



HERVÉ SCHAUER CONSULTANTS

Cabinet de Consultants en Sécurité Informatique depuis 1989

Spécialisé sur Unix, Windows, TCP/IP et Internet

Normes ISO 27001

DCSSI/CFSSI

28 mars 2007

Alexandre Fernandez

Hervé Schauer

<Herve.Schauer@hsc.fr>

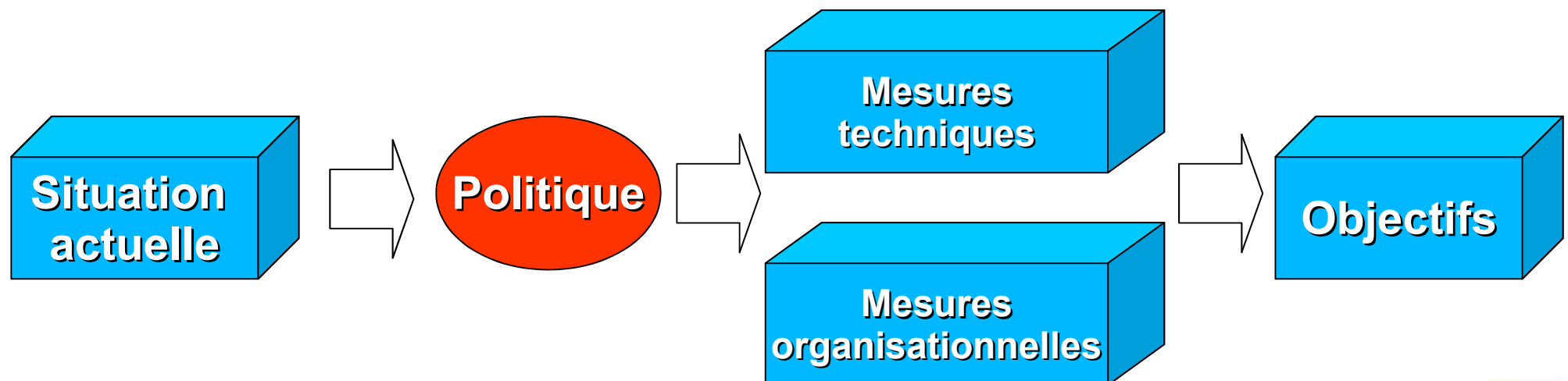
- Système de management
- Concept populaire et enseigné
- SMSI : Système de Management de la Sécurité de l'Information
- Apparition des normes
- Ensemble des normes ISO 27001
 - ISO 27001, ISO 27002, ISO 27000, ISO 27003 ... ISO 27007
- Usages des normes
- Certification
- Conclusion

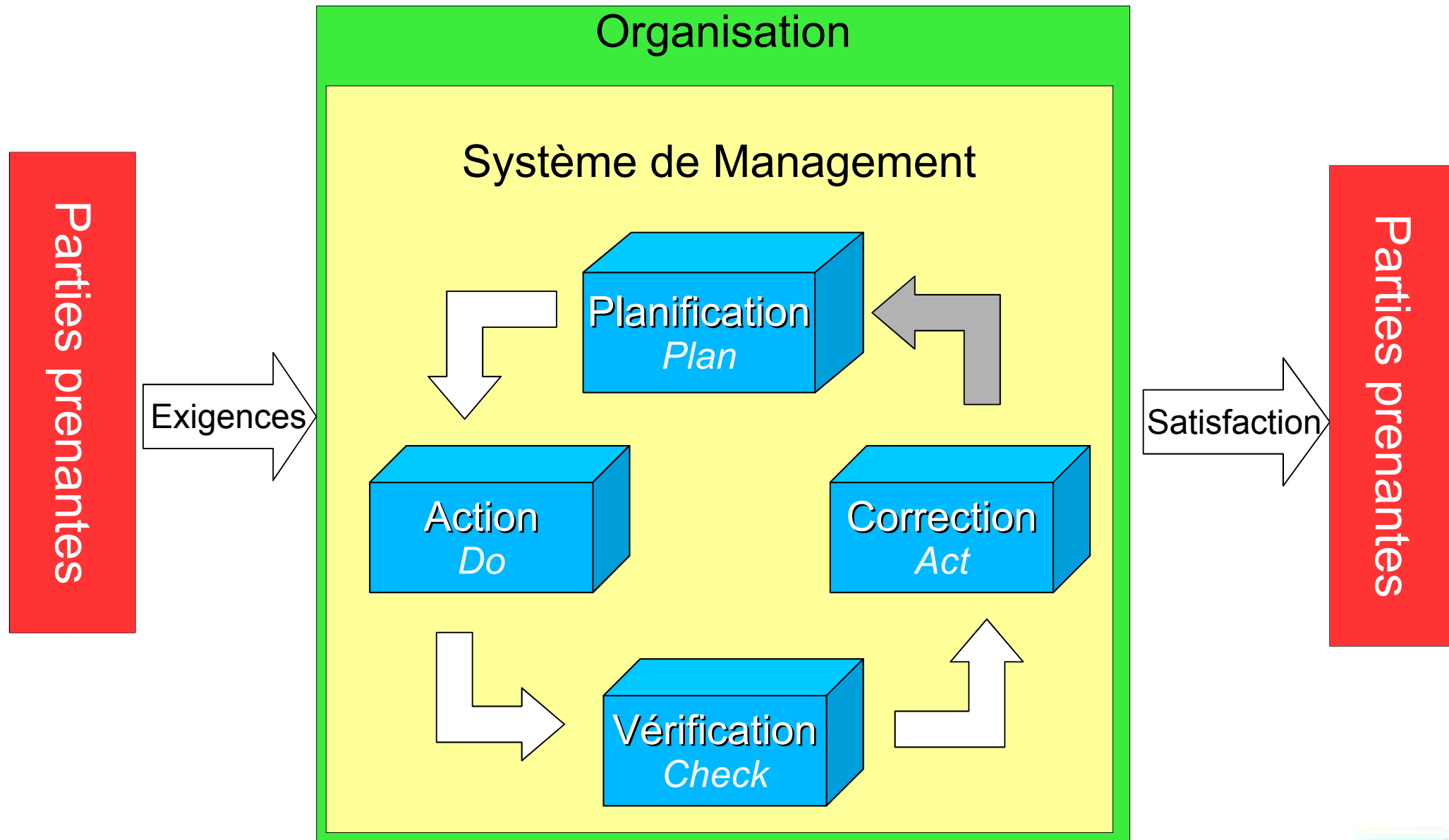
**Les transparents seront
disponibles sur
www.hsc.fr**

- 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

- Apports d'un système de management
 - Oblige à adopter de bonnes pratiques
 - Minimum
 - Oblige à s'améliorer dans le temps
 - 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**

- Exemple : cahiers Oxford Etudiant
- «la spirale de l'excellence»

Des outils d'organisation ...



Nous passons beaucoup de temps à acquérir des connaissances, à apprendre l'utilité de ces connaissances et les conditions de leur mise en œuvre... Mais paradoxalement nous ne consacrons que fort peu de temps à apprendre à nous organiser, seule façon pourtant de valoriser et de concrétiser notre potentiel. Les conséquences sont multiples : situations de stress, mauvaise gestion de soi, beaucoup de démotivation...

