



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

Introduction à l'ISO 27001

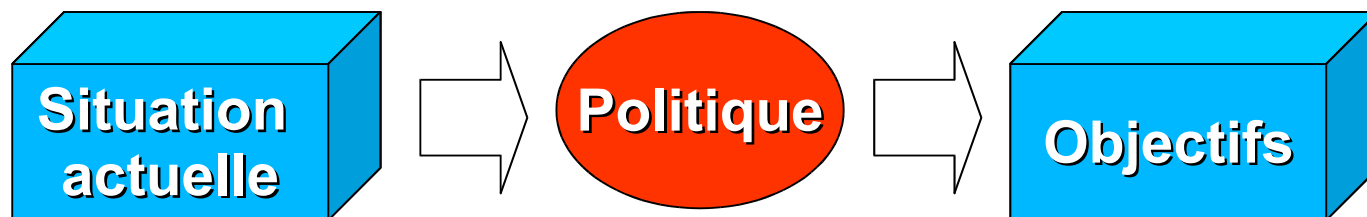


Séminaire sur la Sécurité Informatique
Casablanca, 1 novembre 2006
L'EMIAE

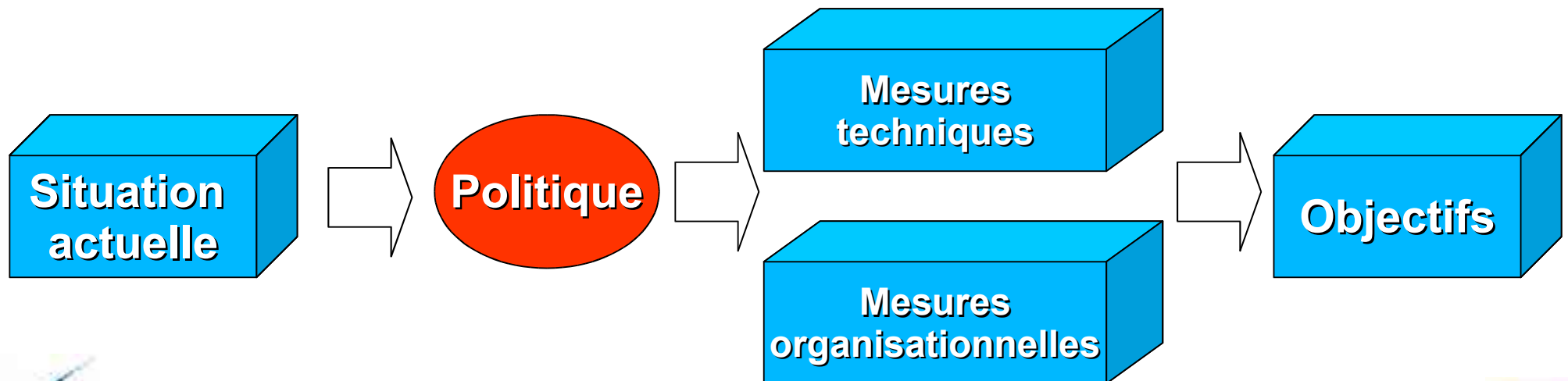
Alexandre Fernandez
Hervé Schauer

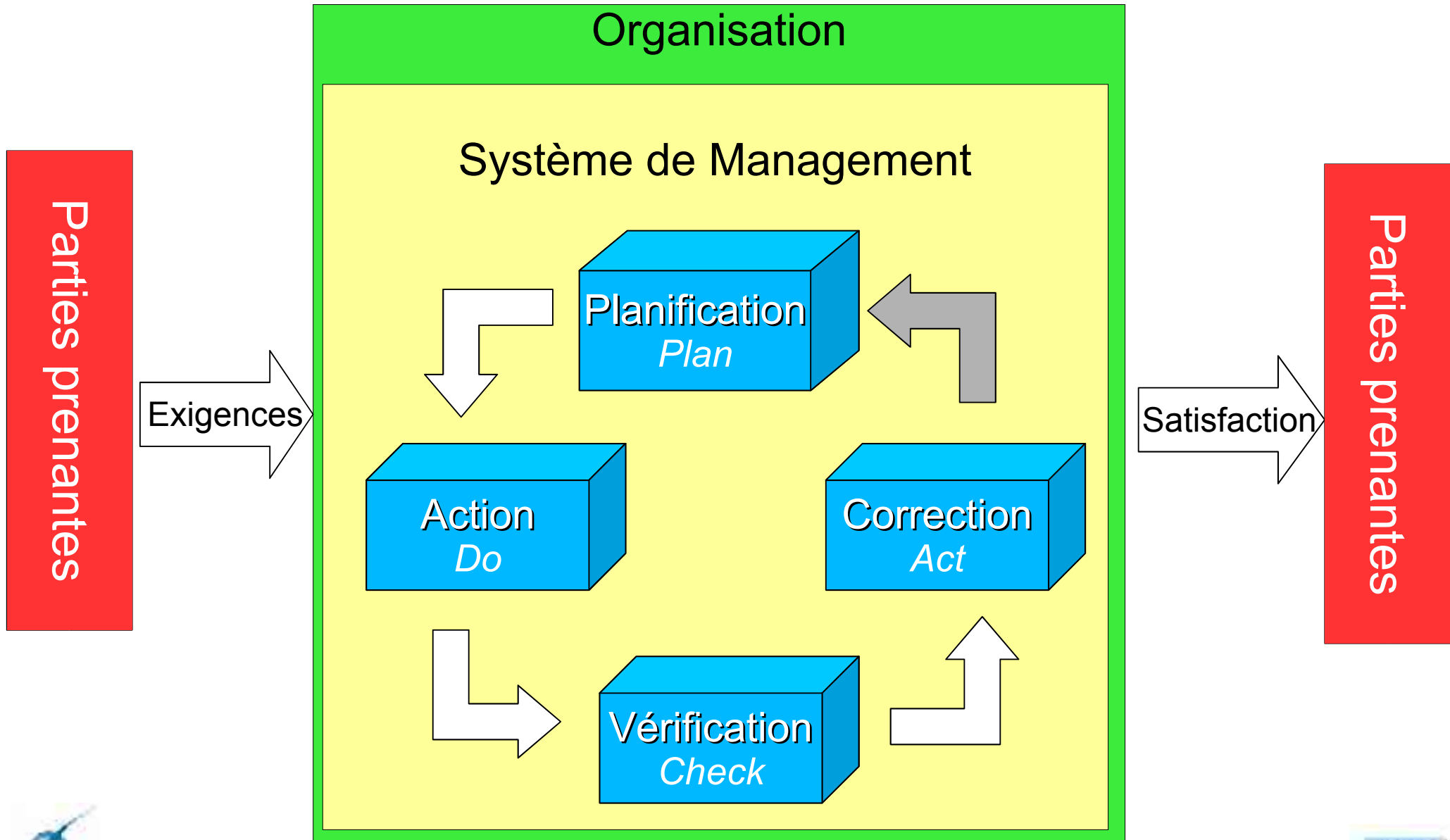
- Système de management
- Sécurité de l'information
- Système de management de la sécurité de l'information : SMSI
- Ensemble des normes ISO 27000
- Historique
- ISO 27001
- ISO 27002 (anciennement ISO 17799)
- ISO 27001 par rapport à ISO 27002
- Usages des normes

- Définition formelle de l'ISO 9000
 - C'est un système permettant :
 - D'établir une politique
 - D'établir des objectifs
 - D'atteindre ces objectifs



- Définition plus empirique
 - Ensemble de mesures
 - Organisationnelles
 - Techniques
 - Permettant
 - D'atteindre un objectif
 - Une fois atteint, d'y rester dans la durée





- Propriétés des systèmes de management
 - Couvrent un large spectre de métiers et de compétences
 - Concernent tout le monde
 - De la direction générale
 - Jusqu'en bas de l'échelle
 - Se basent sur des référentiels précis
 - Importance du document écrit
 - Sont auditables
 - Quelqu'un peut venir vérifier qu'il n'y a pas d'écart entre le système de management et les référentiels

