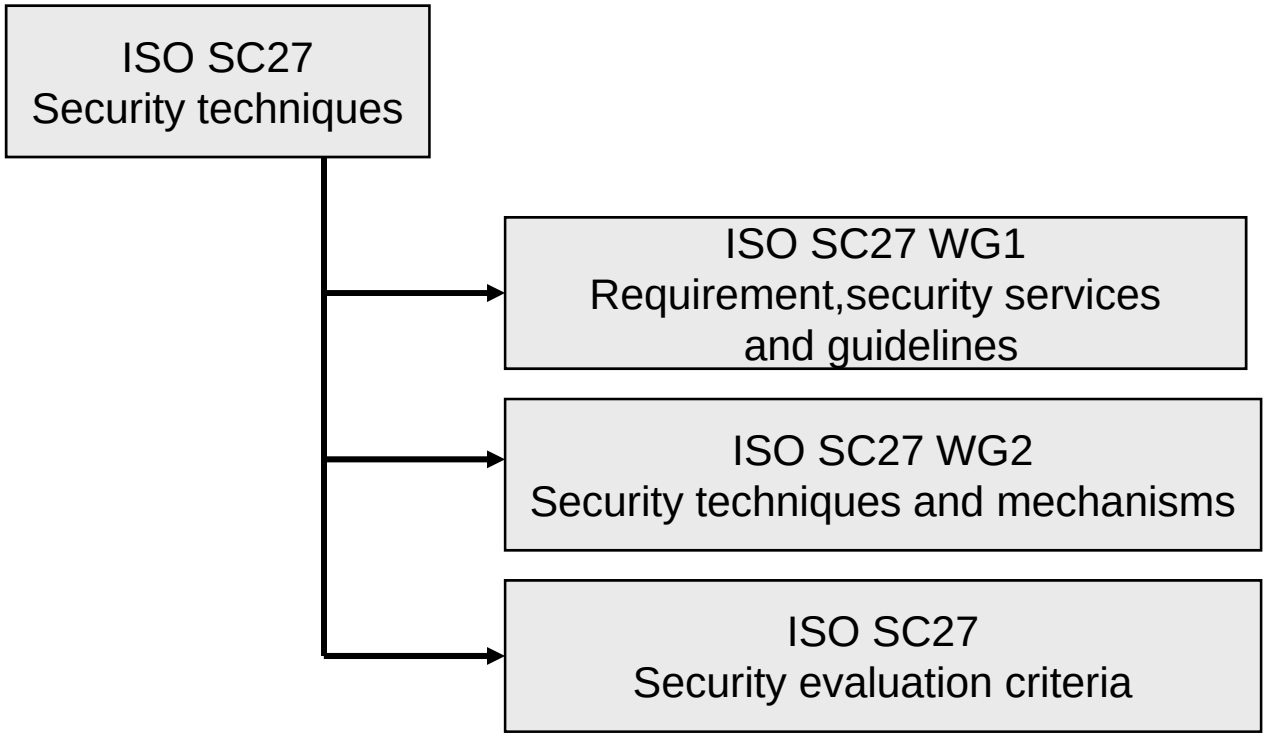
Historique et Devenir

- **ISO et sécurité : comité et sous-comité, standards et rapports techniques**
  - Organisation du sous-comité 27 et structures nationales
  - Élaboration d'un standard ou d'un guide
  - Restructuration de l'ISO SC27
- **Naissance d'une famille : de la BS 7799 à l'ISO 2700X**
  - Naissance de l'ISO 17799
  - Les leçons d'un apprentissage : ISO 27001
  - L'ensemble des standards de management de la sécurité
- **Les standards de la famille 2700X**
- **Quel avenir pour ces standards ?**

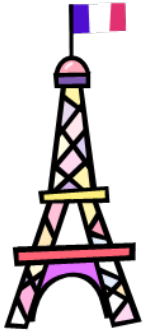
➔ Comité SC27 et sous-comités (jusqu'en 2006)