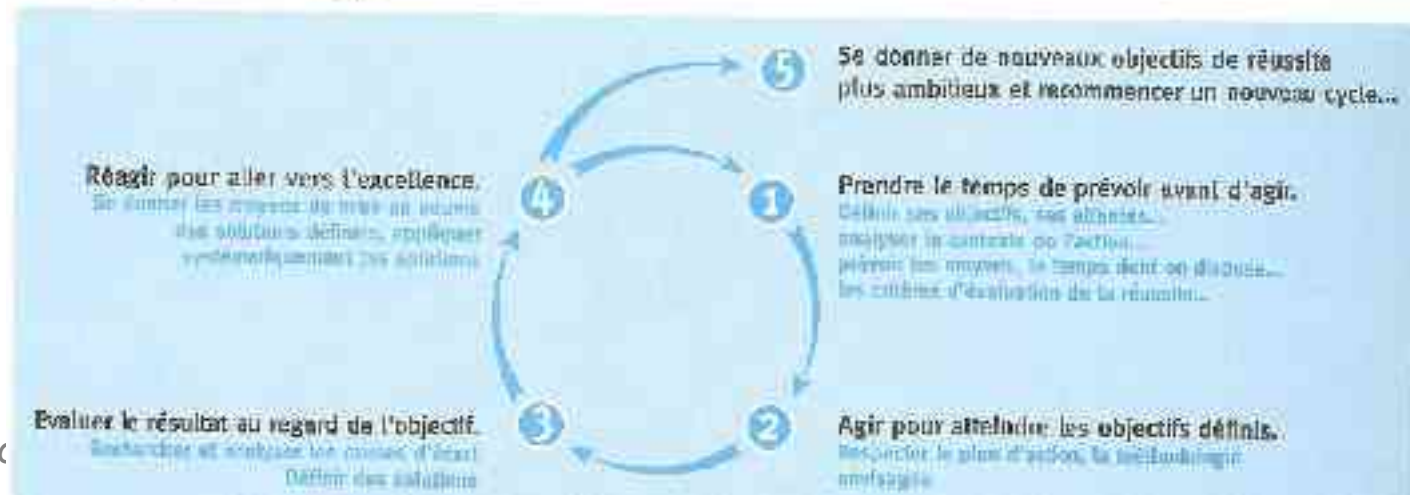
La solution : acquérir des outils d'organisation

- L'analyse stratégique pour atteindre sûrement l'objectif que l'on se fixe et s'améliorer
- La gestion du temps pour se donner le temps d'être méthodique et de jouer gagnant

① Analyse stratégique

■ Appliquer la spirale de l'excellence

Réaliser sans écart l'action définie est l'objectif d'efficacité de l'un chacun. La spirale de l'excellence montre l'enchaînement chronologique à avoir pour entrer dans une dynamique de progrès et d'amélioration continue : définir, agir, évaluer et réagir



Reproduit avec
l'autorisation du
Groupe Hamelin

- Rappelé aux élèves de manière didactique :
 - PDCA pour travailler en cours

► Mettre en application cette spirale est une excellente discipline mentale qui oblige à réfléchir avant d'agir. Elle introduit dans l'action, à la fois la préparation et l'évaluation, tout ce qui permet, si l'on s'en donne les moyens, d'atteindre ses objectifs et de progresser constamment. La façon dont l'objectif est posé conditionnera l'action mise en oeuvre, comme le montre l'exemple suivant :



Attention : Il est important de garder à l'esprit qu'une stratégie ne se met véritablement en place qu'à partir du moment où les objectifs sont personnalisés, de même que le temps passé à la réflexion et à l'analyse est du temps gagné pour l'action qui se déroulera plus vite et plus sûrement.

- 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*
- SGSI (UNE71502)
 - *Sistema de Gestión de la Seguridad de la Información*

Apparition des normes

- Journal officiel de l'Union européenne du 25/03/2005, l'annexe du règlement (CE) n° 1663/95 est modifiée comme suit :
 - http://europa.eu.int/smartapi/cgi/sga_doc?smartapi!celexplus!prod!CELEXnumdoc&numdoc=32005R0465&lg=fr

6 vi) la sécurité des systèmes d'information se fonde sur les critères établis dans une version applicable, pour l'exercice financier concerné, de l'une des normes reconnues sur le plan international ci-après :

- Norme 17799 de l'ISO / Norme britannique BS7799
- BSI (système de sécurité allemand)
- ISACA COBIT

- Appel d'offre du dossier médical personnel, 28/07/2005, annexe "Sécurité"

- <http://www.d-m-p.org/docs/annexes.pdf>

La présente annexe définit les objectifs de sécurité et les exigences fonctionnelles de sécurité que les hébergeurs de DMP devront respecter. Elle s'appuie en particulier sur la norme ISO17799:2005 et la future norme ISO27001 (basée sur la BS7799-2:2002).

Ensemble des normes ISO27001

Exigences
usage obligatoire
dans la certification

2005
ISO 27001
SMSI

2007
ISO 27006
Certification de SMSI

Guides
usage facultatif

2008 ou 2009
ISO 27000
Vocabulaire

ISO 27007
Audit de SMSI

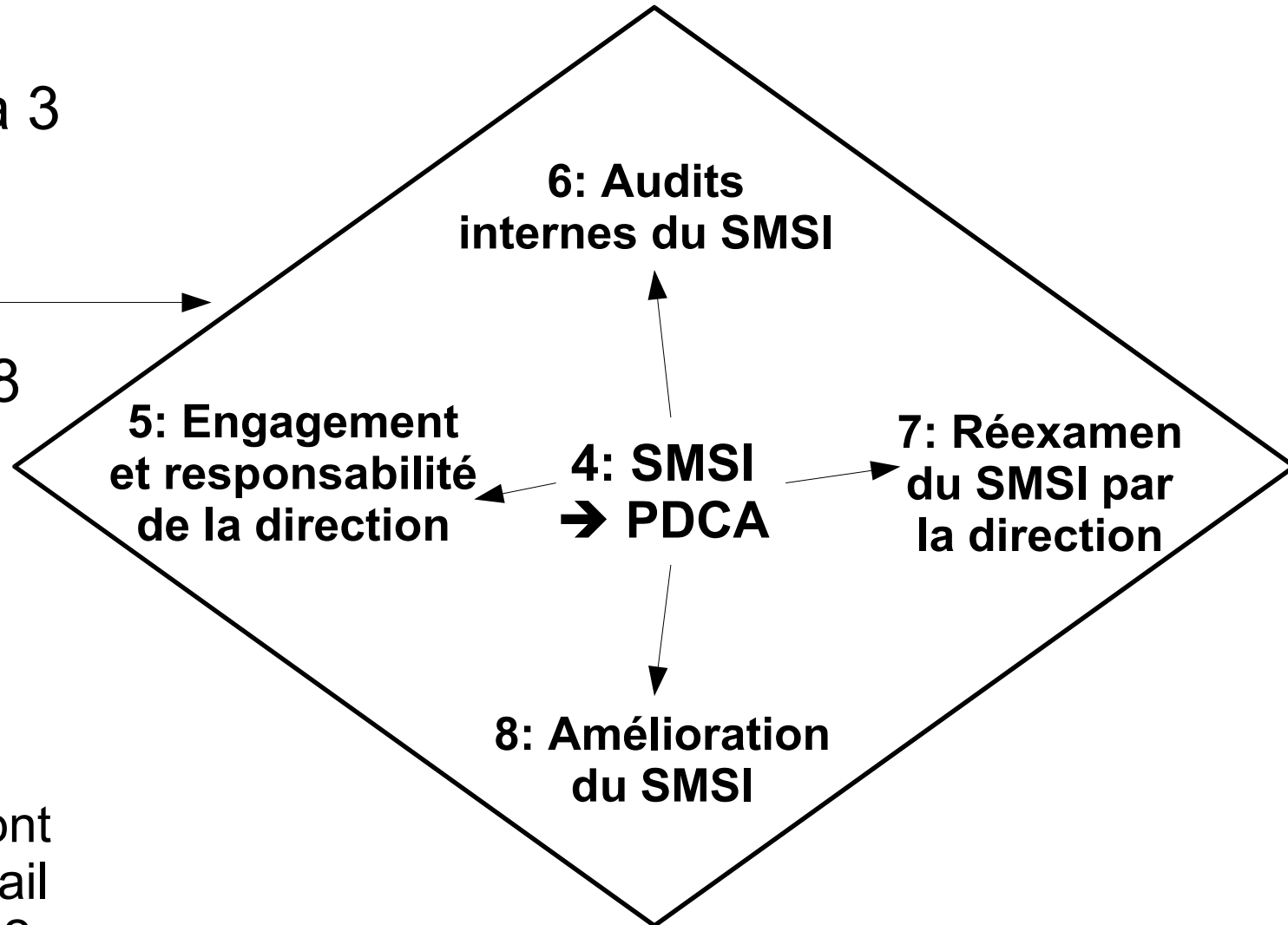
2005
ISO 27002 (17799)
Mesures de sécurité

