



La Normalisation pour l'organisation de la sécurité de l'information

Internet Security Day - 26/03/07
M. Jean-Philippe Humbert



Sommaire

- **Du principe de la Sécurité de l'information**
- **Normalisation & Sécurité de l'information**
- **Les acteurs au G-D de Luxembourg**
- **Exemples pratiques**

Sommaire

- **Du principe de la Sécurité de l'information**
- **Normalisation & Sécurité de l'information**
- **Les acteurs au G-D de Luxembourg**
- **Exemples pratiques**

Définition basique du domaine

La **sécurité de l'information** (regroupant également la **communication**) correspond notamment à la mise en place de moyens de protection (mécanismes de sécurité), permettant d'atteindre des services de sécurité spécifiques essentiels, tels que la **Confidentialité**, l'**Intégrité** ou encore la **Disponibilité (CID)** :

- la **confidentialité** : un état n'autorisant une visibilité de l'information qu'à des personnes déterminées et autorisées
- l'**intégrité** du système et de l'information : garantir que ceux-ci ne sont modifiés que par une action volontaire et légitime
- la **disponibilité** : un état de mise à disposition de l'information en temps, et en performance, défini au préalable

Sécurité de l'information

- Une organisation doit préserver/maîtriser ses acquis pour garantir sa pérennité et son développement « business »
- Une organisation doit maintenir son avantage compétitif en :
 - 1 - offrant une disponibilité constante des outils, notamment d'**information** et de **communication**
 - 2 - assurant l'intégrité et sa confidentialité
- Objectif : l'organisation doit alors appliquer ce type de besoins de sécurité sur ses ressources essentielles

Sécurité de l'information

- La sécurité de l'information : une « contrainte » de plus ?
- Plutôt l'obligation de « faire face », car :
 - les produits IT ne sont pas développés dans un esprit sécurité
 - la découverte et l'exploitation des failles sont devenues un « sport »
 - les produits de sécurité eux-mêmes sont vulnérables et donc à configurer et à maintenir « proprement »
 - il n'existe pas d'instinct de survie numérique (ce n'est pas naturel – effort de mise en place nécessaire)
 - multiplication des *exploits*
 - criminalisation de l'*underground*
 - augmentation des activités d'espionnage industriel
 - impacts pouvant nuire fortement : image de marque, perte de clientèle, frais conséquents, responsabilité pénale...

Sécurité de l'information

- **Comment faire face ?**

-> Entreprendre une démarche globale de sécurité de l'Information :

« **Soyez dissuasifs! Organisez votre sécurité de l'information!** »

- Cela comprend :

- 1) sécurité informatique (IT)
- 2) + sécurité des systèmes d'information (SSI)
- 3) + sécurité des informations et des communications (SIC)

- Nécessité de prendre en compte :

- Démarche sécurité
- Sécurité physique
- Sécurité organisationnelle
- Sécurité IT
- Communication de sécurité (sensibilisation interne)

Sécurité de l'information

- Plan d'action classique :
- Importance de l'engagement de l'organisation dans la sécurité de l'information et de la communication, notamment via sa Direction
- Etablir un diagnostic sécurité (identifier les ressources et données critiques) et définir un plan d'action en référence
- Dérouter une analyse des risques de sécurité, et déterminer les objectifs de contrôles
- Mettre en place des contrôles sur objectifs (contre-mesures)
- Impliquer toute l'organisation dans la mise en place de la sécurité : politique, procédures, contrôles...
- Viser une amélioration continue de l'ensemble du système de gestion de la sécurité de l'information ainsi mis en place

Sécurité de l'information

- Pierre angulaire :
 - Définir une **politique de sécurité** : ensemble des lois, règlements et pratiques qui régissent la façon de gérer, protéger et diffuser les informations et autres ressources sensibles au sein d'un système spécifique, d'une organisation
 - Une politique de sécurité identifie les objectifs de sécurité (cible de sécurité, les contrôles visés)
 - C'est la clé de voûte du système de sécurité mis en place au cœur de l'organisation

Sommaire

- Du principe de la Sécurité de l'information
- **Normalisation & Sécurité de l'information**
- Les acteurs au G-D de Luxembourg
- Exemples pratiques

Normalisation

“La normalisation a pour objet de fournir des documents de référence comportant des solutions à des problèmes techniques et commerciaux concernant les produits, biens et services qui se posent de façon répétée dans des relations entre partenaires économiques, scientifiques, techniques et sociaux”