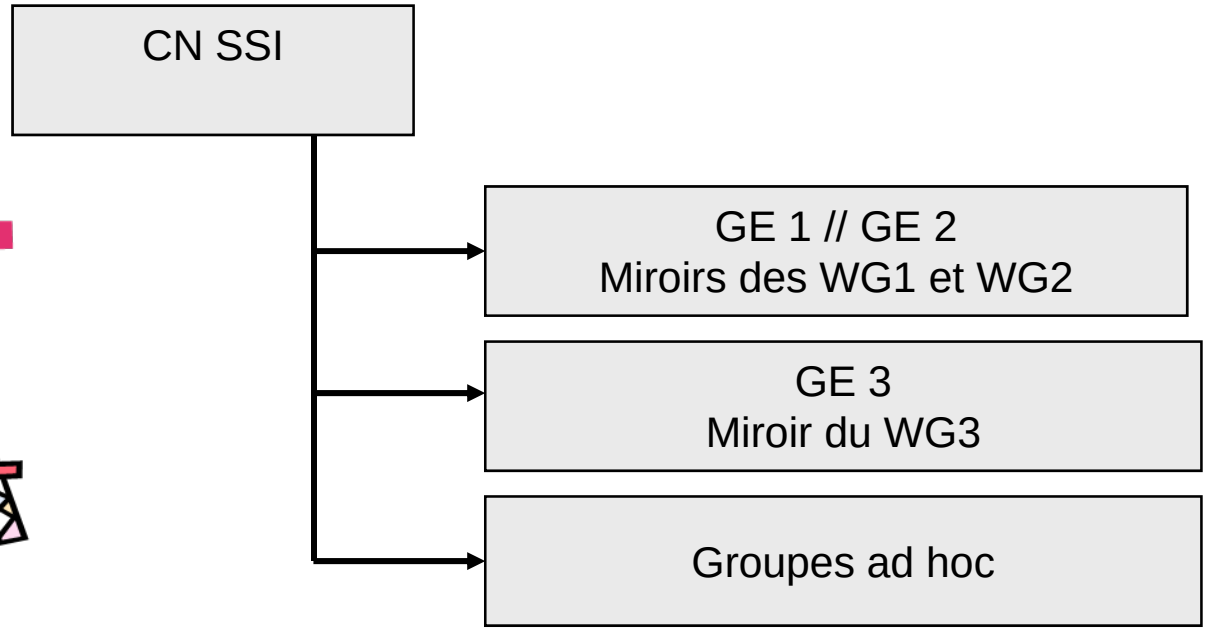


➢ **Des mathématiques appliquées … à la gestion des risques**

ISO SC27 : security techniques. Miroir national

➔ AFNOR : CN SSI « Sécurité des systèmes d'information »

