

Club 27001 Toulouse

01/06/2007



**l'Assurance
Maladie**

Caisse Nationale

Ordre du jour

- Objectifs et fonctionnement
- Tour de table
- État de la norme
- Retour des réunions parisiennes
- Propositions pour la prochaine réunion

Objectifs du club 27001

- Réunir les personnes intéressées par la série des normes **ISO 27000**, sous la forme d'un groupe de travail, de réflexion et d'échanges.
- Les réunions peuvent avoir des présentations, des discussions ouvertes, et des prises de décision.
- Le groupe est ouvert à tous, utilisateurs comme fournisseurs.
- Les présentations sont de toutes natures : explications sur les normes, retours d'expérience, solutions commerciales, etc...
- Il n'est pas nécessaire d'être membre d'une association pour participer au *Club ISO 27001*.

Fonctionnement du club 27001

- Gratuit
- Respect de la déontologie de chacun
 - pas de pub...
- Basé sur le bénévolat
- Propositions de
 - Thèmes pour présentations
 - Salle de réunion
 - Rédacteur du compte rendu
- Comptes rendu sur le site Web
 - validé au préalable par Anne Mur et Dominique Pourcellié
 - Sur le site web : www.club-iso27001.fr

Les normes ISO 2700x : présentation

- **ISO/IEC 27000: Overview and vocabulary.**
 - fondamentaux et vocabulaire propres à la série.
- **ISO/IEC 27001: ISMS requirements.**
 - à la base de la certification d'un SMSI à l'instar de l'ISO 9001 pour la qualité et ISO 14001 pour l'environnement => norme BS 7799-2 : 2005 obsolète.
- **ISO/IEC 27002: Code of practice for information security management.**
 - nouvelle dénomination de la norme ISO 17799 : 2005.
- **ISO/IEC 27003: ISMS implementation guidance.**
 - guide d'aide à l'implémentation des exigences d'un SMSI.
 - Cette norme sera plus particulièrement orientée sur l'utilisation du cycle PDCA et des différentes exigences requises à chaque étape du cycle.
- **ISO/IEC 27004: Information security management measurements.**
 - Aide pour mesurer et rapporter l'efficacité de l'implémentation d'un SMSI.
- **ISO/IEC 27005: Information security risk management.**
 - évolution des parties 3 et 4 de la norme ISO 13335.
 - définit les techniques à mettre en œuvre dans le cadre d'une démarche de gestion des risques.
- **ISO/IEC 27006: Requirements for the accreditation of bodies providing certification of ISMS.**
 - guide les organismes de certification sur les exigences nécessaires à atteindre pour être accrédités en tant qu'organisme de certification d'un SMSI.
- **ISO/IEC 27007: Auditor guidelines.**
 - guide spécifique pour les audits de SMSI, notamment en support à l'ISO 27006.
 - (extrait de la norme 2006 pour ne pas la rendre obligatoire)

