



Club 27001



21 - 22 novembre 2007

CNIT - Paris La Défense

SMSI et normes ISO 27001

introduction et perspectives

Conférence "SMSI et normes 27001"
21 novembre 2007



Hervé Schauer
Eric Doyen

- Cahiers Oxford (publicité)
- Roue de Deming
- ISO 27001
- Ensemble des normes ISO 27001
 - ISO 27000, ISO 27002, ISO 27003, ISO 27004
- ISO 27005 : gestion du risque SSI
- Club 27001
- Programme

**Les transparents seront
disponibles sur
www.club-27001.fr**

- Cahiers Oxford Etudiant en vente lors de chaque rentrée
- «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 d'eux. 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'aimable
autorisation du
Groupe Hamelin

- Rappel aux élèves de ce qu'est un système de management
 - Pour travailler intelligemment

▶ 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 :

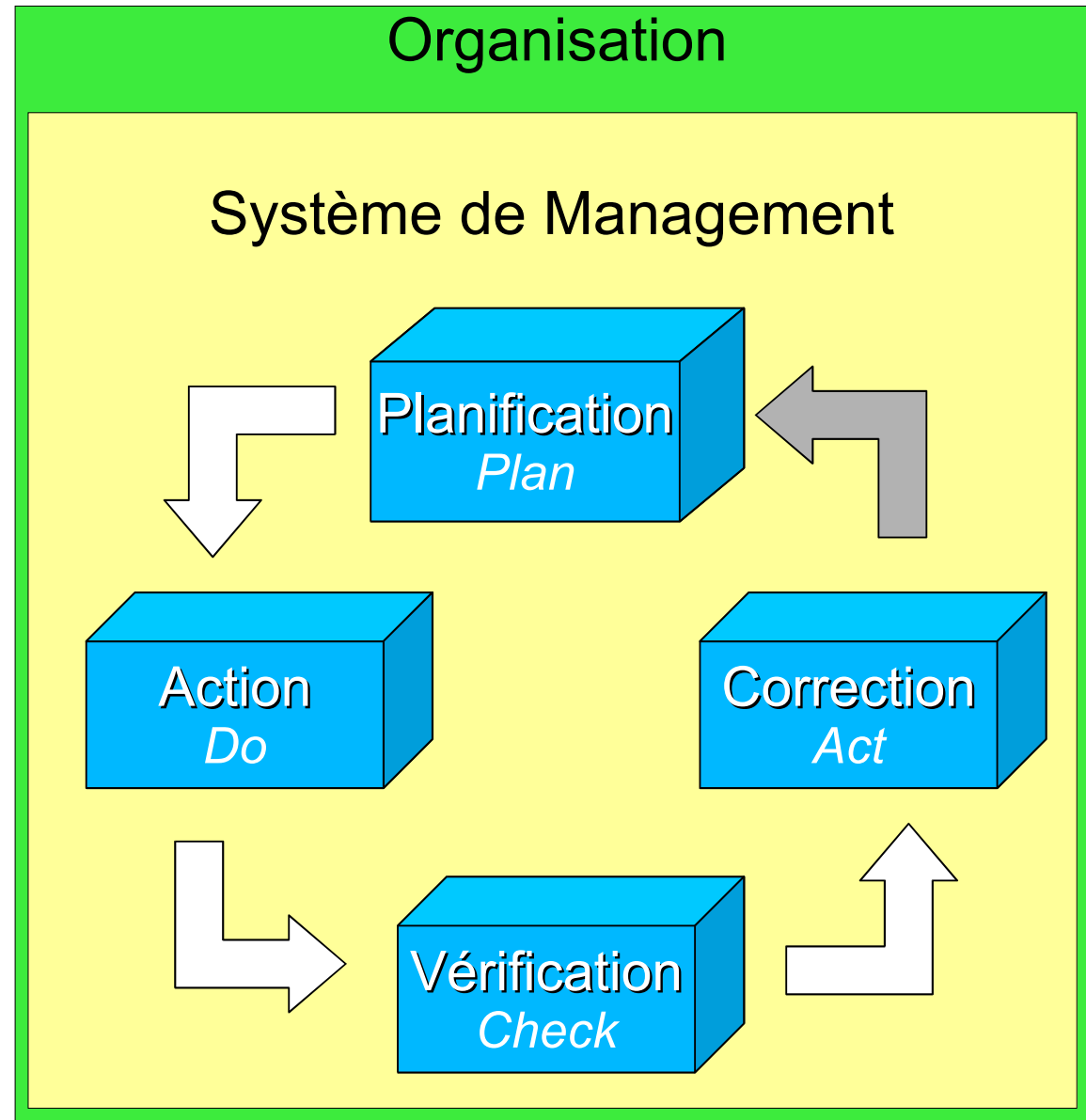


Attention : Il est important de garder à l'esprit qu'une stratégie ne se met véritablement en place qu'à partir du moment où les objectifs sont personnalisés, de même que le temps passé à la réflexion et à l'analyse est du temps gagné pour l'action qui se déroulera plus vite et plus sûrement.