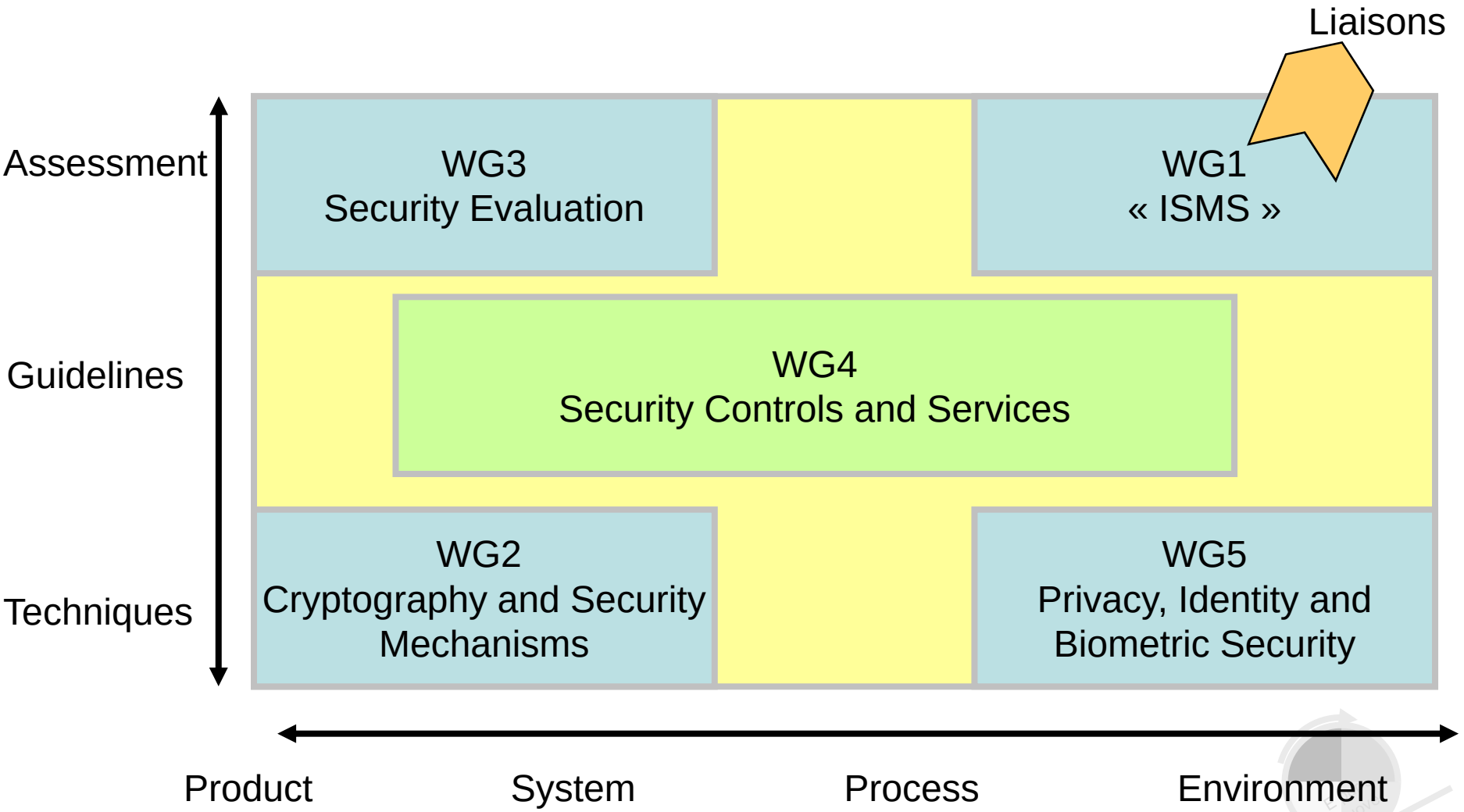




- **GE1 et ISMS : de « ni faire ni laisser faire » à « ni pour ni contre bien au contraire »**

