

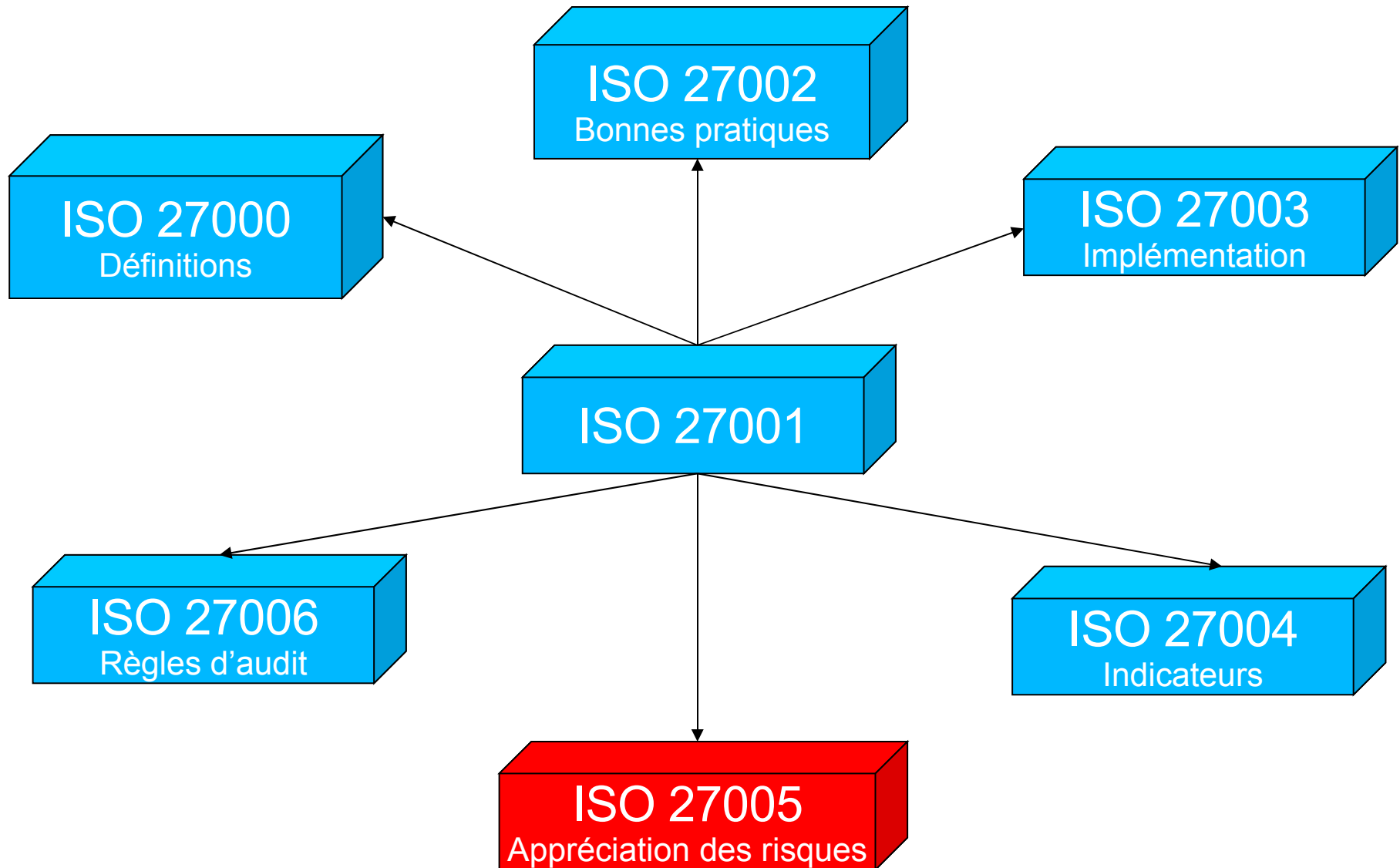


Norme ISO 27001

Démarche globale et cohérente?

