Cinq questions sur la vraie utilité de l'ISO 27001

Alexandre Fernandez-Toro
<Alexandre.Fernandez-Toro@hsc.fr>

Contexte

- On parle de SMSI depuis 2002
- Est-ce un effet de mode ?
- Est-ce une bulle entretenue
  - Par les fournisseurs en mal de « relais de croissance » ?
  - En interne par certains managers ?
- Pourtant
  - On en parle encore aujourd'hui
  - Des cercles extérieurs à la sécurité en parlent
- L'ISO 27001 est donc bien entrée dans les moeurs
- Alors, quelle est la réelle utilité de la norme ?
  - On commence à avoir un recul suffisant pour répondre à la question

Rappels sur l'ISO 27001

- A l'origine
  - Famille de normes relatives aux Systèmes de Management de la Sécurité de l'Information (SMSI)
  - La norme ISO 27001 est le centre de gravité
  - Issue de l'ancienne BS 7799
  - BS 7799 : B comme « British »
- Principe
  - Transposition à la sécurité de systèmes d'information des principes de la qualité ISO 9001
  - Certification possible

Rappels sur l'ISO 27001

- A la base
  - Définition d'un périmètre et d'une politique
  - Appréciation des risques
    - ISO 27005 / EBIOS / MEHARI / etc.
  - Validation par la direction
  - Sélection et implémentation des mesures de sécurité

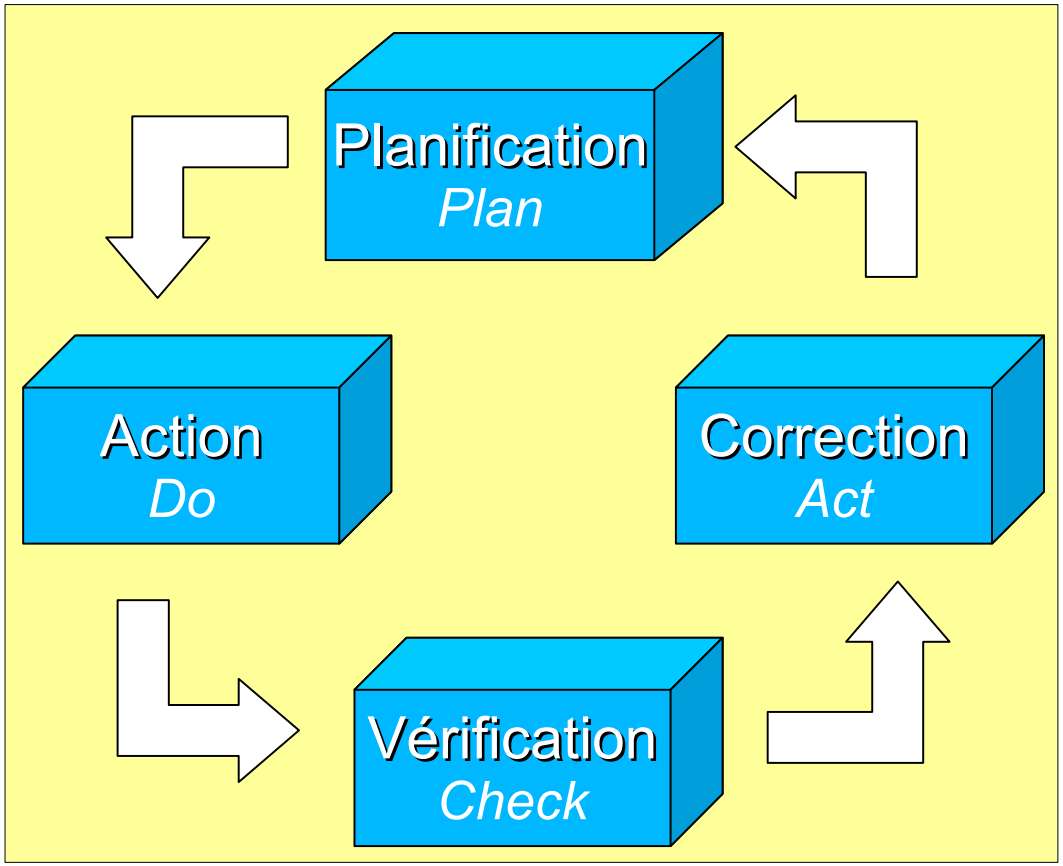
- Amélioration continue
  - Audit interne
  - Gestion des incidents
  - Suivi des actions
  - Revue de direction