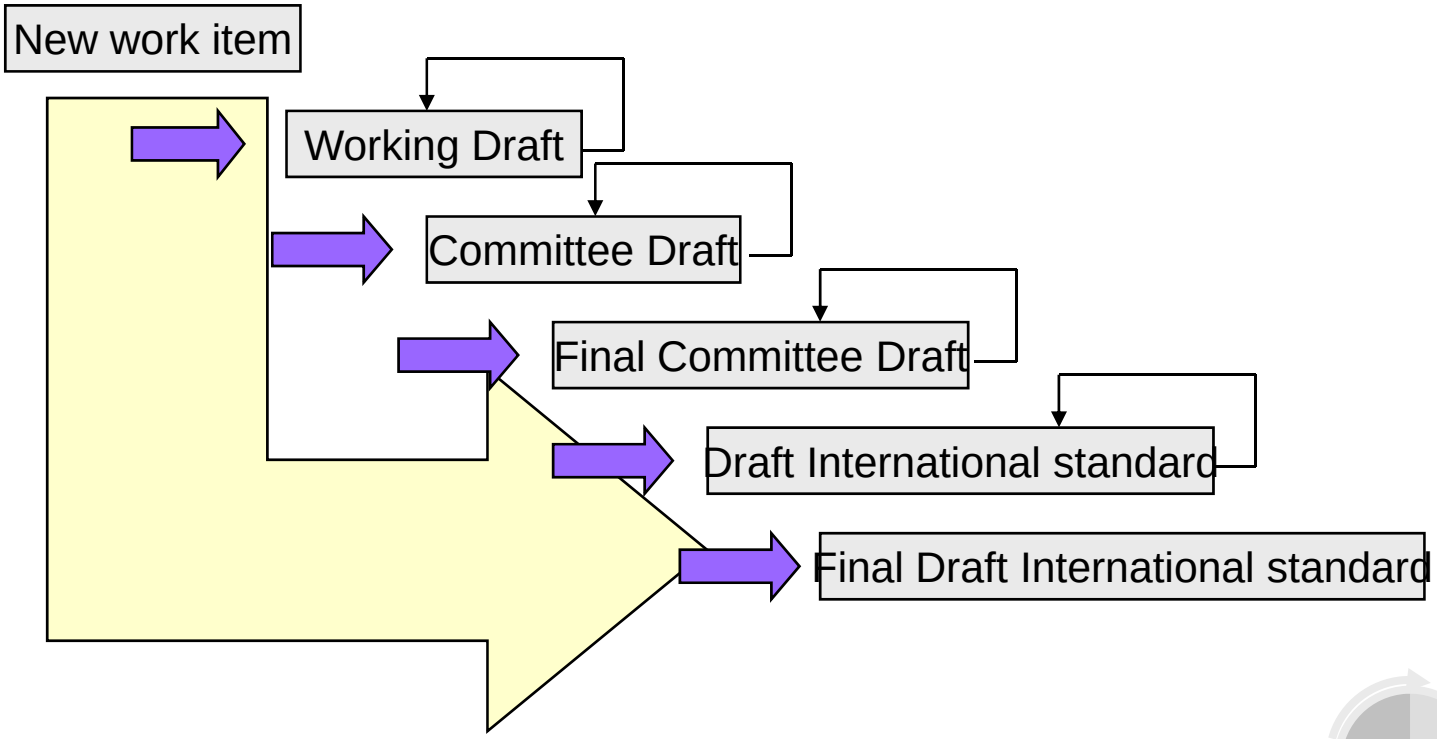
➔ BSI, ANSI, JISC, DIN, …

Devenir : le poids des standards ISMS nécessite une refonte de l'ISO SC27



➔ Standard ou Technical report ?

➔ Elaboration d'un standard : une longue route … (3 à 5 ans)



- Mais des raccourcis (fast track)

- ISO et sécurité : comité et sous-comité, standards et rapports techniques
  - Organisation du sous-comité 27 et structures nationales
  - Élaboration d'un standard ou d'un guide
  - Restructuration de l'ISO SC27
- **Naissance d'une famille : de la BS 7799 à l'ISO 2700X**
  - **Naissance de l'ISO 17799**
  - **Les leçons d'un apprentissage : ISO 27001**
  - **L'ensemble des standards de management de la sécurité**
- Les standards de la famille 2700X
- Quel avenir pour ces standards ?

De la BS 7799 à l'ISO 17799

➔ Naissance de l'ISO 17799 version 1.0

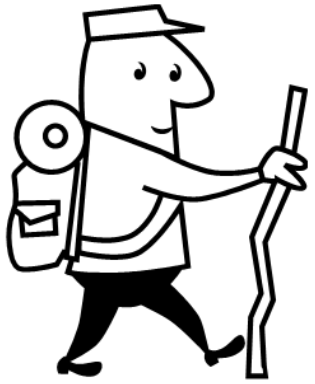
- Tokyo, 2000
- Procédure de fast track avec révision immédiate
- BS 7799

➔ Maturité du standard ISO 17799 version 2.0

- Fortalezza 2005
- N réunions préparatoires
- Appropriation internationale

➔ Du fast track à la marche forcée : ISMS (BS17799-2)

- Etude d'opportunité : Paris 2003
- New work item : Fortalezza 2004
- Final CD : début 2005
- International Standard : fin 2005