Reproduit avec l'autorisation du Groupe Hamelin



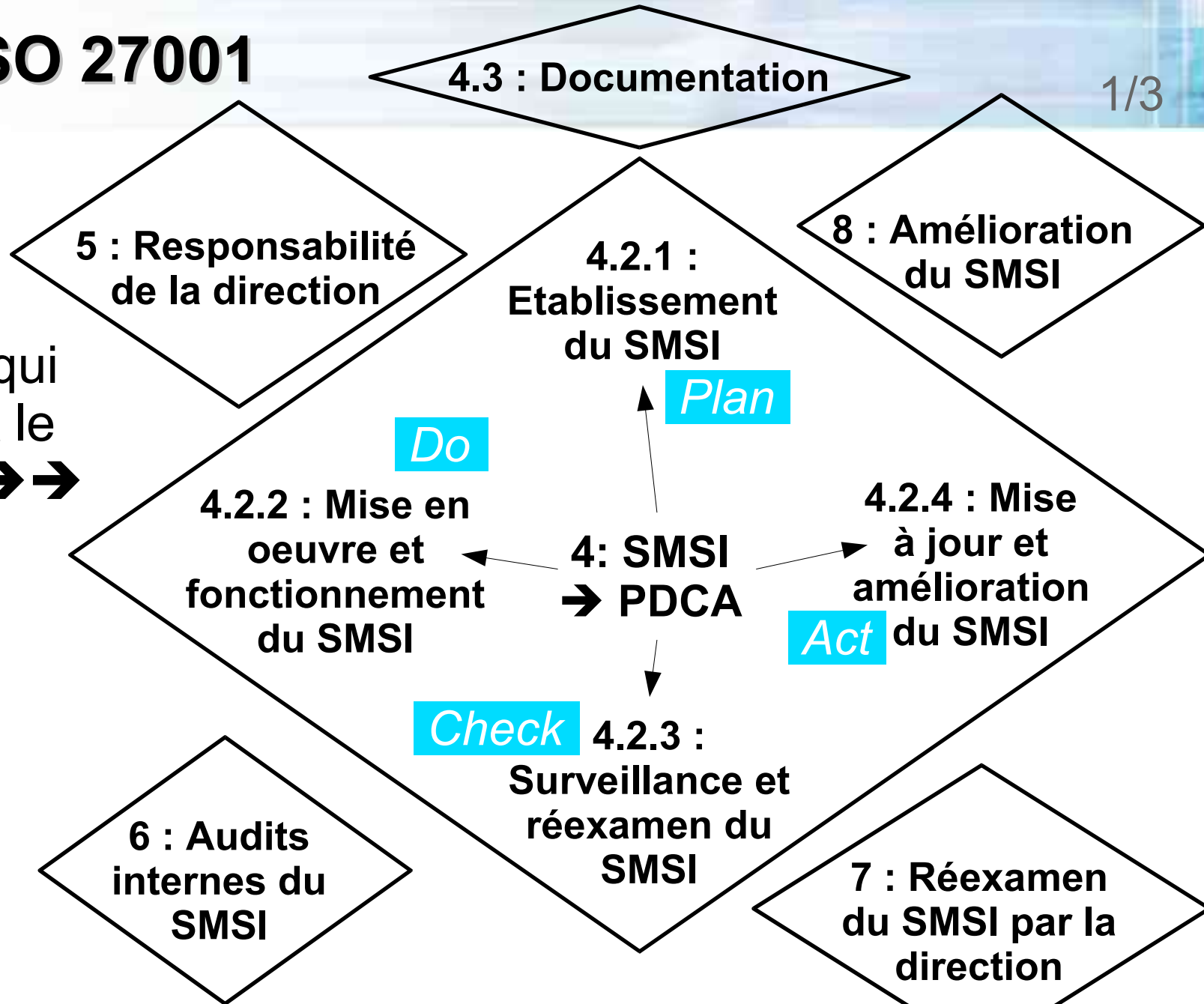
- William Edwards Deming
 - Scientifique américain
 - Inventeur des principes de la **qualité**
 - Reconstructeur du Japon par l'application de ces principes à partir de 1950
- Walter Andrew Shewhart
 - Statisticien américain
 - Inventeur de la roue de Deming
 - Que Deming appelait roue de Shewhart et qu'il lui a emprunté en **1922**



- Principes de la **qualité**
- Systèmes de management :
 - de la **qualité** (SMQ) : ISO 9001:2002
 - **environnemental** (SME) : ISO 14001:2004
 - de la **santé** et la **sécurité** au **travail** (SMSST) : OHSAS 18001:1999
 - **de la sécurité de l'information (SMSI) : ISO/IEC 27001:2005**
 - de la **sécurité alimentaire** (SMSA) : ISO 22000:2005
 - des **services informatiques** des organismes : ISO 20000:2005
 - Issu d'ITIL
 - de la **sûreté** pour la **chaîne d'approvisionnement** : ISO 28000:2005
 - ...