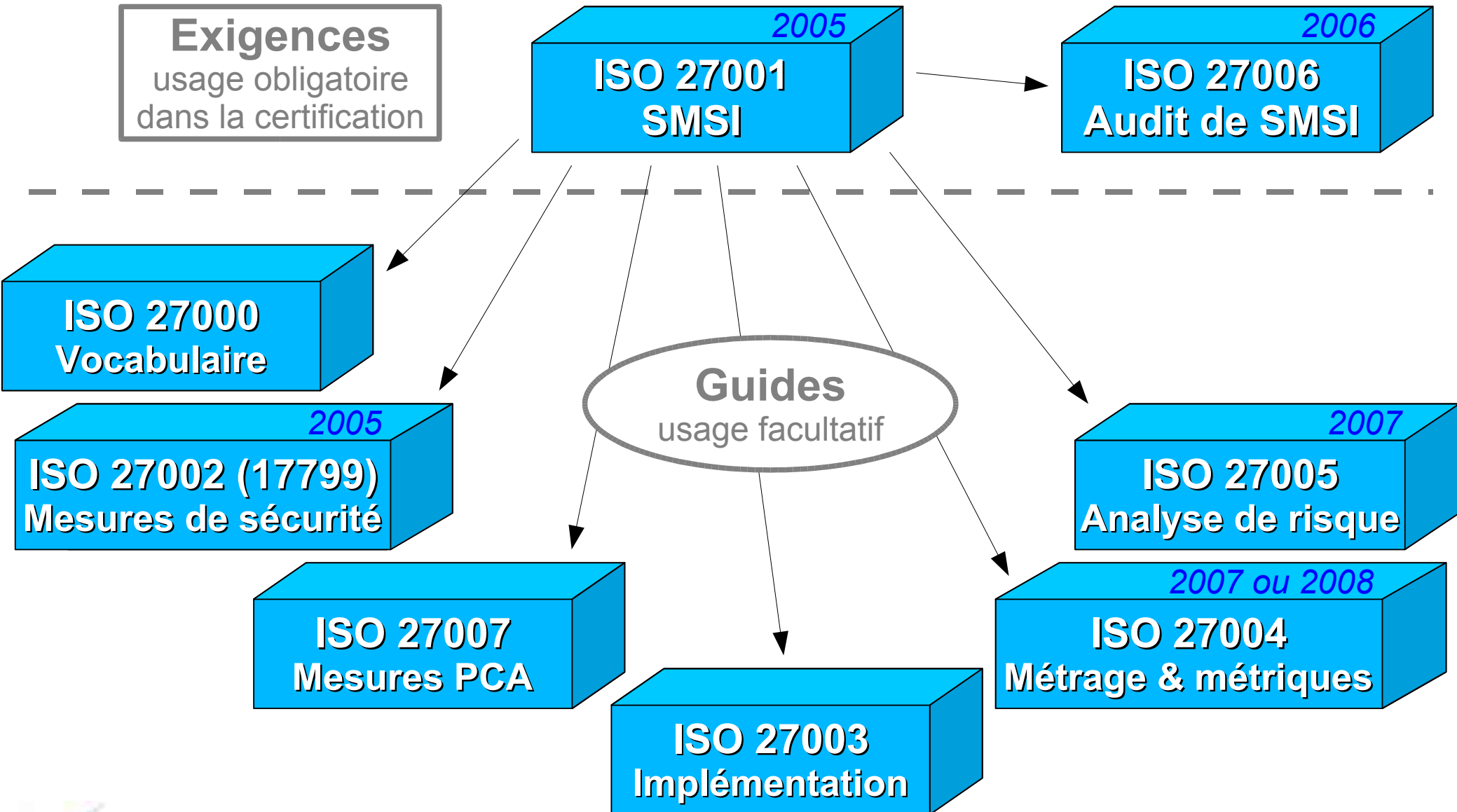
- Conséquences de travailler sur un système de management
 - Travail transversal
 - Tout le monde est concerné
 - De la direction générale
 - A l'accueil
 - Importance de l'écrit
 - Passage de la tradition orale à la tradition écrite
 - Dans certains cas un effort culturel important
 - Peuvent être audités
 - Les processus seront constamment évalués

- Apports d'un système de management
 - Oblige à adopter de bonnes pratiques
 - Augmente donc la fiabilité de l'organisme dans la durée
 - De façon pérenne
 - Comme un système de management est auditable
 - Il apporte la **confiance** aux parties prenantes
- Qui dit **confiance** dit **business**

- Sécurité de l'information (*information security*) (IS 27001 3.4)
 - Confidentialité (*confidentiality*)
 - Intégrité (*integrity*)
 - Disponibilité (*availability*)

- Authenticité (*authenticity*) = authentification + intégrité
- Imputabilité, auditabilité, traçabilité (*accountability*)
- Non répudiation (*non-repudiation*)
- Etc.