➔ Une démarche participative, un standard désiré qui en appelle d'autres

Vers un ensemble de standards complets de la gestion de la sécurité

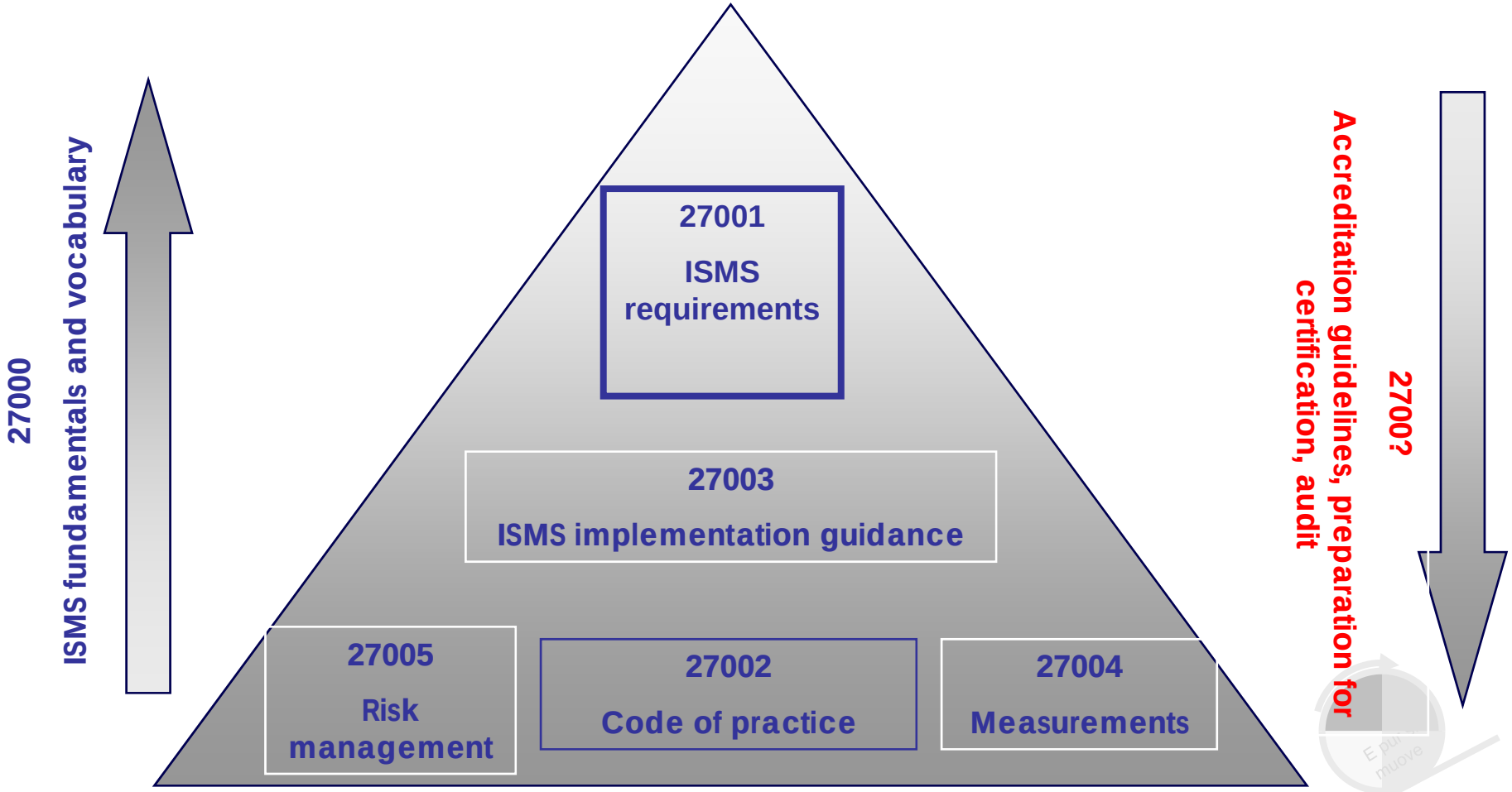
➔ Demain : ISO 2700X

➢ NWI 27000	ISMS fundamentals and vocabulary
➢ IS 27001	ISMS requirements standards
➢ IS 27002	Code of practice (ISO 17799)
➢ WD 27003	ISMS implementation guidance
➢ WD 27004	Information security management measurements
➢ CD 27005	Information security risk management
➢ Autres candidats	NWI : accreditation guidelines for the accreditation bodies operating certification / registration of ISMS