Igalens J, Penan H, *La normalisation*, 1994, PUF - Que sais-je,

Normalisation

- Définition d'une norme :

“Spécification technique ou autre document accessible au public, établi avec la coopération et le consensus ou l’approbation générale de toutes les parties intéressées, fondé sur les résultats conjugués de la science, de la technologie et de l’expérience, visant à l’avantage optimal de la communauté dans son ensemble et approuvé par un organisme qualifié sur le plan national, régional ou international”

Normalisation

- Plusieurs catégories de normes : internationales, européennes et nationales
- ISO (International Standards Organisation) constitue la principale organisation internationale de standardisation
- ISO est chargé d'élaborer des normes applicables mondialement, de promouvoir le développement de la standardisation et activités annexes au niveau mondial, en développant des coopérations dans les sphères d'activités intellectuelles, scientifiques, technologiques et économique
- Il s'agit d'une organisation non-gouvernementale (1947), qui fédère 148 pays, avec un représentant par pays. Les résultats des travaux (accord international) s'effectuent par publication des Standards Internationaux

Normalisation

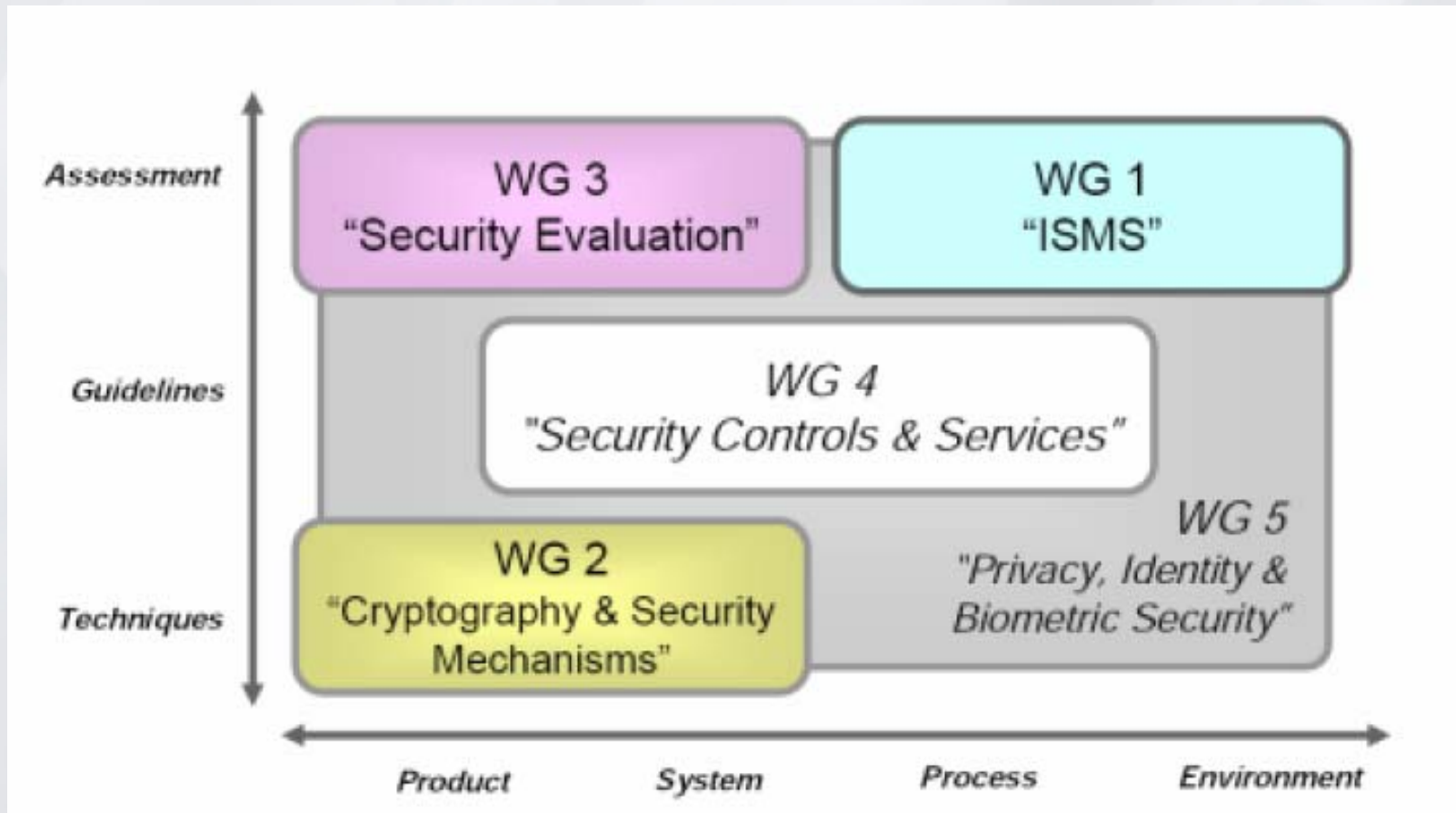
- Autres organismes de normalisation (Niveau européen):
 - CEN (Comité Européen de Normalisation)
 - CENELEC (Comité européen de normalisation électrotechnique)
 - ETSI (Institut européen des normes de télécommunications)
- Organisme de normalisation (Niveau national):
 - SEE (G-D de Luxembourg)