Rappels sur l'ISO 27001

Attentes et exigences en terme de sécurité

- Partenaires
- Fournisseurs
- Clients
- Pouvoirs publics
- Services

Modèle **PDCA** : Plan-Do-Check-Act

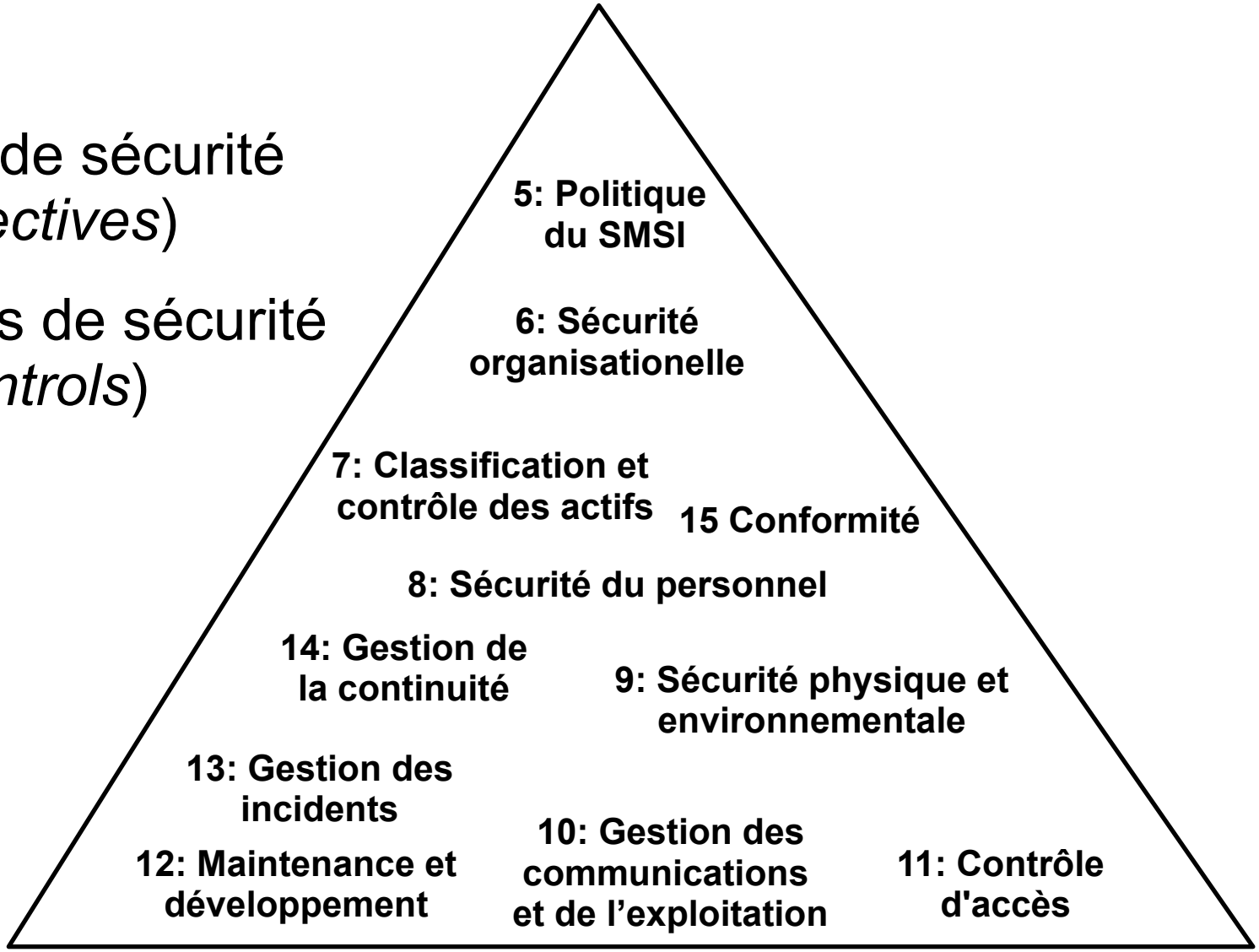


Sécurité effective fournie

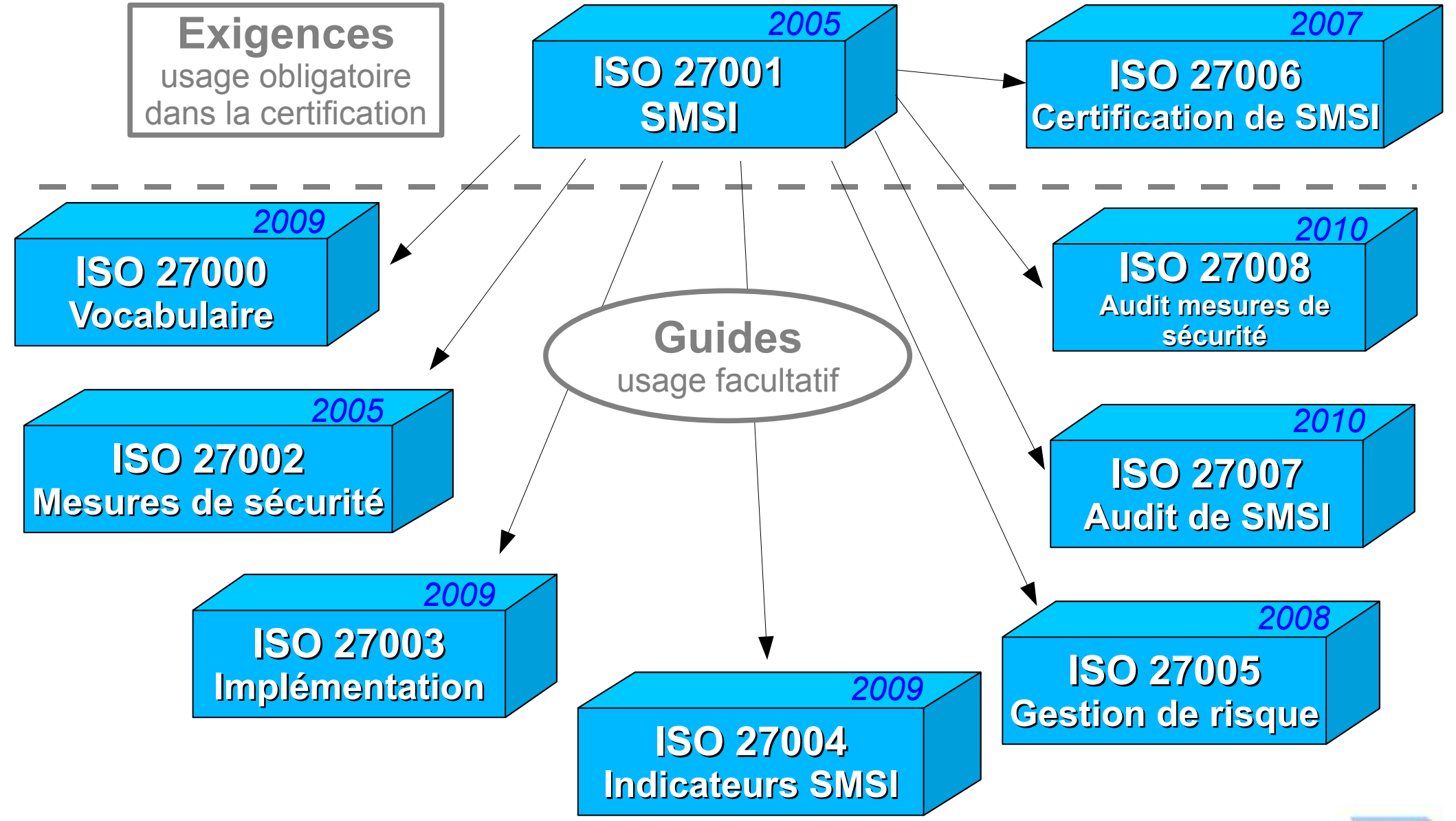
- Partenaires
- Fournisseurs
- Clients
- Pouvoirs publics
- Services

Rappels sur l'ISO 27002

- 11 chapitres
- 39 objectifs de sécurité (*control objectives*)
- 133 mesures de sécurité (*security controls*)



Série des normes ISO 27001



Question 1 : A quoi ça sert ?