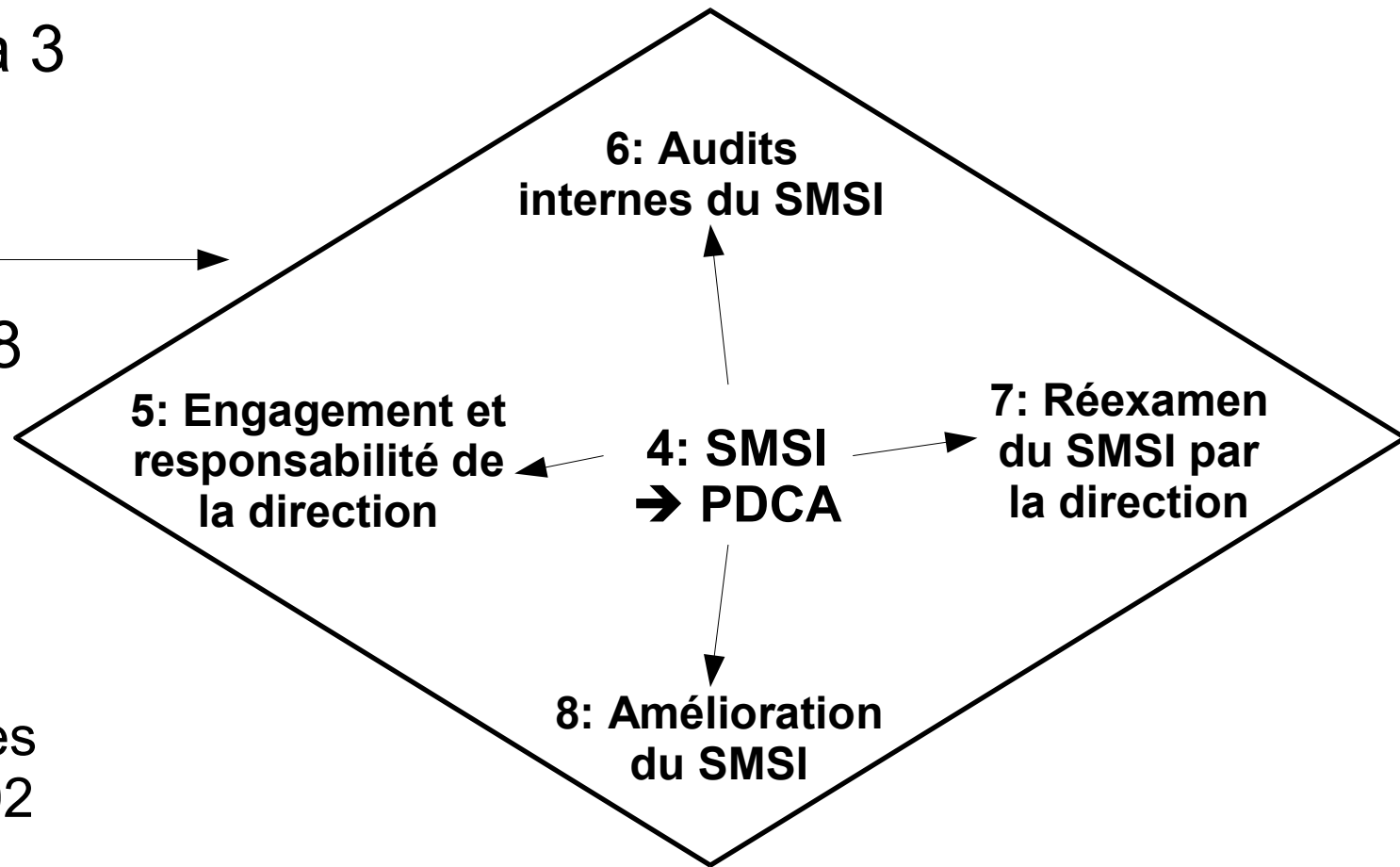
- SMSI (IS 27001 3.7)
 - Système de Management de la Sécurité de l'Information
- SGSI
 - Système de Gestion de la Sécurité de l'Information
- SGSSI
 - Système de Gestion de la Sécurité des Systèmes d'Information
- ISMS (IS 27001 3.7)
 - *Information Security Management System*



- 1995 BS7799
 - Dix mesures clé
 - 100 mesures détaillées, potentiellement applicables
- 1998 Ajout d'une partie 2
 - Notion de SMSI
 - Objectif : Créer un schéma de certification
- 2000 ISO 17799: 2000
 - Correspond à la BS7799-1
 - Pas de notion de SMSI
 - Pas de certification possible
- 2002 BS7799-2: 2002
 - Seconde version de la BS 7799-2

- Juin 2005 **ISO 17799:2005**
 - Nouvelle version de l'ISO 17799: 2000
- Octobre 2005 **ISO 27001:2005**
 - Adoption par l'ISO de la BS 7799-2:2002 avec des améliorations
 - Notion de SMSI
 - Possibilité de certification
- Fin 2006 / début 2007
 - ISO 27006 : audit de certification
- Avril 2007 : **ISO 27002**
 - ISO 17799:2005 est renommée ISO 27002
 - Rentre dans la terminologie de la série ISO 27000 sans changement