2007 ou 2008
ISO 27005
Gestion de risque

2008 ou 2009
ISO 27003
Implémentation

2008
ISO 27004
Indicateurs SMSI

- 4 chapitres introductifs : 0 à 3
- 5 chapitres à respecter : 4 à 8
- Annexe A
 - Mesures de sécurité
 - Mesures qui sont décrites en détail 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

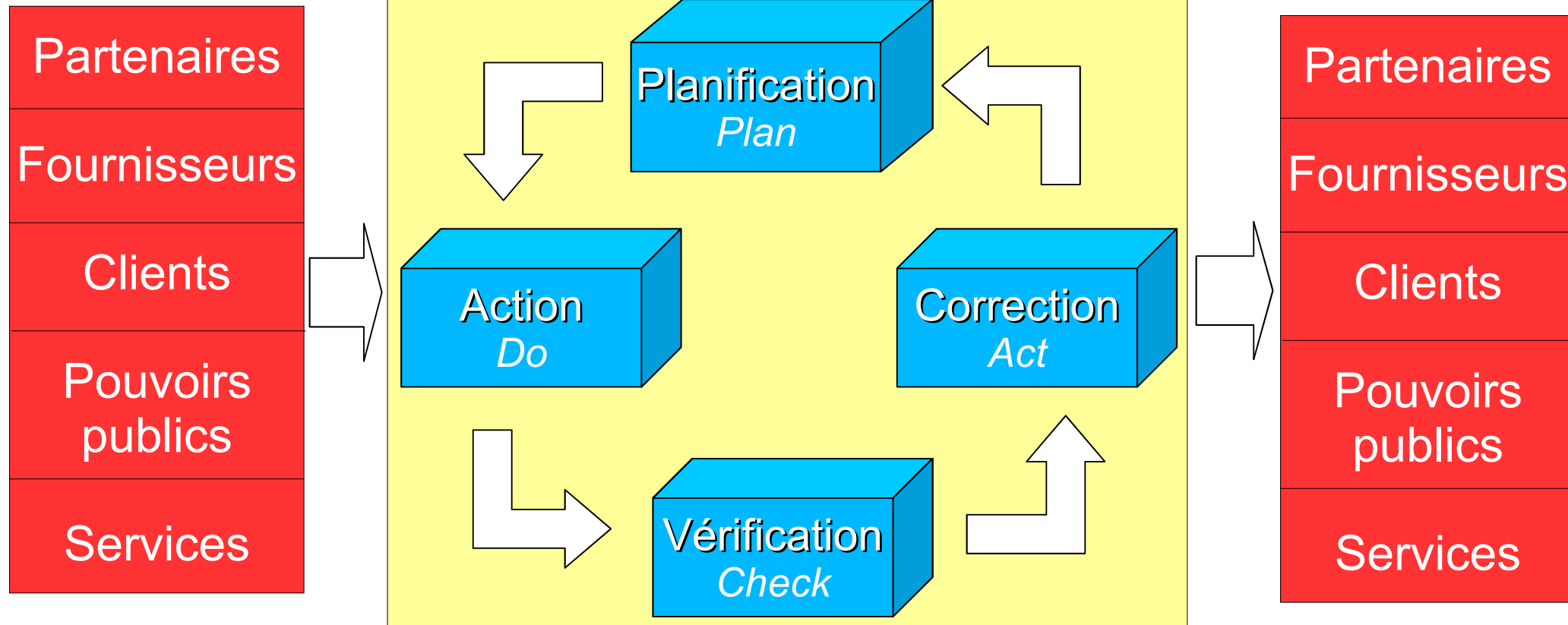
- Ceci doit fournir ^(1.1):
 - Une **protection** des actifs d'information (*information assets*)
 - Patrimoine informationnel
 - Biens sensibles
 - La **confiance** aux parties prenantes (*interested parties*)
 - Sous entendu
 - Clients
 - Actionnaires
 - Partenaires
 - Assureurs
 - etc

- Ceci doit 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
 - Trésorerie (*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