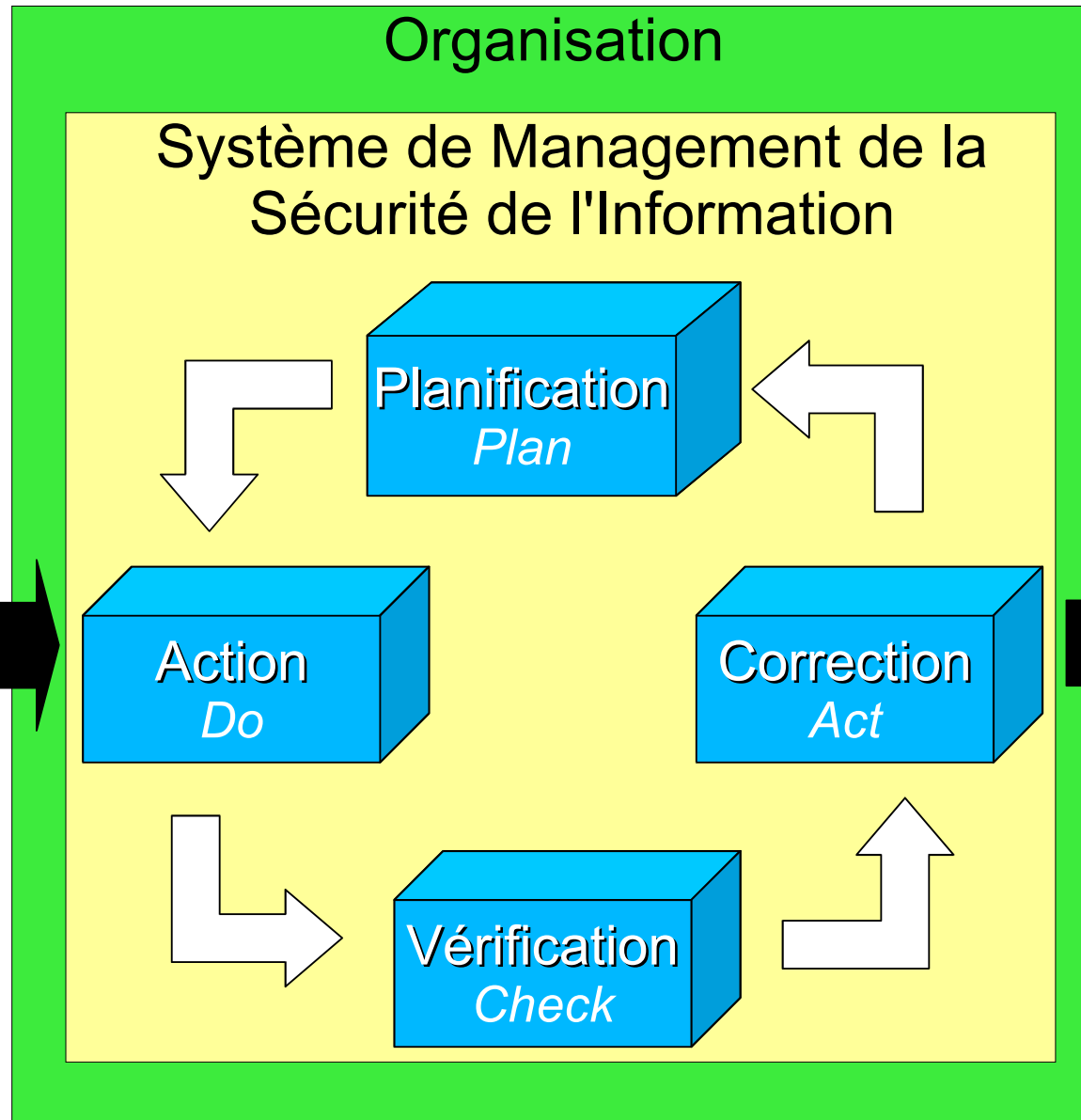
- Norme
- 5 chapitres qui construisent le **SMSI** →→→→
- Annexe A : mesures de sécurité



- Application de la **qualité** pour la **sécurité de l'information**
 - **Systeme de Management de la Sécurité de l'Information (SMSI)**
- Référentiel précis et auditable
- Apporte la **confiance**
- Confiance → **business**

