sécurité complètement disproportionnées
  - Faillite financière garantie

Conformité

- Référenciel PCI-DSS
  - Appréciation des risques faite pour vous pour les données cartes
  - Impose des dispositifs de sécurité précis et nombreux sur les données carte
    - Demeure ouvert par la possibilité de faire sa propre appréciation des risques lorsque qu'un dispositif de sécurité imposé est innapplicable
    - Mesures de sécurité compensatoires
    - A l'appréciation de l'auditeur
  - Appréciation des risques sur le reste à faire en plus
  - Sans PCI-DSS les données carte ne seraient pas protégées

Gestion des risques

- ISO 27001 impose une approche par la gestion des risques
  - Près de 20% de la norme ISO 27001 uniquement sur ce point
    - Impose de l'appréciation des risques donne des résultats comparables et reproductibles (ISO27001 4.2.1.c)
    - Impose à l'auditeur de certification ISO 27001 d'explicitement contrôler tous ces aspects de l'appréciation des risques :
      - Production par l'appréciation des risques de résultats comparables et reproductibles (ISO27006 9.2.3.2.2 a)
      - Analyse de la sécurité par rapport aux menaces pertinente (ISO27006 9.2.3.3.a)
      - Procédures d'identification, d'examen et d'évaluation reliant les menaces aux actifs, vulnérabilités et impacts cohérentes avec la politique, les objectifs et les cibles de sécurité (ISO27006 9.2.3.3.b)
    - Impose une appréciation des risques dans la durée
    - Impose à la direction générale de prendre ses responsabilités (ISO27001 5.1.f & ISO270014.2.1.h)

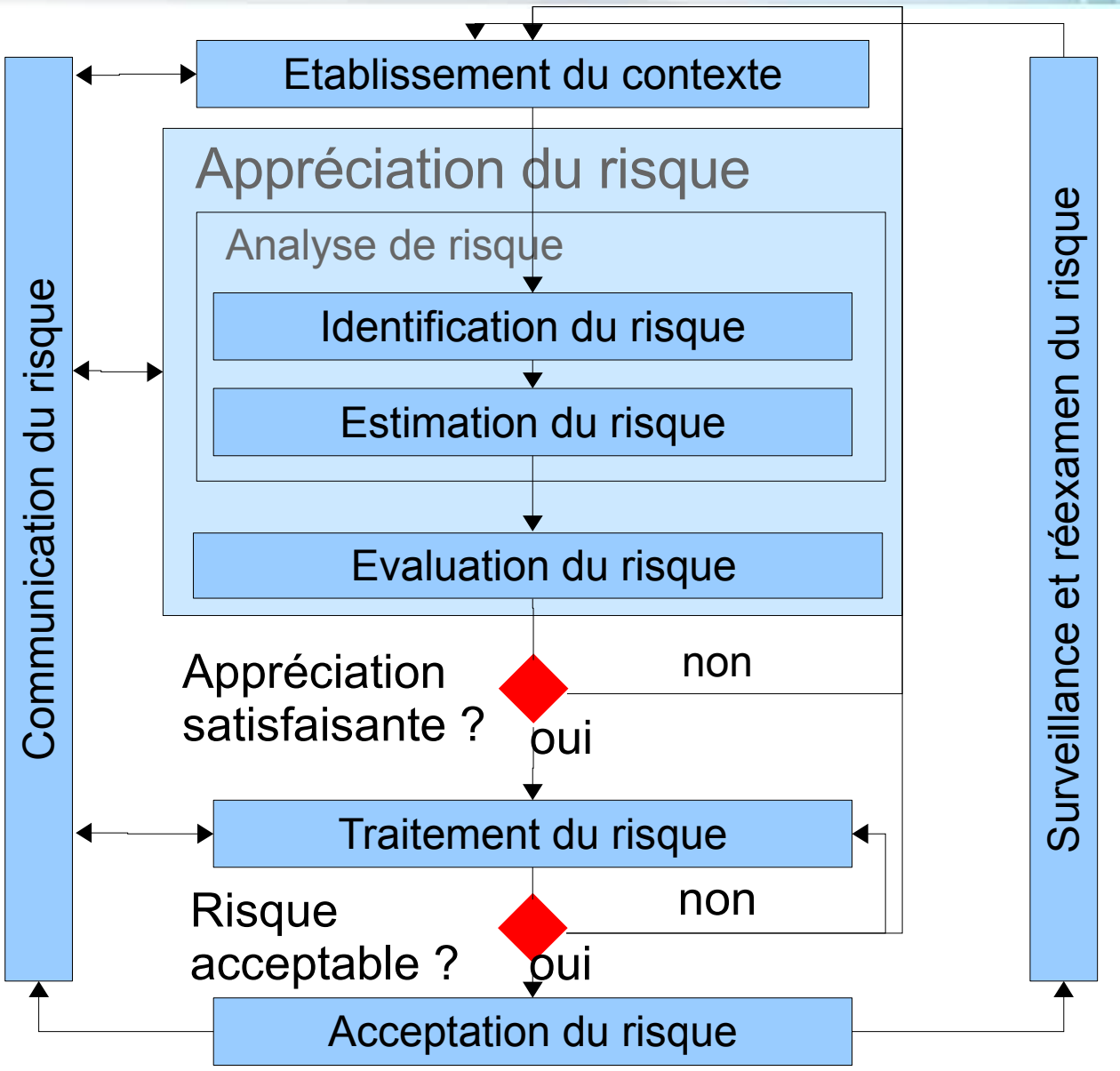
Gestion des risques

- ISO 27001 impose une approche par la gestion des risques
  - Méthode de gestion des risques détaillée dans ISO 27005
  - Du haut vers le bas
    - Processus métiers & information
    - Actifs IT, personnes, services généraux, locaux, cadre organisationnel
    - Menaces, vulnérabilités, scénarios d'incident, conséquences et impacts
    - Choix des moyens de maîtrise des risques : réduction, transfert, refus, maintien
  - Les mesures de sécurité sont sélectionnées là où elles sont le plus utiles
  - Seule manière d'expliquer et justifier les coûts
  - Evidemment, cela impose de travailler, et dans la durée
    - Le contraire du simple...