- 4 chapitres introductifs : 0 à 3
- 5 articles à respecter : 4 à 8
- Annexe A
 - Mesures de sécurité décrites dans ISO 27002



- Tout types d'organismes visés (IS 27001 1.1):
 - Sociétés commerciales
 - Agences gouvernementales
 - Associations, ONG
- Indications de la norme génériques (1.2):
 - Applicables à tout type d'organisation indépendamment du
 - Type
 - Taille
 - Nature de l'activité

- Objectif général de la norme ^(1.1) :
 - Spécifier les **exigences** pour
 - Mettre en place
 - Exploiter
 - Améliorer
 - Un **SMSI** documenté
- Spécifier les exigences pour la mise en place de mesures de sécurité
 - Adaptées aux besoins de l'organisation
 - Adéquates
 - Proportionnées

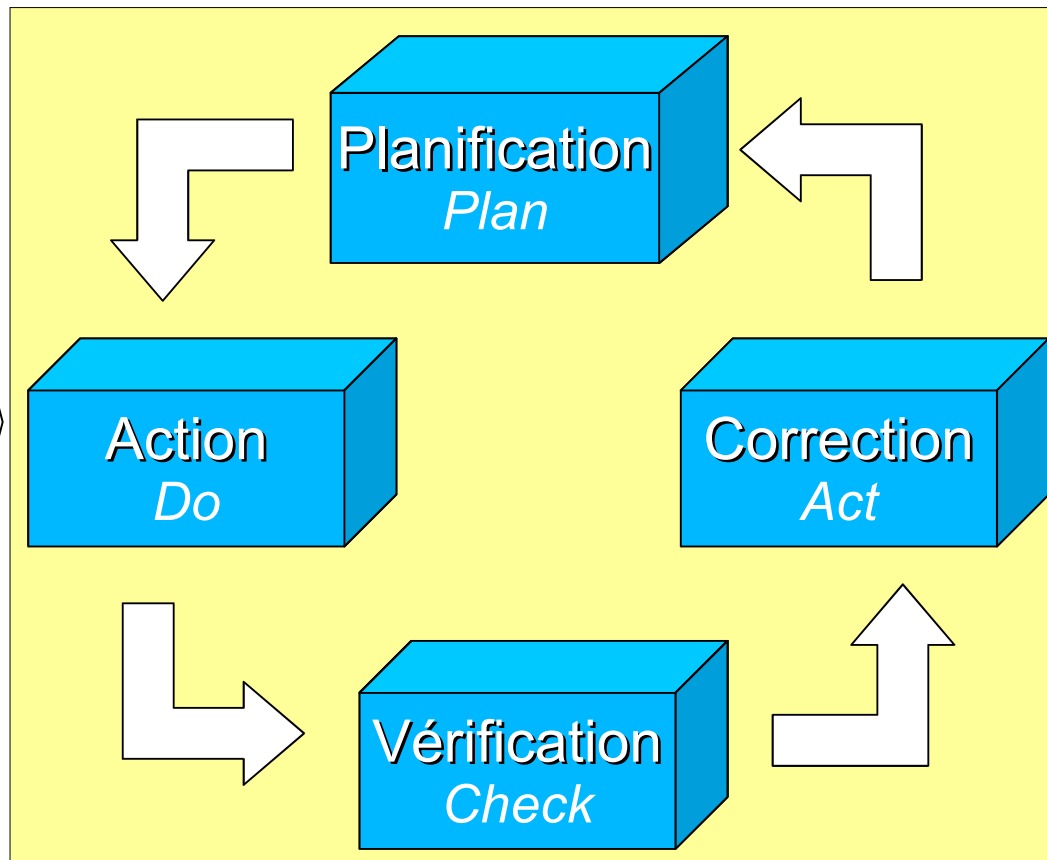
- Ceci doit fournir ^(1.1):
 - Une **protection** des actifs d'information
 - **Confiance** aux parties prenantes
- Maintenir et améliorer ^(BS 7799-2:2002 1.1)
 - *Précision présente dans la BS 7799-2:2002 mais a disparu dans l'ISO 27001:2005*
 - Compétitivité
 - Cash flow (*cash flow*)
 - Profitabilité
 - Respect de la réglementation
 - Image de marque