- supports directs et orientations pour l'implémentation du PDCA process

Vers un ensemble de standards complets de la gestion de la sécurité

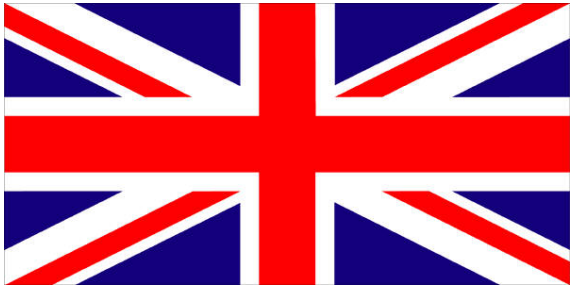
➔ Schéma du positionnement des normes



Vers un ensemble de standards complets de la gestion de la sécurité

➔ L'existant britannique est encore riche …

- BIP 0071 Guidelines on requirements and preparation for ISMS certification
- BIP 0072 Are you ready for an ISMS audit ?
- BIP 0073 Guide to the implementation and auditing of ISMS controls based on ISO/IEC 27001
- BIP 0074 Measuring the effectiveness of your ISMS implementation
- …



- ISO et sécurité : comité et sous-comité, standards et rapports techniques
  - Organisation du sous-comité 27 et structures nationales
  - Élaboration d'un standard ou d'un guide
  - Restructuration de l'ISO SC27
- Naissance d'une famille : de la BS 7799 à l'ISO 2700X
  - Naissance de l'ISO 17799
  - Les leçons d'un apprentissage : ISO 27001
  - L'ensemble des standards de management de la sécurité
- **Les standards de la famille 2700X**
- Quel avenir pour ces standards ?

Vers un ensemble de standards complets de la gestion de la sécurité

➔ 27000 ISMS fundamentals and vocabulary

- New work item (Avril 2006)
- Objectifs : définir les concepts et le vocabulaire des standards de la famille
- Calendrier prévisionnel : FDIS / IS en 2008
- Base 13335-1

➔ 27001 ISMS requirements standards

- IS (2005)
- Base BS 7799-2

Vers un ensemble de standards complets de la gestion de la sécurité

➔ 27002 Code of practice for information security management

- Numérotation en 2007
- Objectifs : définir un guide de bonnes pratiques pour la gestion de la sécurité
- Base ISO 17799 version 2

➔ 27003 ISMS implementation guidance

- WD 2006, IS 2008
- Base British Standard, Annexe B de la BS 7799-1 /
- *Base BIP 0073 Guide to the implementation and auditing of ISMS controls based on ISO/IEC 27001*
- Cible et orientations
  - Modèle PDCA
  - Audience : professionnels de la sécurité, responsables de l'implémentation de l'ISMS
  - Organisation cible : Tout type
  - Contenu : pragmatique, sans caractère obligatoire

➔ 27003 ISMS implementation guidance

- Contenu
  - **Guidance on using the PDCA model**
  - **Guidance on the Plan model**
    - Périmètre, interface et dépendance
    - Politique de management de la sécurité Évaluation des risques
    - Gestion des risques
    - Politique de sécurité
  - **Guidance on the Do process**
    - Implémentation des contrôles
    - Sensibilisation et formation
    - Gestion des incidents
    - Gestion des ressources

➔ 27003 ISMS implementation guidance

➢ Contenu

- **Guidance on the Check process**
  - Monitoring
  - Reviewing
  - Audit interne
  - Tableaux de bord et mesures
  - Contrôle de la documentation et des enregistrements
- **Guidance on the ACT process**
  - Implementing improvements
  - Non conformités
  - Actions préventives et correctives
  - Achieving continual improvment
  - Tests