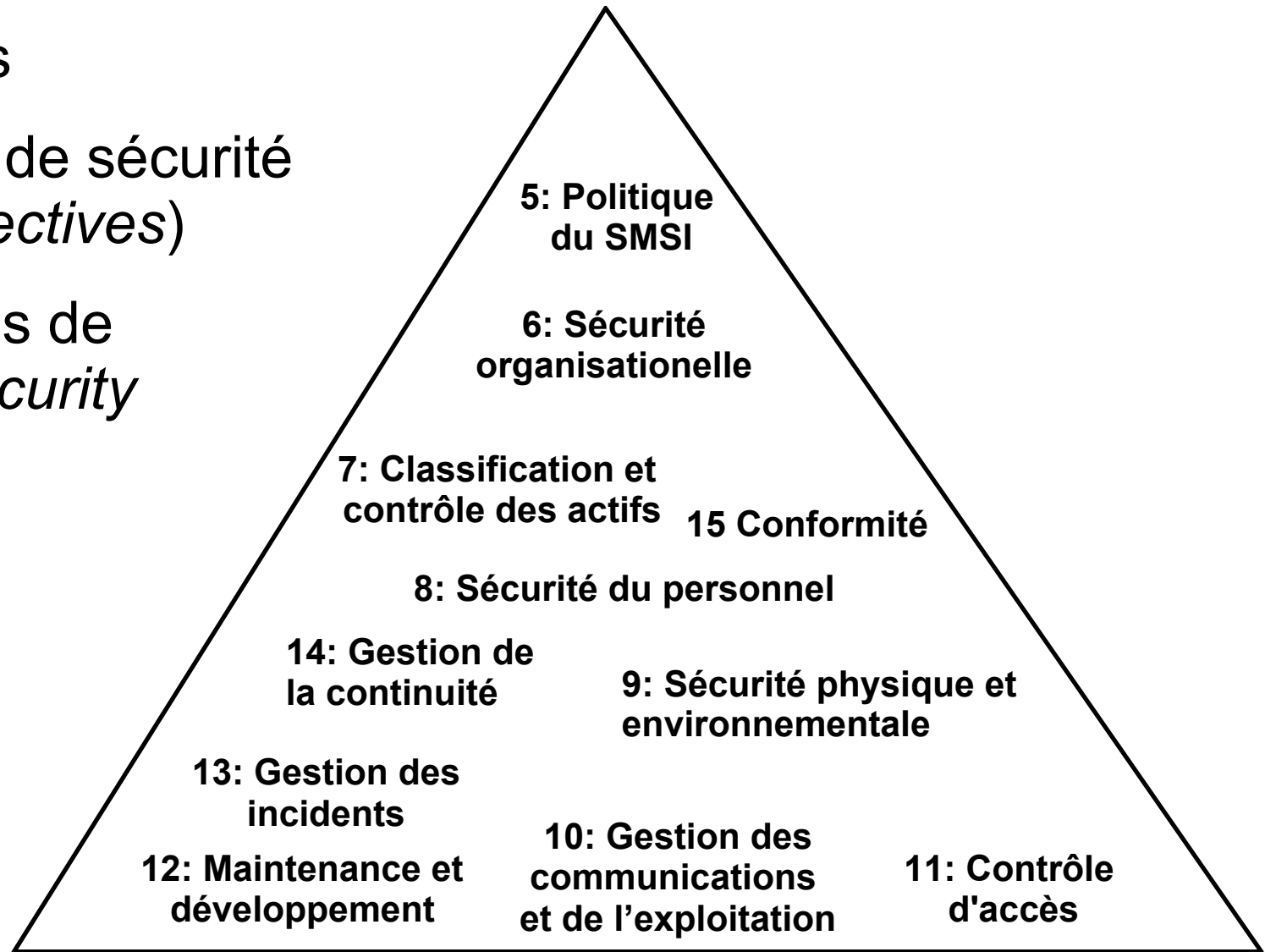
- Phase *PLAN* (4.2.1)
 - Périmètre du SMSI (4.2.1.a)
 - Politique de sécurité et/ou politique du SMSI (4.2.1.b)
 - Plan de gestion des risques
 - Méthodologie d'appréciation des risques (4.2.1.c)
 - Identification et évaluation des risques (4.2.1.d) (4.2.1.e)
 - Traitement des risques (4.2.1.f)
 - Réduction des risques à un niveau acceptable
 - Conservation (acceptation) des risques
 - Refus ou évitement des risques
 - Transfert
 - 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* (4.2.2)
 - 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* (4.2.3)
 - 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^(4.2.4)
 - 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
 - Actions entreprises immédiatement
 - Planification d'actions sur le moyen et long terme

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

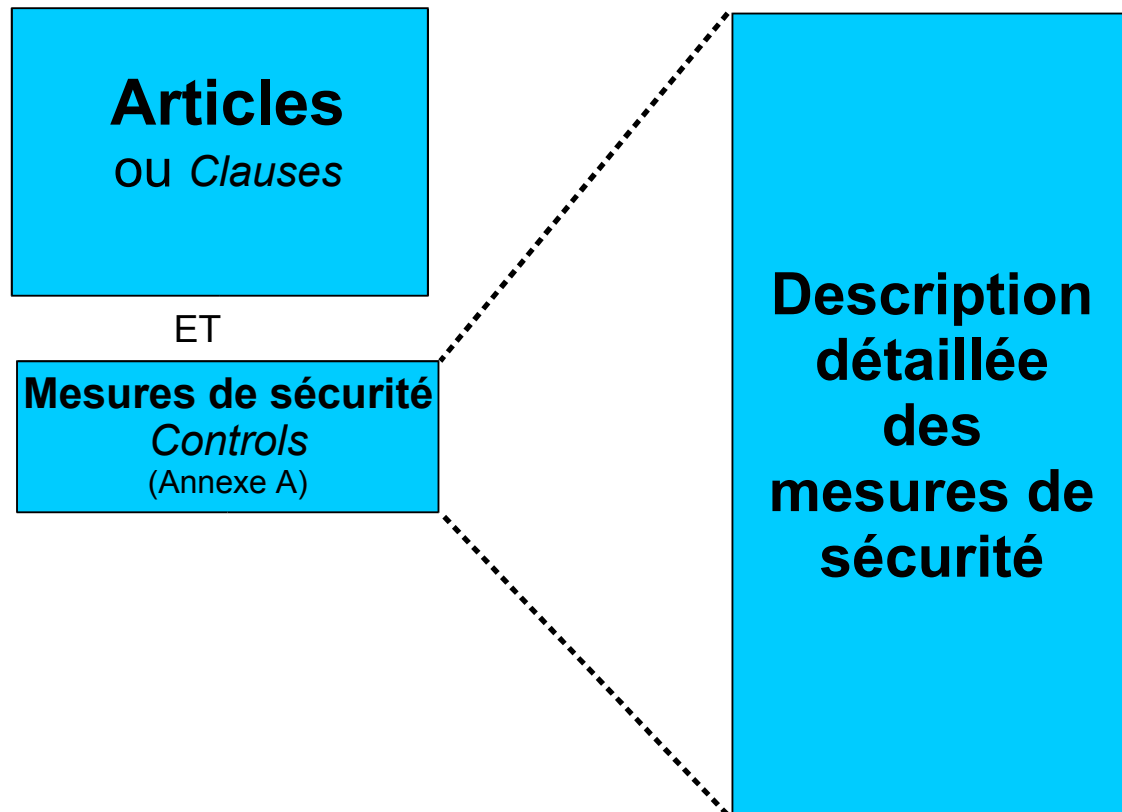


- Anciennement ISO 17799
- Recommandations ou exigences en sécurité
- Reprennent les recommandations classiques des experts en sécurité
 - Certaines mesures de sécurité sont très générales, d'autres très précises
 - Certaines mesures sont applicables à tout l'organisme, d'autres à un serveur ou une application 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 appréciation des risques

ISO 27001

ISO 27002

(anciennement ISO 17799)



- ISO27000 : Principes et vocabulaire
 - Issu en partie des parties 1 et 2 de l'ISO13335 (anciennement MICTS partie 1)
- ISO27003 : Guide d'implémentation d'un SMSI
 - Document de travail du groupe de normalisation
 - Pratique et détaillé
 - Déjà utilisable en l'état, surtout pour la phase plan

- Mesurage du Management de la Sécurité de l'Information
 - *Security control* → mesure de sécurité donc pour éviter les confusions :
Measurement → mesurage
 - Guide de mise en place du mesurage du SMSI
 - Etat : CD, publication prévue en 2008, déjà utilisable et très utile
 - Objectif : mesurer l'efficacité du SMSI et des mesures de sécurité
 - Programme de mesurage et processus de mesurage
 - Rôles et responsabilités
 - Méthodologie de choix des indicateurs
 - Production et exploitation des indicateurs
 - Analyse et restitution des indicateurs
 - Amélioration du processus de mesurage
 - Exemples d'indicateurs