Attentes et exigences en terme de sécurité

Modèle PDCA : Plan-Do-Check-Act

Sécurité effective fournie

- Partenaires
- Fournisseurs
- Clients
- Pouvoirs publics
- Services



- Partenaires
- Fournisseurs
- Clients
- Pouvoirs publics
- Services

- Phase *PLAN*
 - Périmètre du SMSI (4.2.1.a)
 - Politique de sécurité et/ou politique du SMSI (4.2.1.b)
 - Identification et évaluation des risques (4.2.1.c)
 - Plan de gestion des risques
 - Méthodologie ou méthode choisie pour analyser les risques (4.2.1.d) (4.2.1.e)
 - Traitement du risque (4.2.1.f)
 - Réduction du risque à un niveau acceptable
 - Acceptation des risques
 - Transfert
 - Refus ou évitement des risques
 - Objectifs de sécurité et mesures de sécurité (4.2.1.g)
 - → Déclaration d'applicabilité : DDA (*Statement of applicability* ou *SoA*) (4.2.1.j)

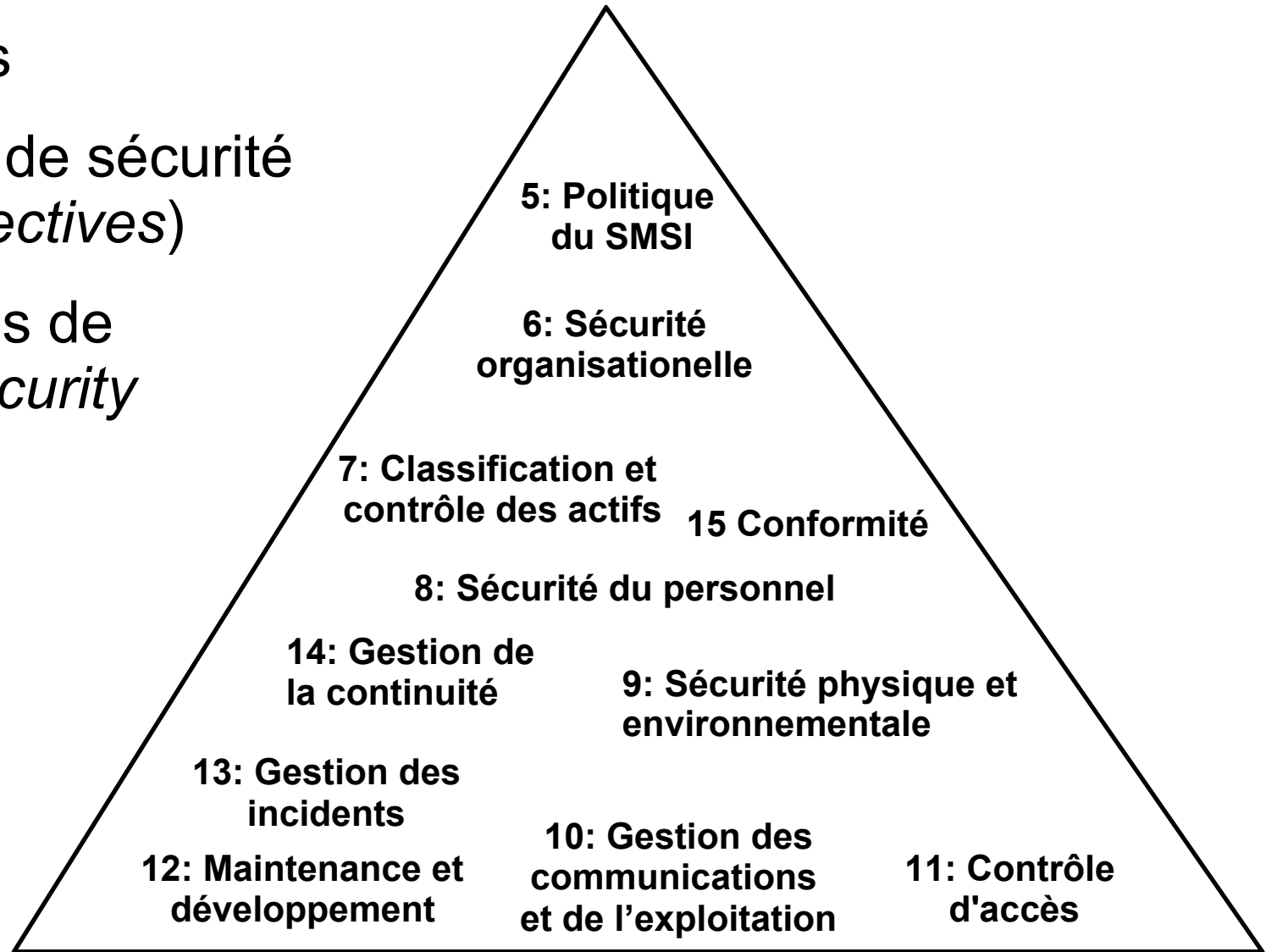
- Phase *DO*

- Allocation et gestion de ressources (4.2.2.a) (4.2.2.b) (4.2.2.g)
 - Personnes, temps, argent
- Rédaction de la documentation et des procédures
- Formation du personnel concerné (4.2.2.e)
- Gestion du risque (4.2.2.a) (4.2.2.b)
 - Pour les risques à réduire :
 - Implémenter les mesures de sécurité identifiées dans la phase précédente (4.2.2.c)
 - Assignation des responsabilités (4.2.2.b)
 - Identifier des risques résiduels
 - Pour les risques transférés : assurance, sous-traitance, etc
 - Pour les risques acceptés et refusés : rien à faire

- Phase *CHECK*
 - Vérification de routine (4.2.3.b)
 - Apprendre des autres (4.2.3.b)
 - Audit du SMSI (4.2.3.e)
 - Audits réguliers
 - Sur la base de
 - Documents
 - Traces ou enregistrements
 - Tests techniques
 - Conduit à
 - Constatation que les mesures de sécurité ne réduisent pas de façon effective les risques pour lesquels elles ont été mises en place
 - Identification de nouveaux risques non traités
 - Tout autre type d'inadaptation de ce qui est mis en place