Attentes et exigences en terme de sécurité

- Partenaires
- Fournisseurs
- Clients
- Pouvoirs publics
- Services



Sécurité effective fournie

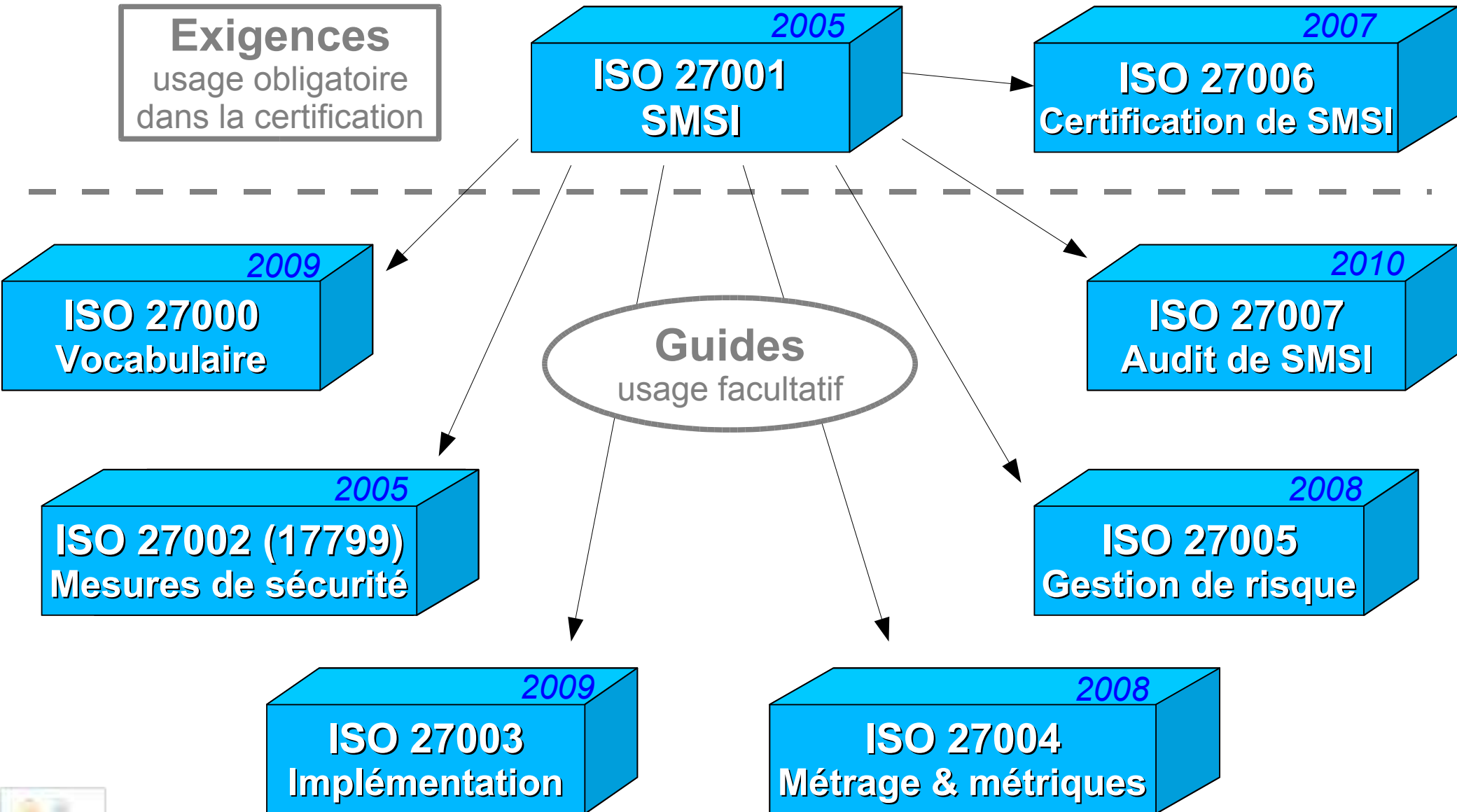
- Partenaires
- Fournisseurs
- Clients
- Pouvoirs publics
- Services



- Amélioration continue
 - Gestion du temps
 - Ce qui n'a cessé de manquer à la SSI depuis son existence
- Universalité
 - Pas de concurrence
 - Applicable à tous les métiers, à tous les secteurs d'activité
 - Applicable à toutes les tailles d'entreprises ou de périmètres
- Complétude
 - Méthodologie d'appréciation des risques
 - Méthodologie de construction d'indicateurs
 - ...

- Construit un **processus**
 - Processus d'amélioration continue
 - → pas un **niveau** de sécurité
 - Donc accessible à tous
- Application de mesures de sécurité pertinentes
 - Pour réduire de vrais risques
 - Sur de vrais actifs
 - Avec une vraie valeur
 - Même si vous faites une rétro analyse au départ
 - → Pas des cases à cocher bêtement sans savoir pourquoi

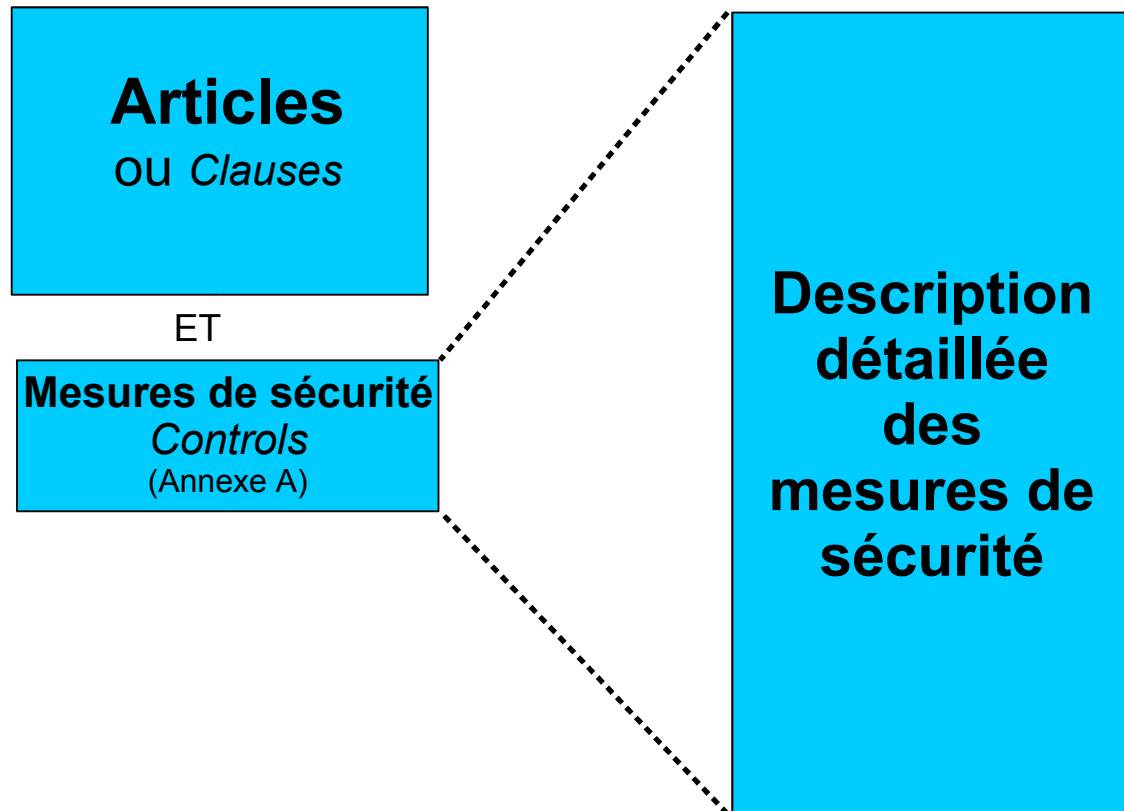
- Dialogue et communication
 - Compréhensible par la direction générale
 - Facilite l'implication des métiers
 - Permet à la SSI d'entrer dans la gouvernance comme le reste
 - Lien avec les processus ISO 2000-1 (ITIL) pour la production informatique
 - Meilleure lisibilité de la SSI et du rôle du RSSI
 - ➔ Compréhensions mutuelles