ISO/JTC1/SC27

- « Normalisation et Sécurité de l'information » principalement traitées au sein de :
 - > ISO/JTC1 : « *Technologies de l'Information* »
- Dix-sept sous-comités techniques dont le « **SC27** » qui traite des « *techniques de sécurité des systèmes d'information* »
 - <http://www.jtc1.org>
 - Secrétariat : American National Standards Institute, 1819 L Street, NW – ANSI - US-Washington, DC 20036
- Domaines d'application :
- Normalisation des techniques et des méthodes génériques pour les besoins de sécurité en informatique, ce qui inclut :
 - identification des besoins généraux pour les services de SSIC
 - développement des mécanismes et des techniques de SSIC

ISO/JTC1/SC27

- ISO/SC27 se compose de cinq « Working Group » (WG) :

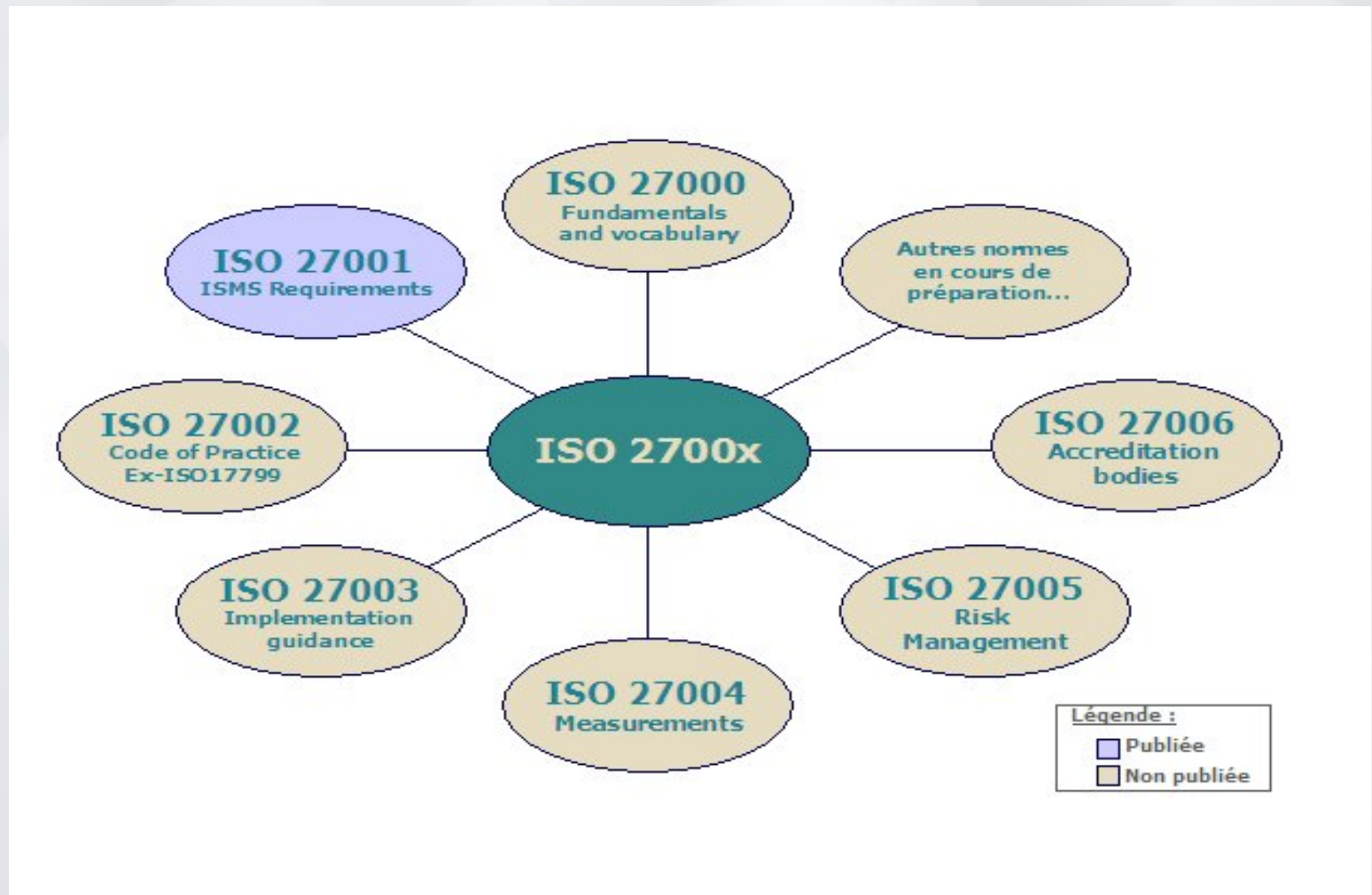


ISO/JTC1/SC27

- Réorganisation en cours de WG1/SC27 en lien avec les systèmes de management Qualité : **série de normes “2700x”** : normes de sécurité de l’information organisationnelle
 - > WG1- « *Exigences, services de sécurité et directives* »
 - > Focus “Série 2700x” ->

ISO/JTC1/SC27

- Les normes de la série 2700x :