Mesure	Entrevues archivées - Processus de revue	
Référence		
Clause ou Mesure de sécurité	7.1 b, 7.2 i,	
Type	Conformité	
Mesure de base / dérivée	Base	
Objectif	Déterminer le niveau d'implication des managers dans le SMSI	
Formule de calcul	$X = (A / B)$ <p>A = Somme des entevues programmées ayant été tenues en temps et en heure B = Sommes de entrebues programmées</p>	
Valeur	Rapport	
Domaine de définition	Entre 0 et 1	
Procédure de production	P-EDKS-V2	
Personnes concernées	Propriétaire	ISMS manager
		ISMS management committe
	Client	ISMS manager
	Collection	Quality System Manager
	Communication	ISMS Managemeznt committee
	Révision	ISMS manager
Cycle de vie	Fréquence	Tous les trimestres
	Date	Cf calendrier des indicateurs
	Procédure d'enregistrement	P-EDKS-V2
	Périodicité du rapport	Trimestriellement
	Durée de validité de la mesure	
	Période d'analyse	Du 1er janvier au 31 Décembre de l'année courrante
Objet concerné		
Critères de décision	<p>0 < X < 0,79 : Non satisfaisant 0,80 < X < 1 : Satisfaisant</p> <p>Si, à la fin de second semestre X < 0,80, alors une action corrective risque d'être nécessaire et communiquée au management du SMSI.</p> <p>Si, à la fin de l'année X est on satisfaisant, la direction générale doit en être informée et on doit lui demander son soutien</p>	
	Indicateur	Non-conformité du SMSI.
	Effets / Impact	Pas de garantie que le processus de revue du SMSI fonctionne bien
		Budget insuffisant
	Causes d'écart	Planification incorrecte
	Valeurs positives	Manque d'engagement du personnel concerné
		Des valeurs en augmentatin indiquent des valeurs positives
	Format de rapport	Barres
Remarques	Herve Schauer Consultants 2000-2007 - Reproduction Interdite	

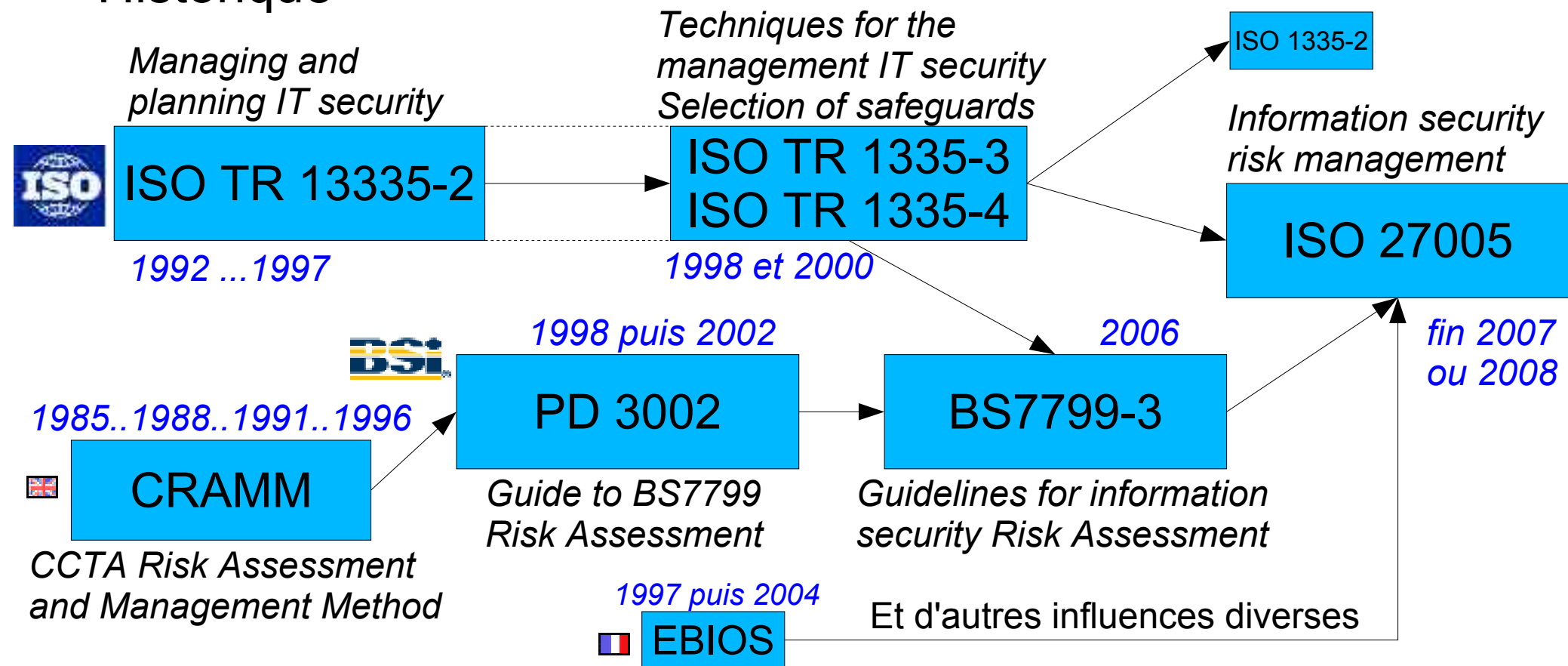
- Guide de mise en oeuvre de la partie appréciation des risques de la sécurité de l'information de l'ISO 27001
 - ISO 27001 4.2.1 c) à 4.2.1 f) 4), plus 4.2.3.d)
 - soit 1 page + 3 ou 4 lignes
- Etat : FCD, publication prévue en 2007 ou 2008

ISO 27001 4.2.1 c) → 4.2.1 f)

- ISO 27005
 - 64 pages
 - 28 pages normatives, chap 1 à 12
 - 36 pages d'annexes A à E

ISO 27005

- Historique

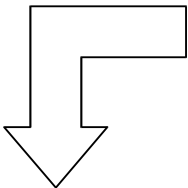
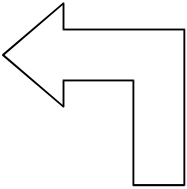


- CCTA est devenu l'OGC, le même organisme gouvernemental britannique qui a fait et est propriétaire d'ITIL
- Attention : CRAMM a été privatisé en 1996

- Rappel : norme = **consensus** entre les acteurs du marché
 - Ne peut être plus complet que toutes les méthodes qui l'ont précédé
 - Représente le noyau commun accepté par tous
 - Peut être complété en allant rechercher ailleurs
- Méthodes d'analyse de risques existantes
 - Continuent à évoluer et innover
 - Contribuent à l'amélioration de la norme ISO 27005
 - A terme certaines méthodes se diront "conformes à la norme ISO 27005"

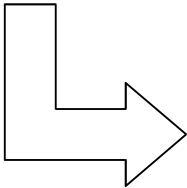
- Est cependant suffisante dans la majorité des cas
- Oblige déjà beaucoup à structurer sa pensée et sa démarche
- Correspond strictement au respect de l'ISO 27001
 - Nécessaire pour la mise en place d'un SMSI
 - Nécessaire pour une certification

- Définition d'un **processus**
 - Continu et qui s'améliore, donc PDCA
- Processus de **gestion de risque de la sécurité de l'information**
 - (*information security risk management process*)
- Processus applicable à tous le SMSI ou à un sous-ensemble