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

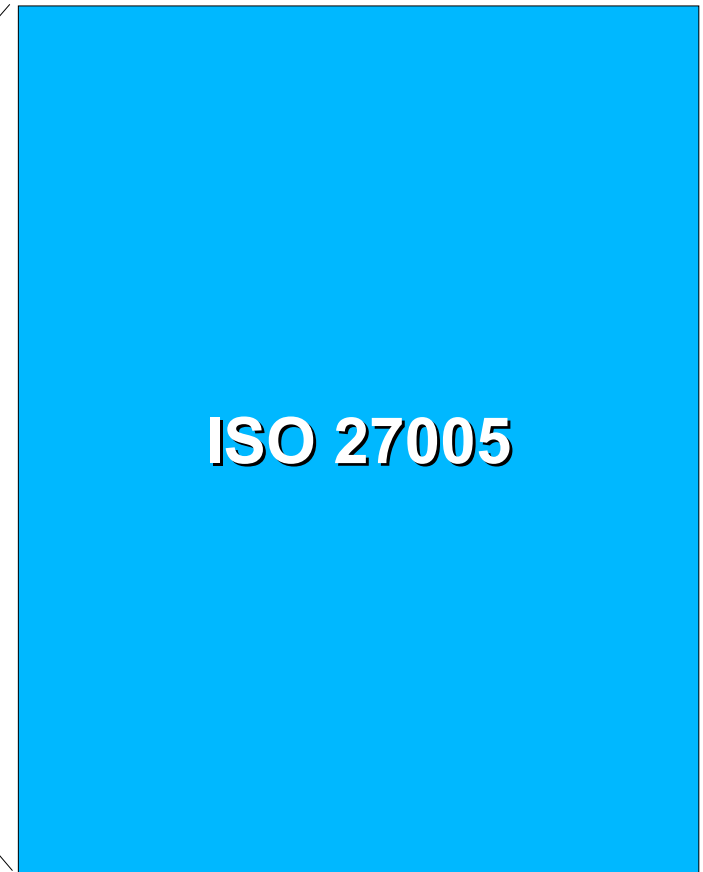
Mesure	Entrevues archivées - Processus de revue	
Référence		
Clause ou Mesure de sécurité	7.1 b, 7.2 i,	
Type	Conformité	
Mesure de base / dérivée	Base	
Objectif	Déterminer le niveau d'implication des managers dans le SMSI	
Formule de calcul	$X = (A / B)$ A = Somme des entevues programmées ayant été tenues en temps et en heure B = Sommes de entrebues programmées	
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
		Quality System Manager
	Collection	Quality 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	0 < X < 0,79 : Non satisfaisant 0,80 < X < 1 : Satisfaisant Si, à la fin de second semestre X < 0,80, alors une action corrective risque d'être nécessaire et communiquée au management du SMSI. 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	
Indicateur	Effets / Impact	Non-conformité du SMSI. Pas de garantie que le processus de revue du SMSI fonctionne bien
		Budget insuffisant
		Planification incorrecte
	Causes d'écart	Manque d'engagement du personnel concerné
	Valeurs positives	Des valeurs en augmentatin indiquent des valeurs positives
	Format de rapport	Barres
Remarques	© Schrauer Consultants 2000-2007 - Reproduction Interdite	