Conférence IDC Risk Management 2008
Paris, 7 février 2008

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

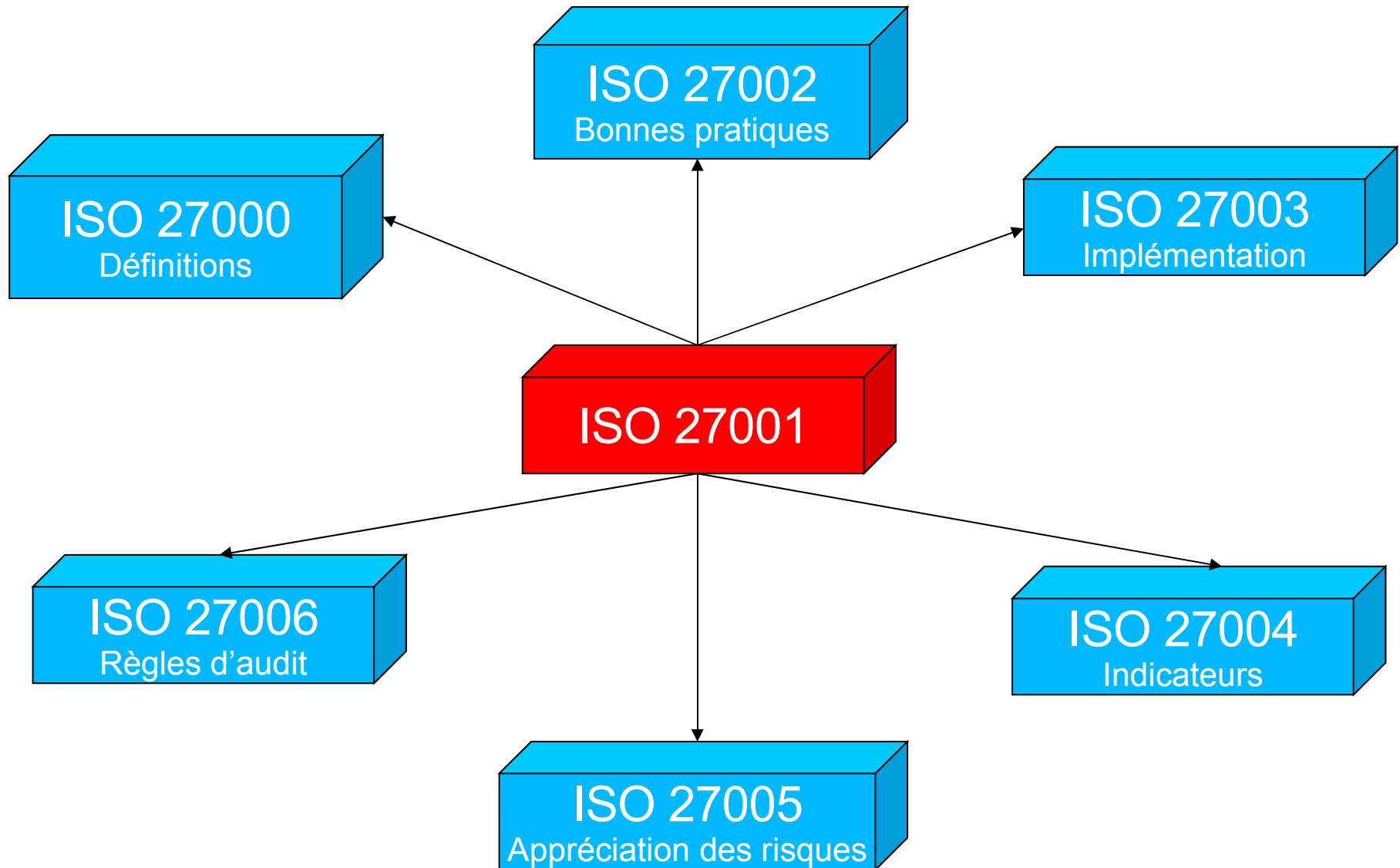


- Les méthodes d'appréciation des risques sont nombreuses
 - EBIOS
 - MEHARI
 - CRAMM
 - ISO 13335-3
 - BS 7799-3
 - Octave
 - Méthodes maison
 - Etc.

- L'ISO 27005 n'a pas réinventé la roue
- Principales étapes de l'ISO 27005
 - Inventaire des actifs
 - Valorisation des actifs
 - Identification des menaces
 - Identification des vulnérabilités
 - Probabilité d'occurrence
 - Niveau de risque
 - Traitement du risque
 - Acceptation / Refus / Transfert / Réduction
 - Risque résiduel
- Processus itératif

- Annexes : très pragmatiques
 - Inventaire des actifs
 - Deux niveaux : primaire et secondaire
 - Liste des menaces
 - Influence de la DCSSI ?
 - Exemples de vulnérabilités
 - Exemples d'appréciation des risques