Normalisation & Liens utiles



www.iso.ch



www.din.de



www.see.lu

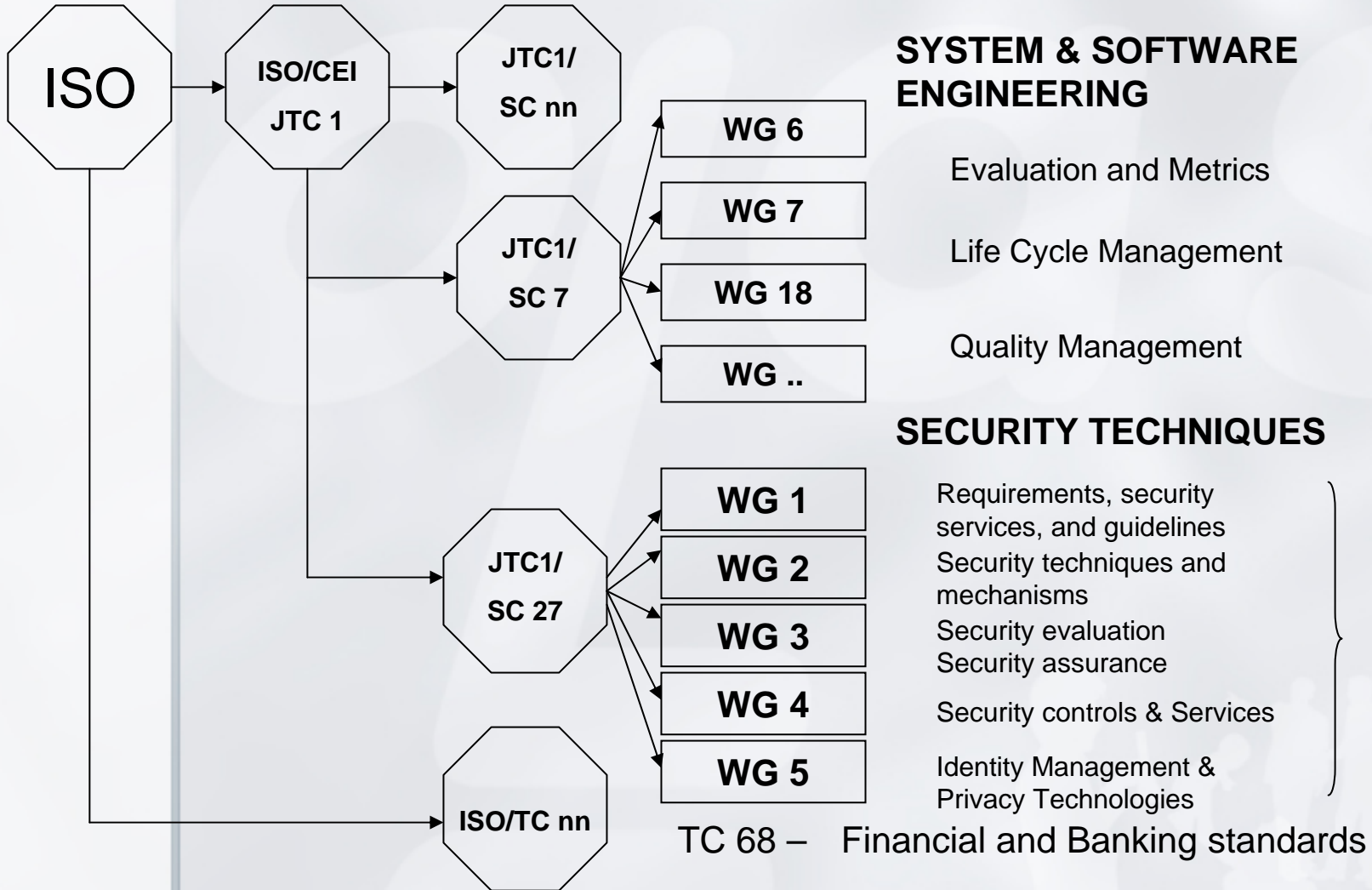
Sommaire

- Du principe de la Sécurité de l'information
- Normalisation & Sécurité de l'information
- **Les acteurs au G-D de Luxembourg**
- Exemples pratiques

ISO, Luxembourg & Sécurité

- **CNLSI** = Comité de Normalisation Luxembourgeois pour la Sécurité de l'Information (CNLSI)
- **CNLSI** = Comité technique ISO/SC27 Luxembourg
- Composition : experts de la sécurité de l'information – G-D de Luxembourg
- Rôle : commentaires et votes sur les normes ISO/SC27, en regard des spécificités et intérêts du G-D de Luxembourg

ISO, Luxembourg & Sécurité



CNLSI :

- Nombre de membres :

Mise à jour récente : dix-sept membres inscrits et actifs provenant de diverses sociétés luxembourgeoises aux domaines d'activités variés (secteur bancaire, informatique, Ministère...)

- Rôle des membres :

- Révisent les textes et rédigent les commentaires (par norme choisie)
- Contribue à la promotion du groupe
- Respectent les normes ISO :
 - Non diffusion des textes
 - Défense du nom et de l'intérêt de l'ISO

ISO, Luxembourg & Sécurité

Actuel programme de travail (WG1) :