Gestion des risques ISO27005

ISO27005 Ch 6

- Processus de gestion du risque
  - Découpé en activités et sous-activités
  - Avec des entrées-sorties
  - Identique à l'ISO 31000 : norme de gestion des risques commune à tous les métiers
  - Objectif : optimiser, équilibrer, ordonnancer, responsabiliser



Intégration ISO 27005 / ISO 27001

- Hiérarchie documentaire
  - Approche descendante (*top-down*)

Périmètre et Politique du SMSI

ISO 27001 4.2.1.a, 4.2.1.b
ISO 27002 5.1.1.a, .b, .d.1, .e

Appréciation des risques

ISO 27001 4.2.1.d, 4.2.1.e
ISO 27005 8

Plan de traitement des risques

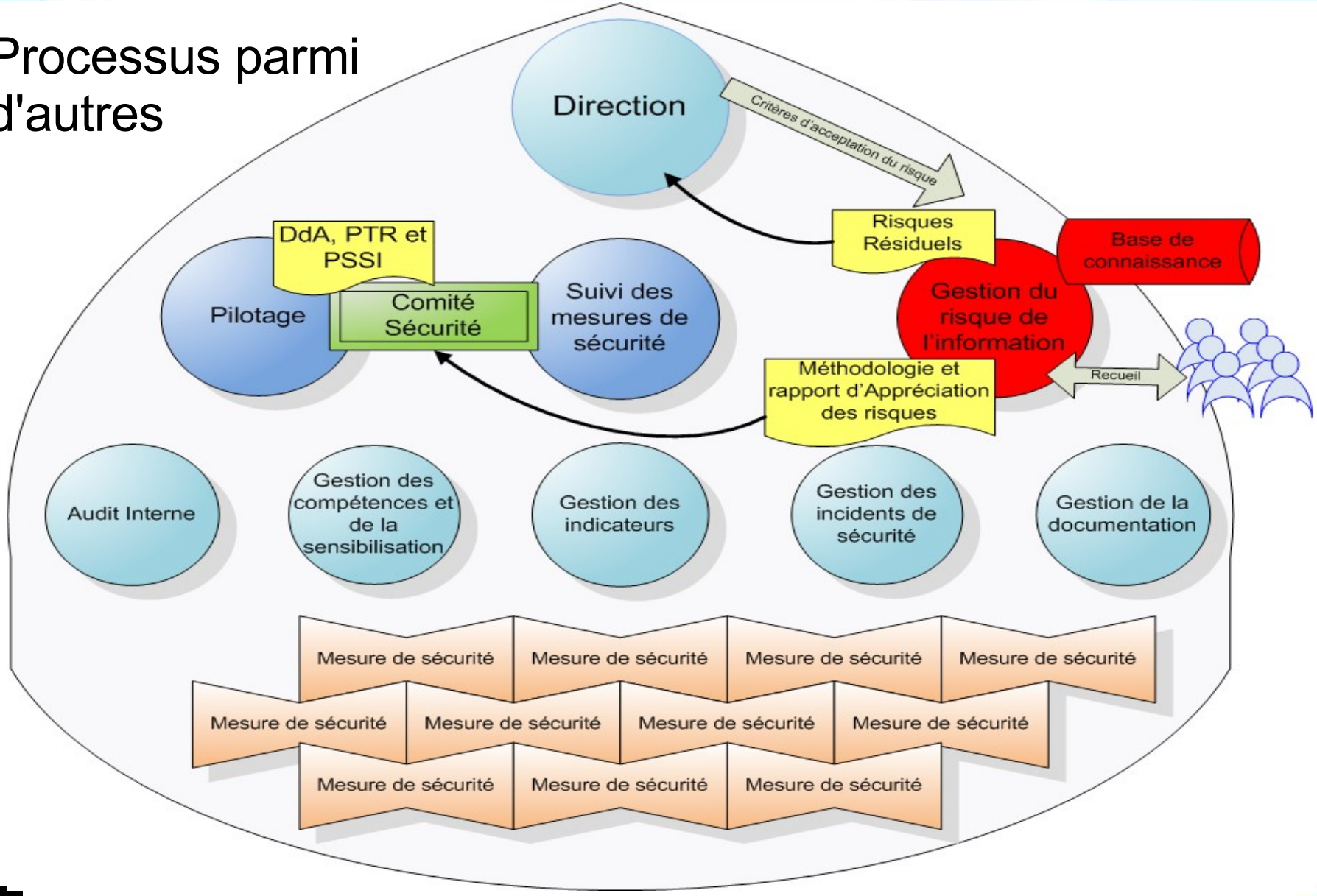
ISO 27001 4.2.1.f, 4.2.1.g
ISO 27005 9

Déclaration d'applicabilité

ISO 27001 4.2.1.j

Intégration ISO 27005 / ISO 27001

- Processus parmi d'autres



Conclusion

- Mesures de sécurité choisies par conformité
  - Exigé car façon de réduire un risque de mauvaise gestion des risques
  - Réellement indispensable dans des cas particuliers & périmètres limités
- Mesure de sécurité choisies par gestion de risque
  - Indispensable pour le cas général
  - Meilleure approche depuis 30 ans
- Toujours possible de tricher quelle que soit l'approche

Questions ?

www.hsc.fr