- 
- Identifier les risques
 - Quantifier chaque risque par rapport
 - aux conséquences que sa matérialisation pourrait avoir sur le business
 - à sa probabilité d'occurrence (*likelihood*)
 - Identifier les actions appropriées pour réduire les risques identifiés à un niveau acceptable
- 
- Plan**

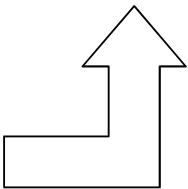
- Implémenter les actions pour réduire les risques
 - Eduquer la direction et le personnel sur les risques et les actions prises pour les atténuer
- Do**

- Rectifier le traitement du risque à la lumière des événements et des changements de circonstances
 - Améliorer le processus de gestion du risque
- Act**

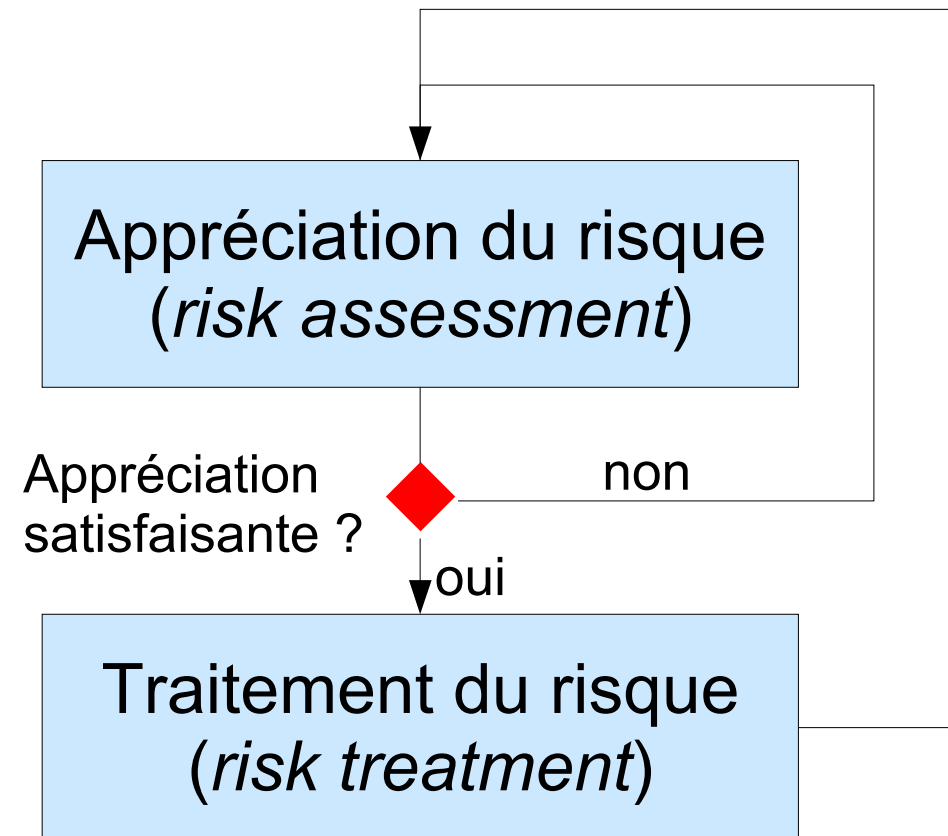


Surveiller et réexaminer les résultats, l'efficacité et l'efficience du processus

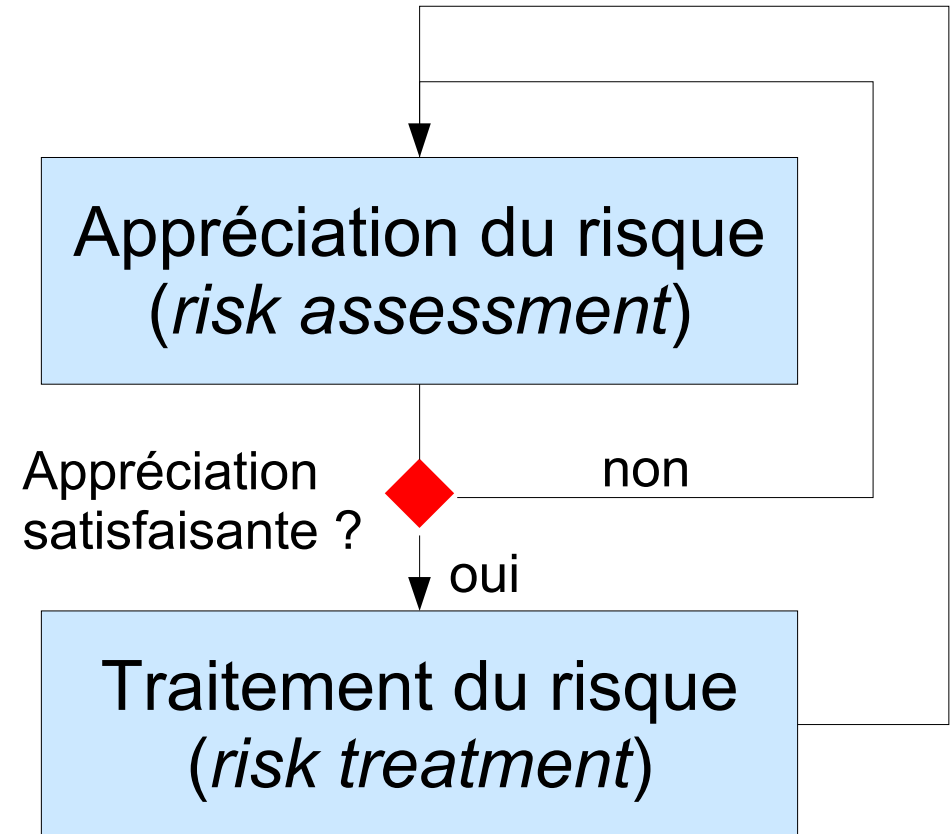
Check



- Décomposé en deux activités séquentielles et **itératives**
- Approche itérative
 - Améliore la finesse de l'analyse à chaque itération
 - Garanti une appréciation des risques élevés
 - Minimise le temps et l'effort consenti dans l'identification des mesures de sécurité
- Appréciation des risques satisfaisante ?
 - Passer au traitement du risque



- Approche itérative ou cyclique
 - Permet d'**avancer** avec des
 - Interlocuteurs absents ou incapables de savoir ou qui refusent de répondre
 - Livrables incomplets
 - Incapacité du management de se prononcer sur l'approbation des risques résiduels sans connaître d'abord les coûts associés
 - Facilite la gestion des susceptibilités et des aspects politiques entre
 - Interviewvés
 - Actifs et processus métier



- Facilite les liens entre les risques et les impacts sur les processus métier

- Appréciation du risque ⁽⁸⁾
 - Analyse des risques
 - Mise en évidence des composantes des risques
 - Estimation de leur importance : **méthode de calcul laissée libre**
 - Evaluation des risques
 - Analyse d'ensemble et prise de décision sur les risques
- Traitement du risque ⁽⁹⁾
 - Sélection des objectifs et mesures de sécurité pour réduire le risque
 - Refus, transfert ou conservation du risque
- Acceptation du risque ⁽¹⁰⁾
 - Approbation par la direction des choix effectués lors du traitement du risque
- Communication du risque ⁽¹¹⁾