1. Votes et commentaires sur ISO N5456rev1 1st CD 27000 (*“Information Security Management Systems – Overview & Vocabulary”*)
2. Votes et commentaires sur ISO N5460 1st CD 27004 (*“Information Security Management Measurements”*)
3. Commentaires sur ISO N5462 FCD 27005 (*“Information Security Risk Management”*)
4. Commentaires sur ISO N5458 3rd WD 27003 (*Information Security Management System Implementation Guidance”*)

ISO, Luxembourg & Sécurité

- 1°) **SEE, ORGANISME LUXEMBOURGEOIS DE NORMALISATION**
Contact : Marc Clément,
34 avenue de la Porte-Neuve, L-2227 Luxembourg
TEL : + 352 46 97 46 - 1
FAX : + 352 46 97 46 - 39
see.normalisation@eg.etat.lu
www.see.lu

- 2°) **Comité de Normalisation Luxembourg pour la Sécurité de l'Information (CNLSI)**
Contact : Jean-Philippe Humbert (HOD ISO/SC27 Luxembourg - Président CNLSI – Vice-Président ANSIL)
34 avenue de la Porte-Neuve, L-2227 Luxembourg
TEL : +352-46 97 46 42
FAX : +352-46 97 46
jean-philippe.humbert@olas.etat.lu

- 3°) **TELINDUS PSF LUXEMBOURG**
Contact : Cédric Mauny (Secrétariat CNLSI - Secrétaire Général ANSIL)
81-83 Route d'Arlon – L-8009 Strassen
TEL : +352.45.09.15.1
FAX : +352.45.09.11
cedric.mauny@telindus.lu