- Pourquoi adopter l'ISO 27005 ?
 - Parce qu'elle reprend le meilleur des méthodes d'appréciation des risques.
 - Parce qu'elle est conforme aux exigences de l'ISO 27001
 - Et pour cause...
 - A cause de « l'ISO » de « ISO 27005 »

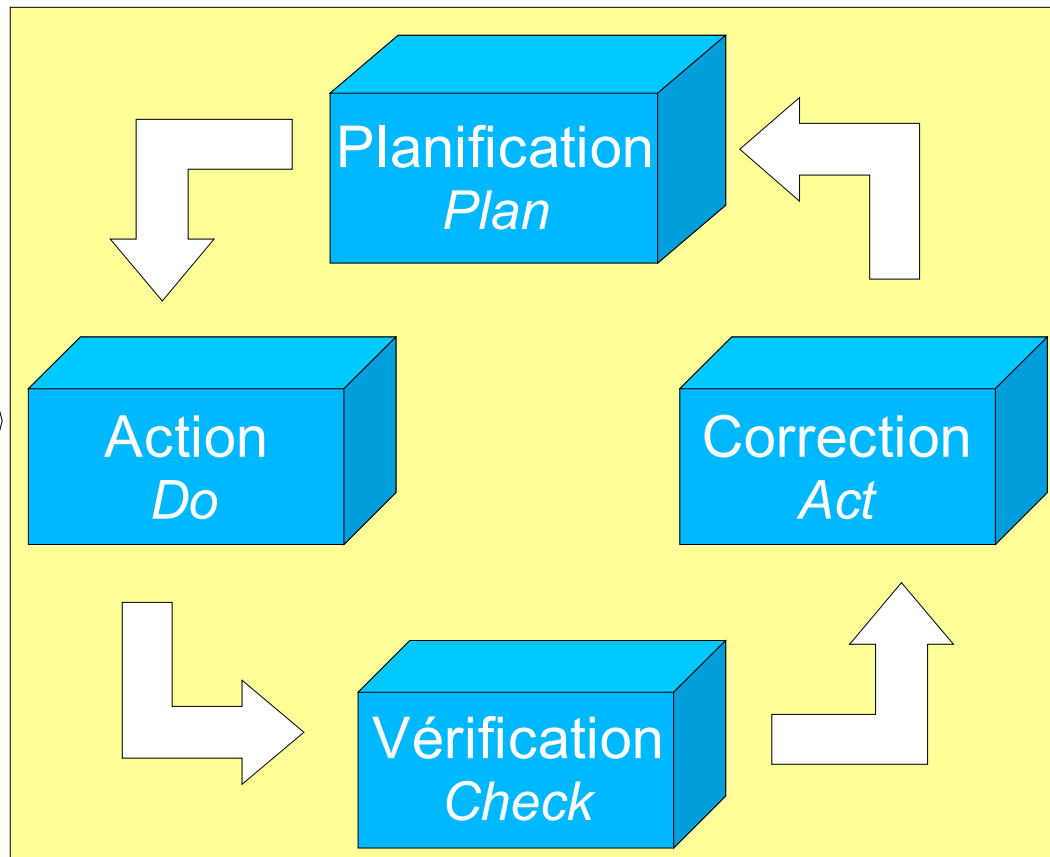


- Norme précisant les exigences pour
 - La mise en place
 - L'exploitation
 - L'amélioration
- d'un SMSI.
- Clauses 4 à 8
 - Obligatoires
 - Pas d'exceptions permises
- Mesures de sécurité de l'annexe A
 - Sélection en fonction du traitement du risque