- En principe
  - A piloter la sécurité par le risque
  - Appréciation des risques obligatoire (4.2.1 c)
  - Validation obligatoire des risques résiduels par la direction (4.2.1 h)
  - Cohérence entre les mesures de sécurité sélectionnées l'appréciation des risques (4.3.1 # 2)
- A améliorer (BS 7799-2:2002 1.1)
  - Compétitivité
  - Cash flow
  - Profitabilité

Question 1 : A quoi ça sert ?

- Dans la pratique
  - Sert la carrière de ceux qui implémentent le SMSI
    - Changement d'employeur
    - Valorisation du RSSI
  - Impact en terme d'image
    - Communiqué de presse
    - La tentation de l'abus est forte
  - Augmente la valorisation de l'entreprise
    - Dans l'optique d'une cession
      - Surtout pour les PME

Question 1 : A quoi ça sert ?

- On est bien loin de la sécurité...
  - ==> Question suivante

Question 2 : Est-ce que ça améliore vraiment la sécurité ?

- En principe
  - Non... mais oui
  - Pas dans un premier temps
    - La 27001 oblige à adopter de bonnes pratiques
    - Principe d'amélioration continue
    - Cela n'empêchera pas
      - D'avoir des incidents
      - De se rendre compte que l'on est passé à coté de certains risques
      - etc...
  - Mais dans la durée oui
    - Audits internes
    - Suivi des actions
    - Revues, etc...

Question 2 : Est-ce que ça améliore vraiment la sécurité ?

- Dans les faits il y a deux cas
  - Cas 1 : Ceux qui implémentent l'ISO 27001 dans le but exclusif de la conformité
    - L'ISO 27001 n'améliore en rien la sécurité
  - Cas 2 : Ceux qui l'implémentent pour s'en servir vraiment
    - Oui, car ça met de l'ordre dans la sécurité
      - Instances transversales
      - Sensibilisation des utilisateurs
      - Suivi des projets

Question 3 : Comment reconnaître un « cas 1 » et un « cas 2 » ?

- Cas 1 :
  - Les enregistrements opérationnels ont été créés au moment de la mise en place du SMSI
  - Les documents du SMSI datent de 15 jours avant chaque audit.
  - Des non-conformités majeures sont régulièrement établies
    - ➔ Nombreux audits complémentaires
    - Possibles suspensions temporaires du certificat
- Cas 2 :
  - Les enregistrements opérationnels existent depuis longtemps
  - Les documents SMSI sont produits en temps et en heure
  - Pas de non-conformités majeures
    - Pas d'audits complémentaires

Question 4 : Quels sont les domaines impactés ?

- Quels sont les domaines les plus impactés ?
  - Sécurité physique
  - Plan de continuité d'activité
  - Projets de gestion des habilitations
  - Prise en compte de la sécurité dans la démarche projet de l'entreprise
- Et la technique ?
  - Ca créé un dialogue réel et constant entre la technique et l'organisationnel
  - Le responsable du SMSI est souvent organisationnel
  - Hormis le responsable du SMSI, mes interlocuteurs lors des audits de certification sont essentiellement des ingénieurs techniques

Question 5 : A quoi ça sert vraiment ?

- A rationaliser la sécurité
- Socle de base
  - PCI-DSS / SAS 70 / RGS / Polsec / etc / etc / etc /
  - Rationalisation
  - Mutualisation
- Intégration de la sécurité dans la nouvelle gouvernance de l'entreprise
  - Depuis quelques années, on constate trois tendances de fond
    - Transversalisation
    - Standardisation
    - Mutualisation
  - ISO 27001 participe complètement dans cette démarche

Conclusion

- L'ISO 27001 est vraiment utile
- Mais son utilité n'est pas là où on l'attend apriori
  - Pas d'amélioration immédiate de la sécurité
  - Pas de « pactole » ISO 27001
- En revanche, elle apporte
  - La rationalisation de la sécurité
  - La prise en compte de la sécurité à tous les niveaux
  - Une amélioration de la sécurité dans la durée

Questions