♦ n° 1

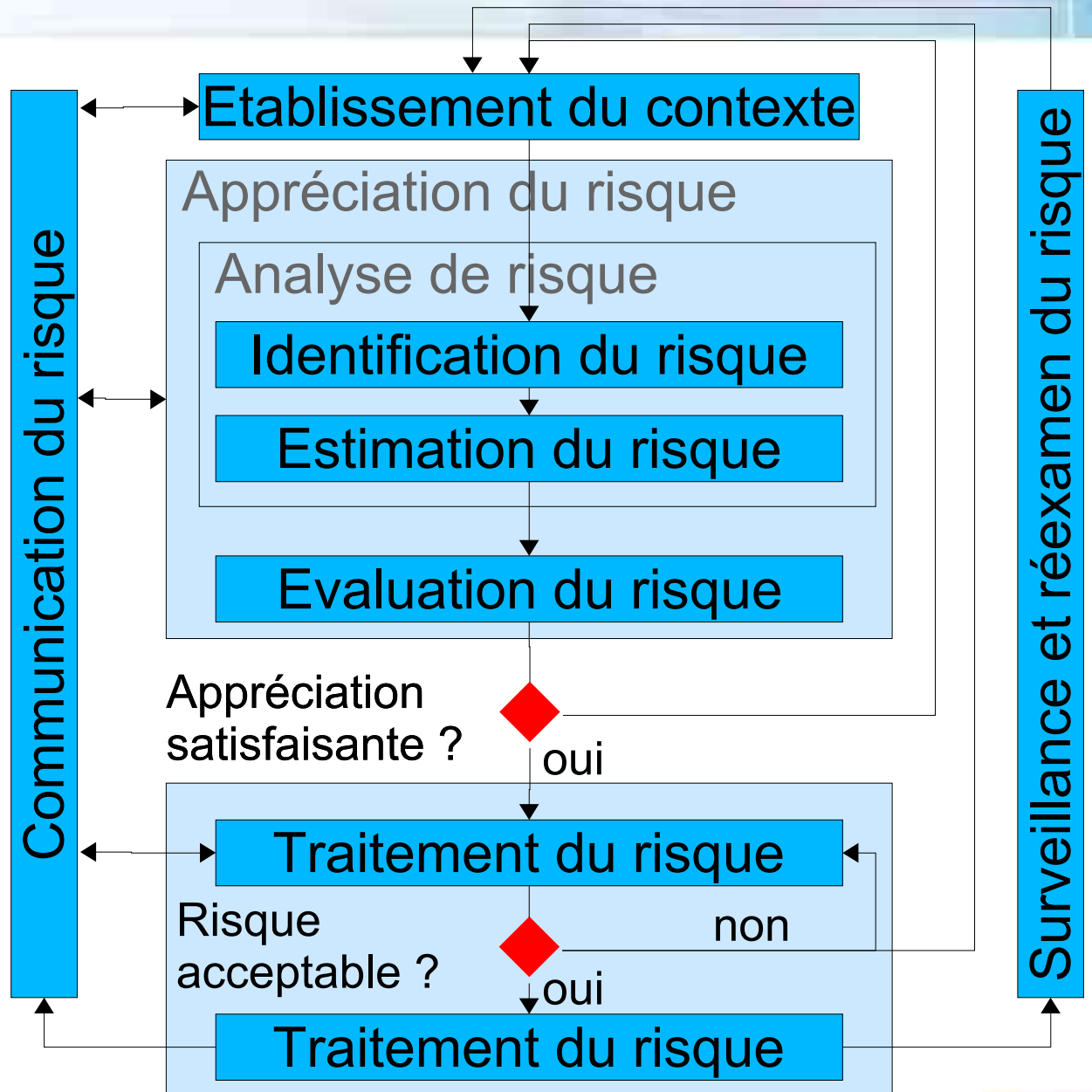
- Assez d'éléments pour déterminer les actions nécessaires à la réduction des risques à un niveau acceptable ?

♦ n° 2

- Risque acceptable ?

Communication à la hiérarchie et aux équipes opérationnelles à chaque étape

- Risque identifié utile immédiatement à la gestion des incidents



- Exigences pour l'accréditation des organismes de certification des SMSI
 - Remplace la norme EA 7/03
 - S'appuie sur la norme ISO 17021
 - Apporte des précisions pour les audits de certification ISO 27001
 - Classement des mesures de sécurité : organisationnelles / techniques
 - Vérifications à faire ou pas pour les mesures de sécurité techniques
- ISO27007 : Guide d'audit de SMSI
 - Etait à l'origine dans l'ISO 27006, séparé pour ne pas être obligatoire

- Normes ISO 2703X
- Ajoutent ou modifient l'application de l'ISO27002 pour un secteur d'activité
 - Opérateurs de télécommunications
 - Secteur financier
 - Industrie des jeux
 - Industrie automobile
- Santé : ISO 27799:2006
 - Fait dans la normalisation de la santé
 - Adaptation de l'ISO27001 et ISO27002 en un seul document pour le secteur de la santé
 - Caractère d'application des mesures de sécurité obligatoires dans certains cas
 - Sera sans doute renuméroté en ISO 2703X dans une prochaine version

- Pour adopter les bonnes pratiques en SSI
 - ISO 27001 + ISO 27002 (anciennement ISO17799)
 - Constat objectif que vous adoptez les bonnes pratiques en matière de SSI
 - Processus d'amélioration continue, donc le niveau de sécurité a plutôt tendance à croître
 - Meilleure maîtrise des risques
 - Méthodologie d'appréciation des risques (méthode d'analyse de risque)
 - Diminution de l'usage des mesures de sécurité qui ne servent pas
 - Peut permettre d'évoluer, le moment venu, vers une certification

- Pour homogénéiser
 - ISO27001 + ISO27002 (ISO17799)
 - Référentiel universel, international, sans concurrence
 - Permet des comparaisons entre entités, sites, pays
 - Facilite les échanges d'expérience et la communication interne
 - Facilite les liens avec les autres métiers et les autres référentiels
 - Facilite la communication aux auditeurs hors de la SSI
- Pour les tableaux de bord
 - ISO27001 + ISO27002 (ISO 17799) + ISO27004
 - ISO27001 pour le SMSI nécessaire à l'élaboration de métriques
 - ISO27002 pour les mesures de sécurité à mesurer
 - ISO27004 pour le mesurage d'un SMSI

- Pour les audits conseils en sécurité
 - ISO 27002 (ISO 17799)
 - Conclusions font référence aux mesures de sécurité de la norme
 - Espéranto de la sécurité
- Pour donner une image de sérieux aux partenaires
 - ISO 27001 + éventuellement certification, au moins à terme
 - Constat extérieur, objectif et à terme officiel que "vous adoptez les bonnes pratiques en matière de SSI"
 - Un minimum de base
 - Une amélioration continue

- Pour communiquer formellement aux parties prenantes
 - Ou au moins une partie prenante le demande
 - ISO 27001 + certification
 - Constat impartial, objectif et officiel que "vous adoptez les bonnes pratiques en matière de SSI"
 - Engagement dans la durée

- Pour réduire les coûts
 - *D'après ceux qui ont mis en oeuvre...*
 - Mutualisation des audits
 - Diminution d'usage de mesures de sécurité inutiles
 - Processus en lui-même plutôt moins coûteux que d'autres en SSI