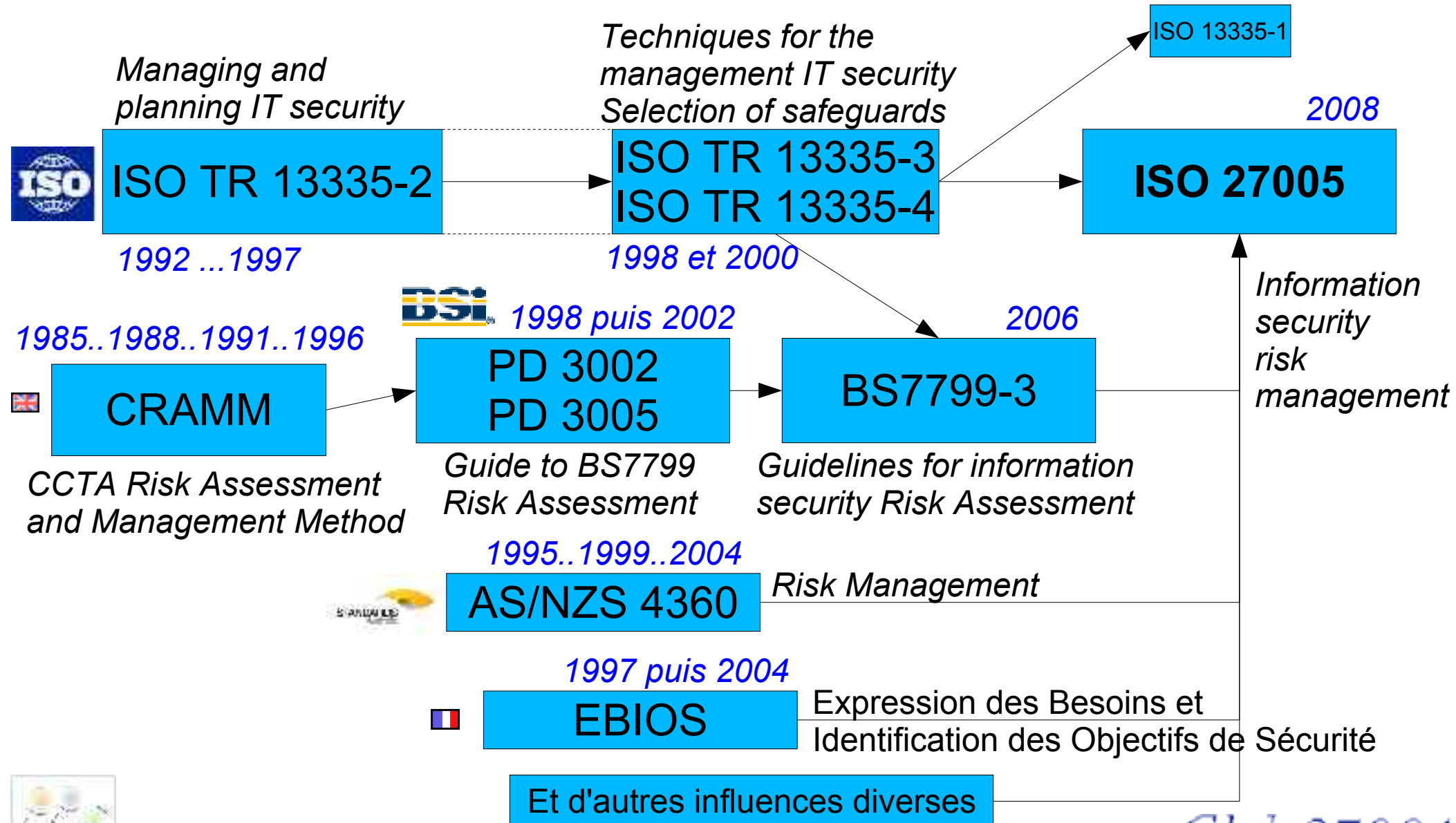
- Guide de mise en oeuvre de la partie appréciation des risques de la sécurité de l'information de l'ISO 27001
 - ISO 27001 4.2.1 c) à 4.2.1 f) 4), plus 4.2.3.d)
 - soit 1 page + 3 ou 4 lignes
- Etat : FCD, publication prévue début 2008

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

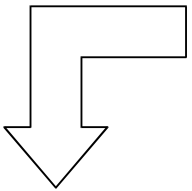
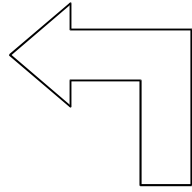


- Norme → **consensus** entre les acteurs du marché
- ISO 27005
 - Ne peut être plus complet que toutes les méthodes qui l'ont précédé
 - Représente le noyau commun accepté par tous
 - Peut être complété en allant rechercher ailleurs
- Méthodes d'appréciation des risques existantes pourront
 - Continuer à évoluer et innover
 - Contribuer à l'amélioration de la norme ISO 27005
 - Compléter la norme
 - Se qualifier de "conformes à la norme ISO 27005"

- ISO 27005 = Méthodologie complète
 - Structure sa démarche
 - Autonome
- Correspond strictement au respect de l'ISO 27001
 - Nécessaire pour la mise en place d'un SMSI
 - Nécessaire pour une certification
- Entrera dans la gestion de risque en général
 - Normalisation ISO 31000 de tous les types de risques : financiers, industriels, routiers, santé, ...
- Vocabulaire
 - Compréhensible et plutôt proche du langage courant

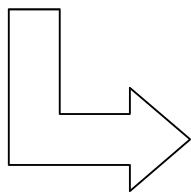
- Choix de traduction dans l'ISO 27001
 - *Risk Analysis* → Analyse du risque
 - *Risk Estimation*^(3.4) → Estimation du risque
 - *Risk Evaluation*^(3.5) → Evaluation du risque
 - *Risk Assessment* ^(IS27001 3.12) → Appréciation du risque
- Langage courant
 - Analyse de risque ⇔ *Risk Assessment*
 - Usage **impossible** à garder sans confusions
 - Pas d'autre traduction possible que *Risk Analysis* → Analyse du risque
 - Confusion avec *Risk Assessment*
- Donc : ***Risk Assessment* → Appréciation du risque**
- Processus dans son ensemble