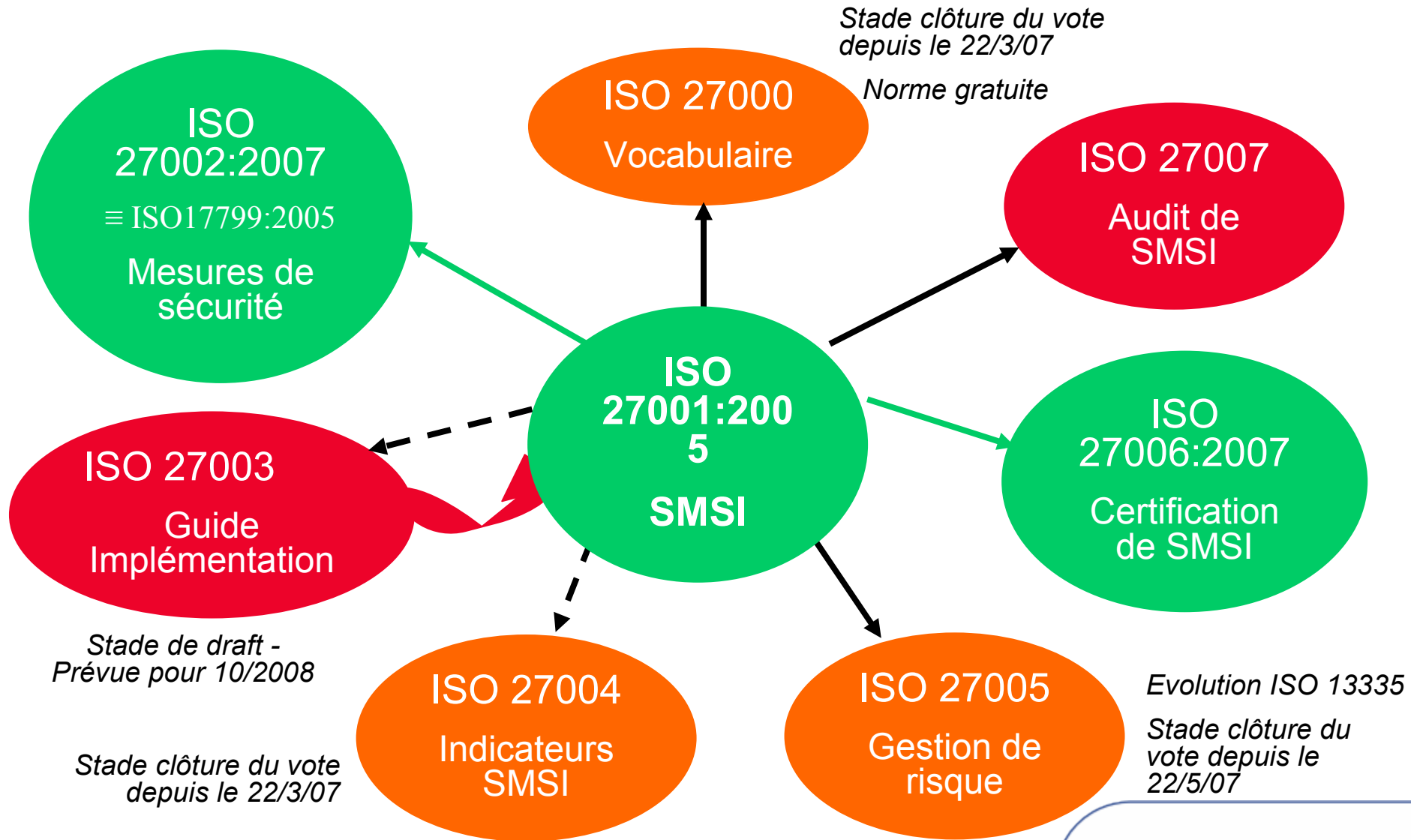


Oblig



Oblig

Les normes ISO 2700x : disponibilité



ISO 27005 : gestion de risque

Guide de mise en œuvre de la partie appréciation du risque de l'ISO 27001

Plan

- Établissement du contexte
- Appréciation du risque :
 - Identification du risque : mise en évidence de ses composantes
 - Estimation du risque : estimation de leur importance
 - Évaluation du risque : analyse d'ensemble et prise de décision sur les risques
- Elaboration du plan de traitement du risque
 - Sélection des objectifs et mesures, refus, transfert ou conservation du risque

Do

- Implémenter les actions pour réduire les risques
- Éduquer direction et personnel sur les risques et actions prises pour les atténuer