Processus de certification

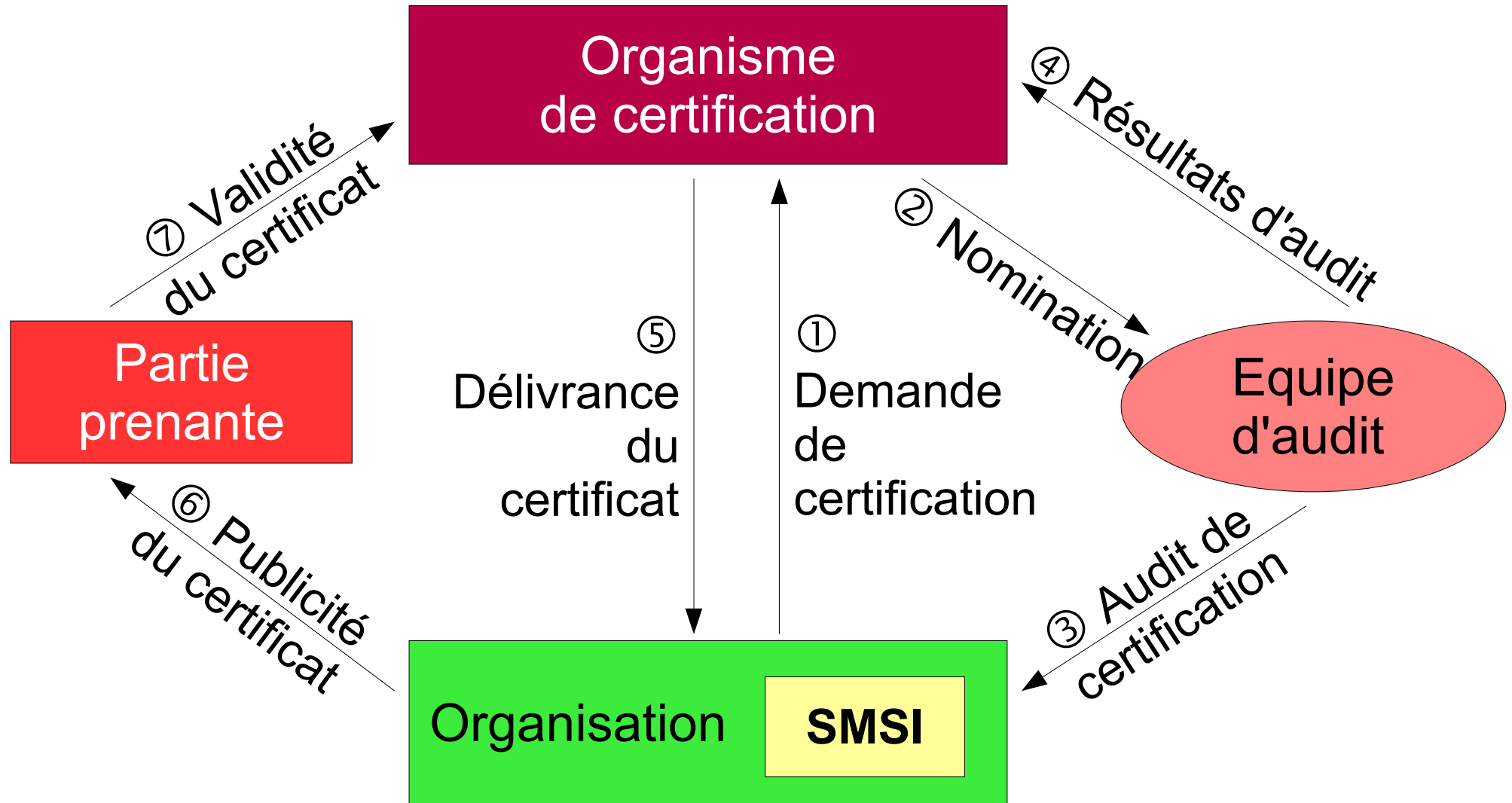
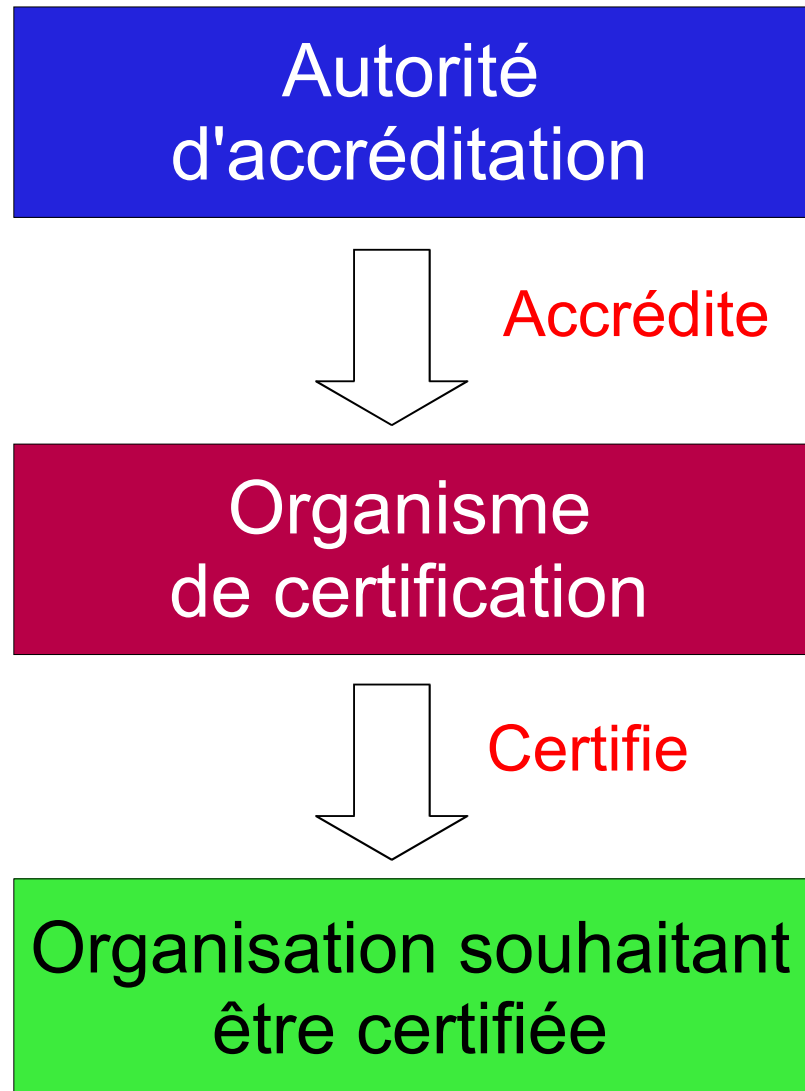


Schéma de certification



- Schéma commun à toutes les certifications
- Autorité d'accréditation
 - Une seule par pays
 - Organisme d'état
- Organisme de certification (IS 17021 1)
 - Nombreux
 - Généralement des sociétés privées
 - Peut être un organisme gouvernemental
 - Avec ou sans pouvoir réglementaire

Conclusion

- ISO 27001 : approche adoptée universellement
- Aucune concurrence
- Complémentarité avec les autres référentiels
 - ITIL / ISO 20000 appliqué par les directions informatiques
- Permet ou permettra de démontrer la conformité en SSI à tous les autres référentiels ou règlements
 - SoX et SAS70, Commission bancaire, Cour des comptes
- France : seul pays d'europe n'ayant pas (ou si peu) de certificats ISO 27001

Questions ?

Herve.Schauer@hsc.fr

www.hsc.fr