- Phase *ACT*
 - Prendre les mesures résultant des constatations faites lors de la phase de vérification
 - Actions possibles
 - Passage à la phase de planification
 - Si de nouveaux risques ont été identifiés
 - Passage à la phase d'action
 - Si la phase de vérification en montre le besoin
 - Si constatation de non conformité
 - Actions correctives ou préventives

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



- Anciennement ISO 17799
 - Renumérotation en avril 2007
 - Traductions et nouvelles normes utilisent déjà la nouvelle numérotation
- Vocabulaire
 - *Control* (IS 27002 2.2)
 - Mesure de sécurité
 - "Contrôle de sécurité"
- Ensemble des mesures de sécurité pouvant être appliqués
 - Description de la mesure
 - Description de l'indication de cette mesure

- Recommandations ou exigences en sécurité
- Reprennent les recommandations classiques des experts en sécurité
 - Certaines mesures de sécurité sont très générales, d'autres très précises
 - Certaines mesures sont applicables à tout l'organisme, d'autres à un serveur ou une application particulière
 - Donnent des recommandations parfois très larges pouvant inclure d'autres mesures de sécurité
- Sélectionnées pour réduire un risque à un niveau acceptable à l'issue d'une analyse de risque

- Définition de la mesure de sécurité pour satisfaire l'objectif de sécurité
- Détails afin d'aider à l'implémentation de la mesure de sécurité
 - Pas toujours applicables
- Explications complémentaires sur le guide d'implémentation
 - Aspects complémentaires
 - Autres facteurs à prendre en compte

Mesure de sécurité

Guide d'implémentation

Autres informations

- Pas de classement des mesures de sécurité dans ISO 27002
- Mesures de sécurité classées dans ISO 27006 (A.4)
 - Organisationnelles
 - Organisationnelles et techniques
 - Techniques
- Audit différent