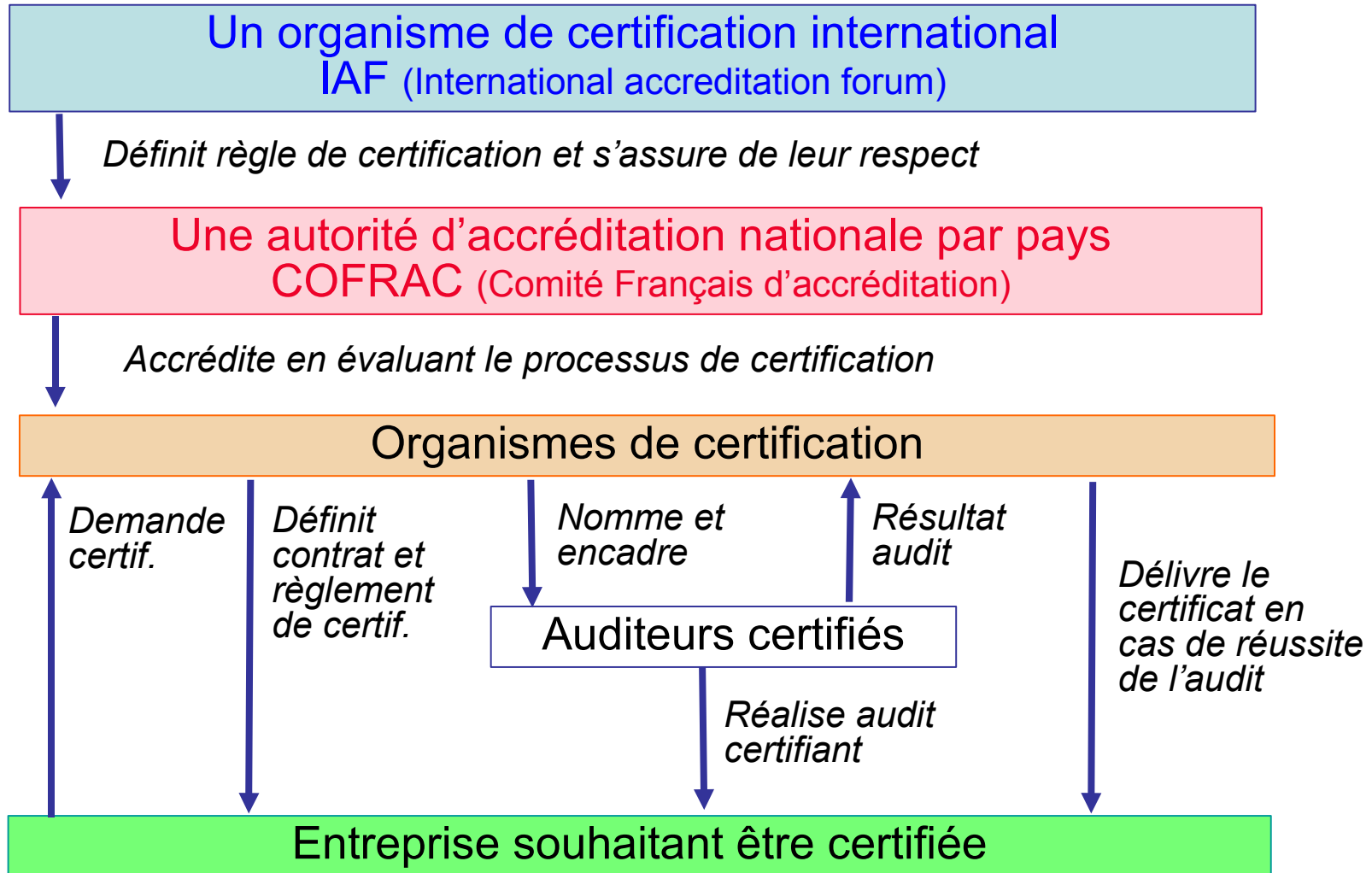
Check

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

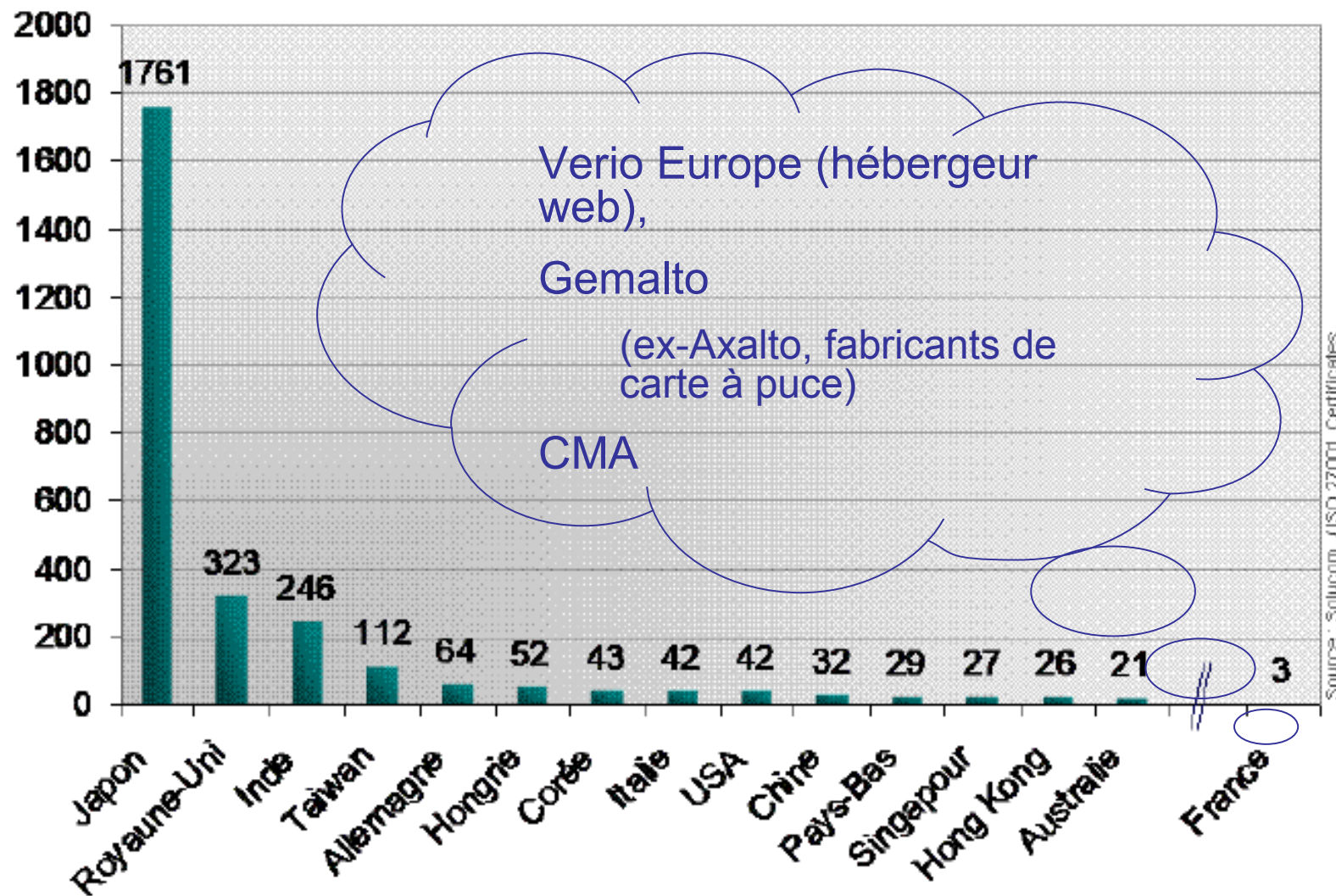
Act

- Rectifier le traitement du risque / événements et changements
- Améliorer le processus de gestion du risque

Acteurs et étapes de certification



Organismes certifiés : très très peu en France...



Organismes certifiés

- Autres chiffres (HSC) :
 - Fin 2006
 - Royaume-Uni : 229 certificats
 - France : **2** certificats
 - Prévus pour fin 2007:
 - Royaume-Uni : 319 certificats
 - France : **3** certificats

Propositions pour le Club 27001 toulousain

- Fréquence ?
 - Tous les 3 mois
- Jour ?
 - Vendredi après midi
- Date des 2 prochaines réunions ?
 - 28 septembre – Rockwell Collins
 - 14 décembre – UT 1 Sciences sociales
- Proposition de thèmes ?
 - ISO 27005 – Ebios
 - Retour du groupe de travail ITIL

Merci de votre participation

Anne.mur@edelweb.fr
Dominique.pourcellie@cnamts.fr