Vers un ensemble de standards complets de la gestion de la sécurité

➔ 27004 Information Security Management measurements

- WD 2006, IS 2008
- Base contribution USA et Espagne
  - Objectifs : définir des indicateurs pour mesurer la maturité du système de management et des contrôles mis en oeuvre
  - Elément important du processus continu d'amélioration

Vers un ensemble de standards complets de la gestion de la sécurité

- **2700? International Accreditation guidelines for the accreditation of Bodies Operating certification / registration of ISMS**
  - New Work Item, en cours de vote mai 2006
  - Base EA 7/03 « guidelines for the accreditation of Bodies Operating Certification / Registration of ISMS
  - Proposition de Fast track

- ISO et sécurité : comité et sous-comité, standards et rapports techniques
  - Organisation du sous-comité 27 et structures nationales
  - Élaboration d'un standard ou d'un guide
  - Restructuration de l'ISO SC27
- Naissance d'une famille : de la BS 7799 à l'ISO 2700X
  - Naissance de l'ISO 17799
  - Les leçons d'un apprentissage : ISO 27001
  - L'ensemble des standards de management de la sécurité
- Les standards de la famille 2700X
- **Quel avenir pour ces standards ?**

➔ Des guides d'implémentation, d'audit et de certification

- Une réalité : la définition de « stratégie de gouvernance de la sécurité » selon le standard 27001
  - Un modèle qui a fait ses preuves
  - Accessible aux Directions
  - Facilitant la maîtrise budgétaire
  - Autorisant une mise en œuvre progressive

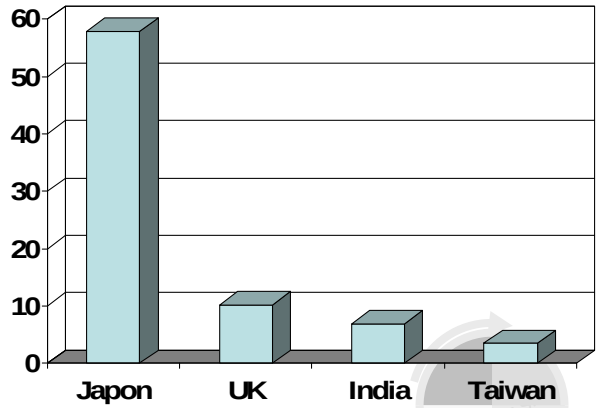
- Une tautologie : la mise en œuvre précède la certification ... sauf dans le domaine normatif

➔ Un moteur dans certains pays : la certification

- **Etat des lieux 2006, source ISMS US usergroup**

Japan	1271*	Czech Republic	6	Slovak Republic	2
UK	225	Turkey	6	South Africa	2
India	151	Brazil	5	Armenia	1
Taiwan	76	Greece	5	Bahrain	1
Germany	54	Spain	5	Chile	1
Italy	42	Croatia	4	Egypt	1
Korea	37	Iceland	4	Lebanon	1
USA	32	Philippines	4	Lithuania	1
Netherlands	27	Saudi Arabia	4	Luxemburg	1
China	25	Argentina	3	Macedonia	1
Hungary	24	Kuwait	3	Morocco	1
Hong Kong	20	Mexico	3	New Zealand	1
Australia	18	UAE	3	Qatar	1
Finland	15	Belgium	2	Romania	1
Norway	13	Canada	2	Russian Federation	1
Switzerland	13	Colombia	2	Serbia and Montenegro	1
Ireland	11	Denmark	2	Slovenia	1
Singapore	11	France	2	Thailand	1
Austria	9	Isle of Man	2		
Poland	8	Macau	2	Relative Total	2195
Sweden	7	Malaysia	2	**Absolute Total**	2183*

De 1000 certificats (2004) à 2000 certificats (2006) mais …



➔ Références. Sites WEB

- www.iso.org
- www.afnor.fr
- www.bsi-global.com
- www.xisec.com (ISMS international users group), et ses pendants
  - www.us-isms.org, www.isg.org, …