Attentes et exigences en terme de sécurité

Modèle **PDCA** : Plan-Do-Check-Act

Sécurité effective fournie



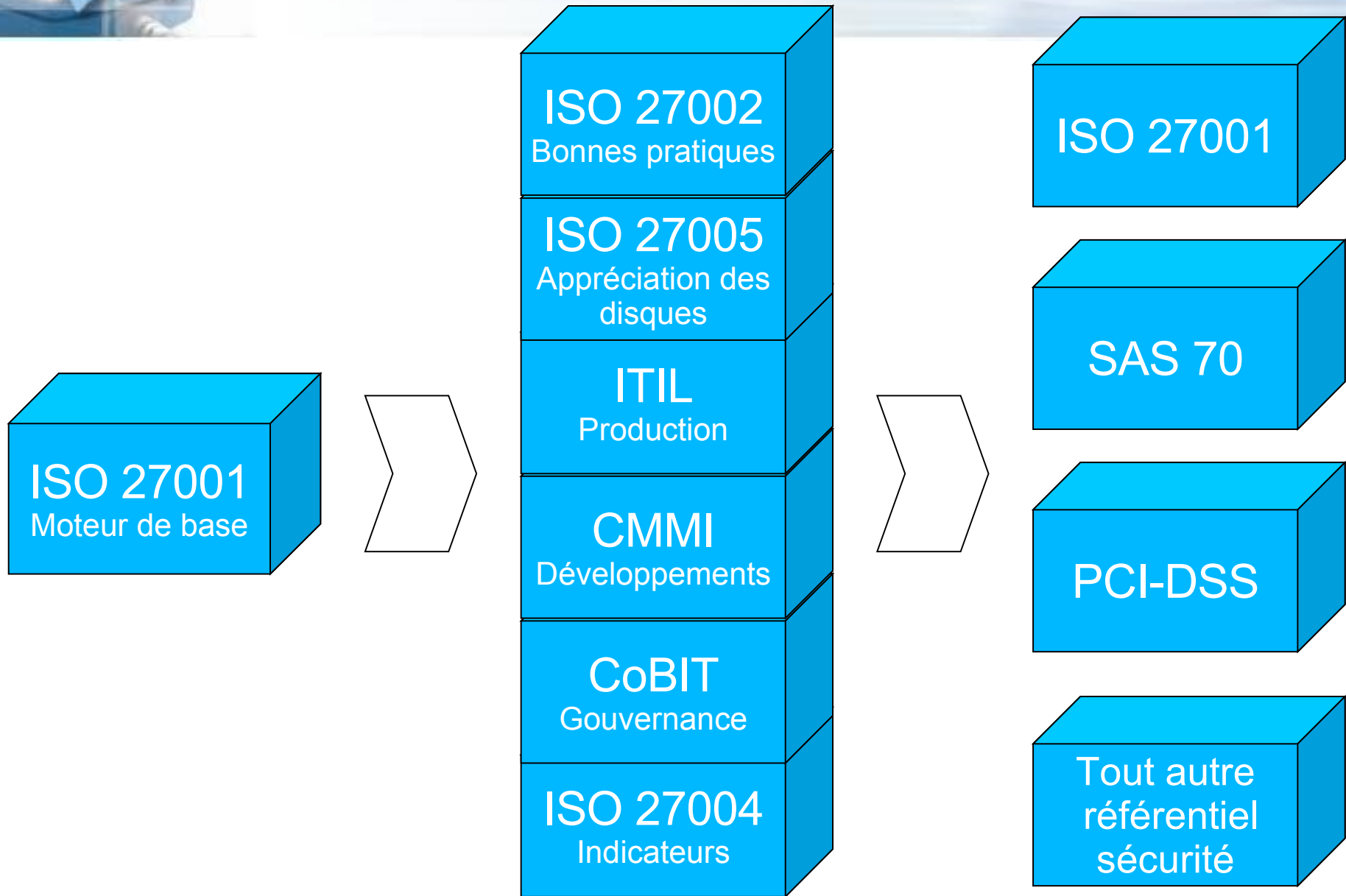
- Implémentation ISO 27001
 - Une idée reçue
 - Faire une appréciation des risques
 - Faire « de la documentation »
 - En fait
 - Définir un périmètre et une politique
 - Procéder à une appréciation des risques
 - Mettre en place des mesures de sécurité
 - **Rendre conforme l'existant au modèle PDCA**
 - **Gérer la documentation**
 - **Faire des audits internes**
 - **Faire du suivi d'actions**

- ISO 27001 et conformité
 - Sarbanes Oxley
 - SAS 70
 - PCI-DSS
 - Politiques de sécurité groupe
 - Autres référentiels sectoriels
- Points communs
 - Politique
 - Maîtrise des risques
 - Actions correctives et préventives
 - Formalisation de procédures
 - Gestion des incidents
 - Audits réguliers (audits internes et audits externes)
 - Indicateurs de conformité et d'efficacité

- ISO 27001 et autres méthodologies
 - ITIL
 - CMMI
 - CoBIT
 - Etc.

- ISO 27001 et autres certifications
 - ISO 9001
 - ISO 20000
- Un mot d'ordre : **mutualiser** autant que possible
 - Ne jamais refaire deux fois le même travail
 - Identifier le plus en amont possible les opportunités de mutualisation
 - Ce qui a été fait pour un référentiel doit être réutilisé pour l'autre

Conclusion



Alexandre.Fernandez-Toro@hsc.fr