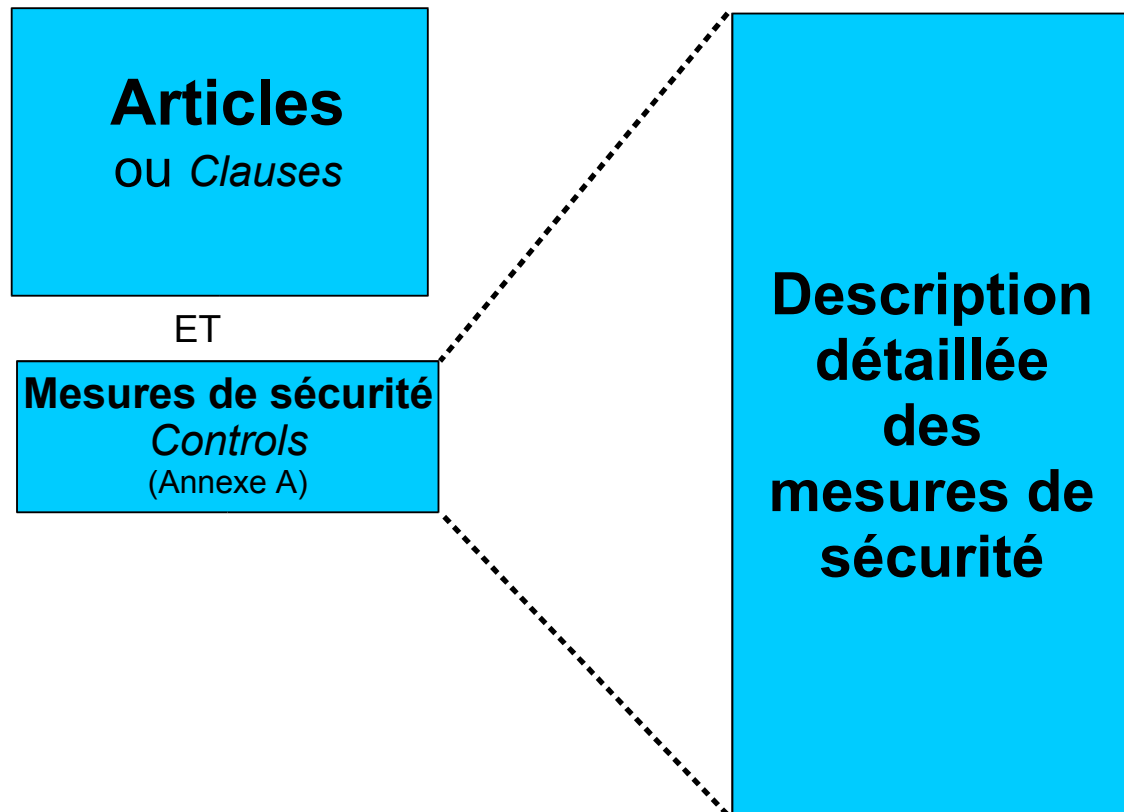
- Mesures de sécurité organisationnelles plutôt dans :
 - 5 : politique de sécurité
 - 6 : organisation de la sécurité
 - 7 : gestion des actifs
 - 8 : ressources humaines
 - 9 : sécurité physique
 - 13 : gestion des incidents
 - 14 : gestion de la continuité d'activité
 - 15 : conformité
- Auditées par : (IS 27006 A 4.2)
 - Revue de la documentation des processus, interviews, observation et inspection physique

- Mesures de sécurité techniques ou en partie techniques plutôt dans les chapitres :
 - 10 : gestion de l'exploitation
 - 11 : contrôle d'accès
 - 12 : acquisition, développement et maintenance du système d'information
- Auditées par : (IS 27006 A 4.2)
 - Idem que les procédures organisationnelles
 - Vérification par des tests réels sur les systèmes :
 - Possibles
 - Conseillés
 - Obligatoires } → mesures de sécurité à étudier plus particulièrement

ISO 27001

ISO 27002

(anciennement ISO 17799)



- ISO 27001

- Traite des systèmes de management
- Volumétrie
 - Nombre total de pages
 - 33
 - Articles → 10 pages
 - Annexes → 23 pages

- ISO 27002 (ISO 17799)

- Ne traite pas des systèmes de management
- Volumétrie
 - Nombre total de pages
 - 115
 - Notes préliminaires → 6 pages
 - Liste des mesures de sécurité → 109 pages

- ISO 27001

- Traite des systèmes de management
- Modèle PDCA
- Usage du verbe
 - **SHALL**
- Certification possible
- Application de **tous** les articles 4, 5, 6, 7 et 8 **obligatoire** (1.2)

- ISO 27002 (ISO 17799)

- Ne traite pas des systèmes de management
- Pas de modèle PDCA
- Usage du verbe
 - **SHOULD**
- Aucune obligation d'application
- Pas de certification

- Pour les audits
 - ISO 27002 (ISO 17799)
 - Les conclusions font référence à la norme
 - Espéranto de la sécurité

- Pour les tableaux de bord
 - ISO 27002 (ISO 17799)
 - Approche pragmatique

- Pour adopter les bonnes pratiques
 - ISO 27001 + ISO 27002
 - Constat objectif que vous adoptez les bonnes pratiques en matière de SSI
 - Permet d'évoluer, le moment venu, vers une certification
 - Risque : non-conformité avec la norme
- Pour donner une image de sérieux aux partenaires
 - ISO 27001
 - Constat, extérieur et objectif que vous adoptez les bonnes pratiques en matière de SSI
 - Permet d'évoluer, le moment venu, vers une certification

- Pour être certifié
 - ISO 27001
 - Constat impartial, objectif et officiel que "vous adoptez les bonnes pratiques en matière de SSI"
 - Engagement dans la durée

Questions ?

Herve.Schauer@hsc.fr

www.hsc.fr