- Définition d'un **processus**
 - Continu et qui s'améliore, donc PDCA
 - Principe de la reproduction du PDCA général du SMSI à chaque processus dans le SMSI
- 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
- Inclus une étape pour prendre en compte les coûts et mettre la direction devant ses responsabilités

- 
- 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**
- 

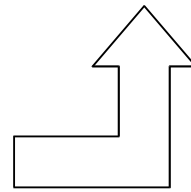
- Implémenter les actions pour réduire les risques
 - Eduquer la direction et le personnel sur les risques et les actions prises pour les atténuer
- Do**

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

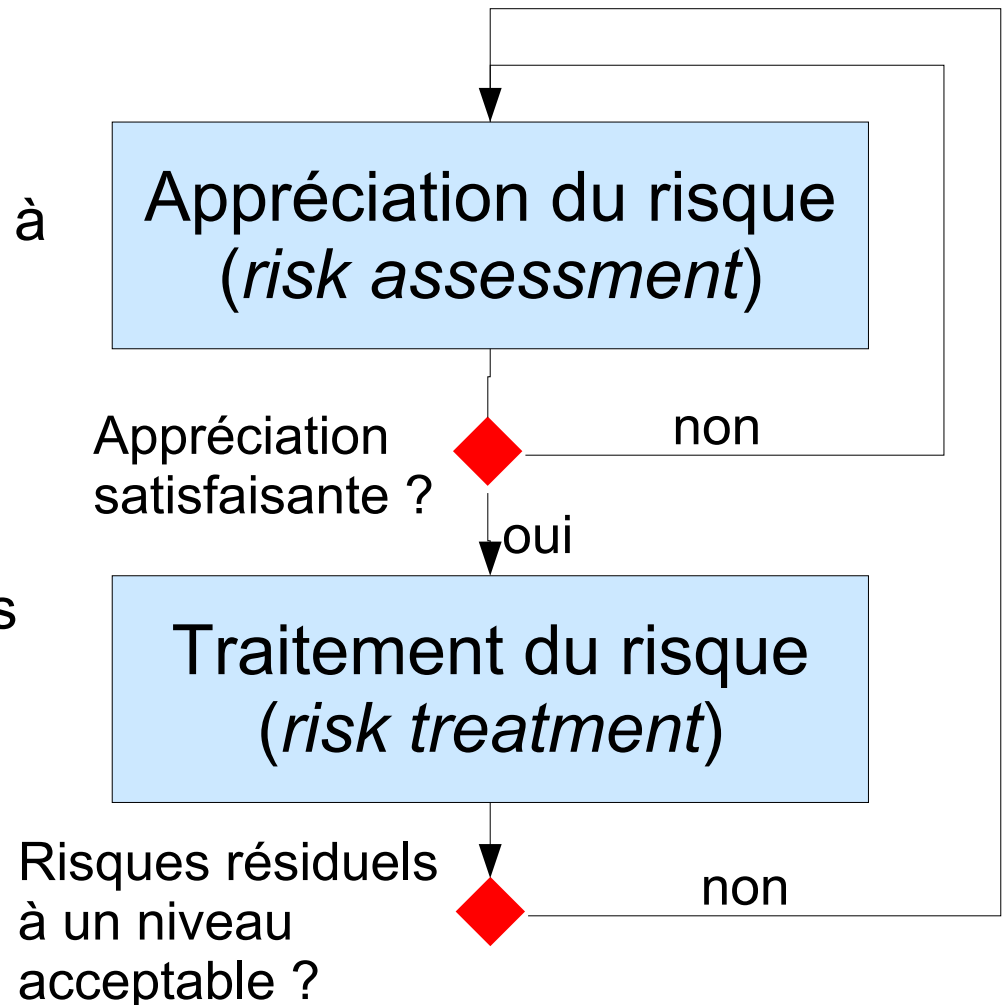


Surveiller et réexaminer les résultats, l'efficacité et l'efficience du processus

Check



- Processus de gestion de risques décomposé en deux activités séquentielles et **itératives**
- Approche itérative
 - Améliore la finesse de l'analyse à chaque itération
 - Garantie une appréciation des risques élevés
 - Minimise le temps et l'effort consenti dans l'identification des mesures de sécurité
- Appréciation des risques satisfaisante ?
- Risques acceptables ?



◆ n° 1

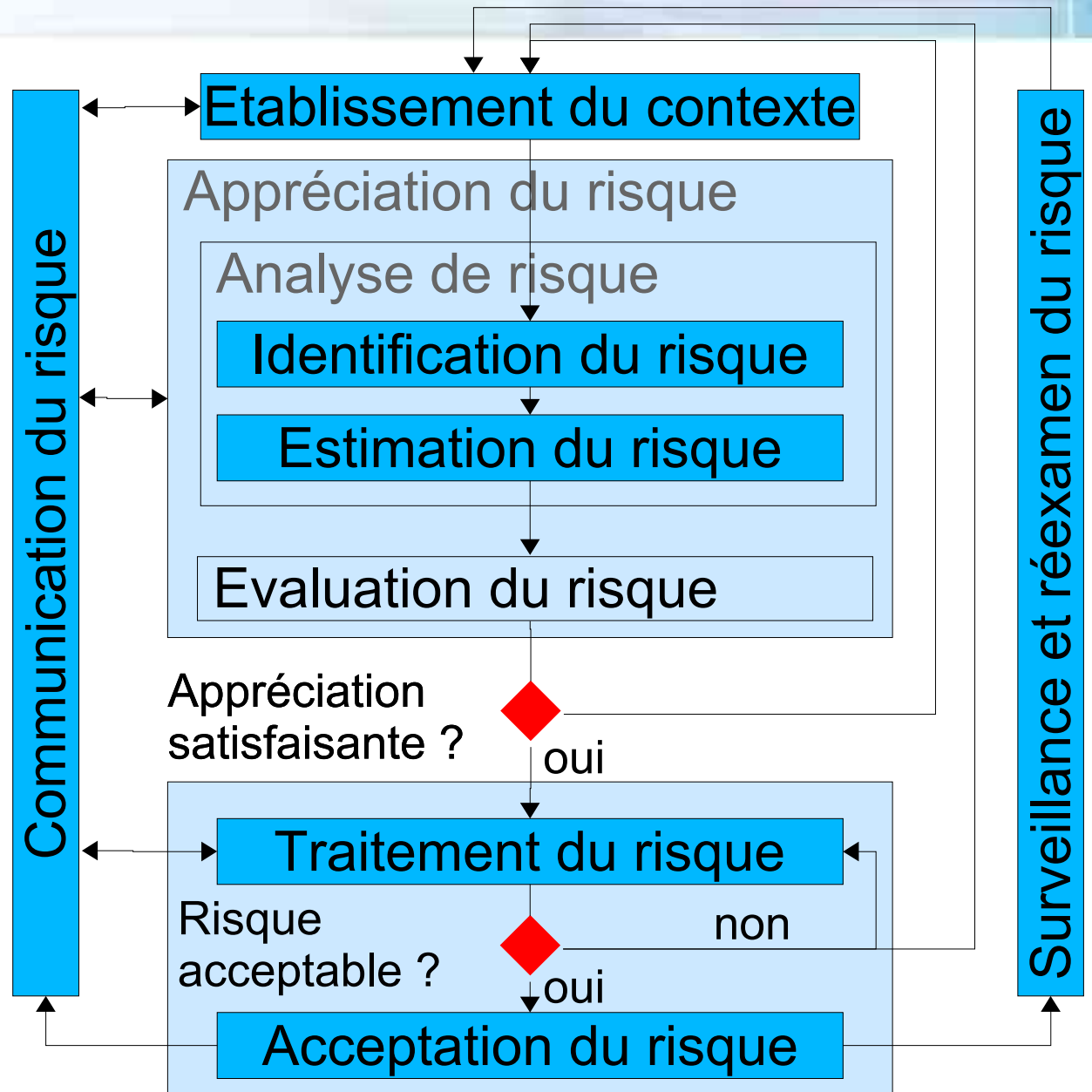
- Assez d'éléments pour déterminer les actions nécessaires à la réduction des risques à un niveau acceptable ?

◆ 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
 - S'appuie sur la norme ISO 17021 (et remplace EA 7/03)
 - Quelques exigences pour les audits de certification ISO 27001
 - Production par l'appréciation des risques de résultats comparables et reproductibles (9.2.3.2.2 a)
 - Analyse de la sécurité par rapport aux menaces pertinente (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 (9.2.3.3.b)
 - Vérifications concrètes pour les mesures de sécurité techniques
 - Calcul du nombre de jours d'audit adaptés aux SMSI
 - SMSI doit avoir vécu au minimum pour être certifié : (9.2.5)
 - 1 audit interne complet du SMSI
 - 1 revue de direction

- Reflexions et échanges autour des normes
- Ouvert à tous
- Trois groupes :
 - Paris
 - Toulouse
 - Mutualisation ITIL/ISO20000-1 et ISO 27001

- 9h00** : SMSI et normes ISO 27001, introduction et perspectives par les membres du Club 27001
- 9H45** : Retour d'expérience d'un certifié
- . Odile Bouchy, responsable sécurité, Gemalto
 - . Christine Lauvernier, chef de projet sécurité, Gemalto
- 10h30** : **Pause**
- 11h00** : Retour d'expérience sur la mise en oeuvre d'un SMSI
- . Luc Petitpré, RSSI, Crédit Mutuel Nord Europe
- 11h45** : L'approche ISO 27001 au sein du Gie Systalians de Réunica Bayard.
- . Emmanuel Garnier, RSSI, Systalians (Réunica-Bayard)
- 12h30** : **Repas**

- 14h00** : Mise en place d'une méthode d'appréciation des risques SI à partir des normes ISO 27001 et 27002 et des méthodes EBIOS et Méhari
 . Rene Khanh, Responsables Méthodes à la DSI, AREVA
- 14h45** : ISO 27001 : conformité oui, certification ?
 . Eric Wiatrowski, Orange-FT
- 15h30** : **Pause**
- 16h00** : Retour d'expérience d'audit ISO 20000-1 et ISO 27001 chez IBM Infogérance
 . Gerard Grelou, responsable qualité, IBM
 . Muriel Collignon, consultant sécurité, IBM
- 16h45** : Table-ronde "Apport de l'ISO27001 à la démarche SSI en entreprise", animée par Alexandre Fernandez, avec Fabrice Bru, Eric Doyen, Jean-François Louapre Lazaro Pejsachowicz et les intervenants de la journée
- 17h30** : **Fin**