ISO, Luxembourg & Sécurité

- **ANSIL - Association de Normalisation pour la Société de l'Information Luxembourg**
- **Buts :**
- Un pont entre SC7 et SC27
- Étudier, analyser toutes formes de documents normatifs
- Constituer des groupes d'experts (committees)
 - ...intérêts économiques du G-D de Luxembourg
 - ...travailler par consensus
- Interface entre acteurs et institutions officielles
- Sensibiliser...promouvoir...encourager la normalisation
- Participer à des projets de recherches
- Services d'expertise
- En conformité avec l'ISO/IEC, le CEN, CENELEC
- <http://www.ansil.eu> (avril 2007)

ISO, Luxembourg & Sécurité

- **ILNAS - Institut luxembourgeois de la normalisation, de l'accréditation et de la sécurité des produits et services**
 - (OLAS (www.olas.lu)+SEE+SML...)
- Les missions (aspects de sécurité) :
 - la normalisation (Normes ouvrant à certification sécurité, suivi des activités CNLSI ...)
 - l'accréditation (PSC, Organismes de certification sécurité (ISMS) ...)
 - la procédure d'information dans le domaine des normes et réglementations techniques et des règles relatives aux services de la société de l'information
 - la sécurité générale des produits
 - la surveillance du marché
 - la promotion du management de la qualité
 - les BPL

Normes & Sécurité SI

Luxembourg une bonne pratique!

- Rapport de la Commission Européenne (Octobre 2006)
- ***“Les PME et la normalisation en Europe, 23 bonnes pratiques pour promouvoir la participation de l’artisanat et des PME à la normalisation et l’utilisation des normes (EIM Business & Policy Research)”***
- G-D de Luxembourg parmi les 23 exemples de bonnes pratiques listés (Chapitre 6)
- Lien fort avec le portail de la sécurité de l’information du G-D de Luxembourg : <http://www.cases.public.lu>

Normes & Sécurité SI

Luxembourg une bonne pratique!

	Administrations nationales	Organismes nationaux de normalisation	Organisations de PME et d'entreprises artisanales	Autres	Total
Subvention	6.18 Slovaquie - Aide directe (142)	6.4 Finlande - Indemnités de déplacement (74) 6.12 Malte - Mise à disposition de normes à prix réduit (116) 6.21 Espagne - Subventions de participation pour réunions européennes (154) 6.22 Suède - Indemnités de déplacement pour réunions de normalisation (158)			5
Ateliers de travail & séminaires	6.1 Croatie - Services de cofinancement et de certification (60) 6.11 Luxembourg - Normes pour la sécurité de l'information (113)	6.10 Italie - Conventions institutionnelles (107) 6.13 Pays-Bas - Projet de sensibilisation (119) 6.14 Norvège - Forums de réseau (125)	6.2 République tchèque - Points d'information pour les entrepreneurs (66) 6.19 Slovénie - Séminaire et atelier de travail (146)	6.15 Pologne - Formation et séminaires 'Welding' (soudage) (128)	8
Information & publications		6.6 Allemagne - Rapports KAN sur la normalisation SST (84)	6.23 RU - Réunions et lettres d'information (161)		2
Site web			6.9 Italie - Site web (101)		1
Conseil & formation		6.3 Danemark - Université de normalisation danoise (70) 6.8 Hongrie - Séminaires, formation de sensibilisation (97)		6.16 Pologne - Formation sur les normes écologiques (134)	3
Autres	6.5 France - Actions de standardisation, ministère des PME (79)	6.17 Portugal - Contacts en face à face (139)	6.7 Allemagne - Comité de normalisation en construction mécaniques (NAM) (90) 6.20 Espagne - Promotion des groupes de travail (150)		4
Total	4	11	6	2	23

Sommaire

- Du principe de la Sécurité de l'information
- Normalisation & Sécurité de l'information
- Les acteurs au G-D de Luxembourg
- **Exemples pratiques**

Sécurité de l'information & Normalisation - Exemples

- Deux référentiels normatifs sont devenus incontournables :

- ISO/IEC 17799:2005 : « *Code of practice for information security management systems* »

- ISO/IEC 27001:2005 : « *Information security management systems – Requirements* »

Sécurité de l'information & Normalisation - Exemples

- « *Council Resolution du 28/01/2002* » - Union Européenne
 - **Point 11** : « *La norme ISO 17799 et d'autres dispositions nationales similaires sont aujourd'hui des références reconnues pour la gestion des problèmes de sécurité dans les organismes privés et publics* »

Sécurité de l'information & Normalisation - Exemples

ISO/IEC 17799:2005 (Politique de sécurité) – Les domaines :

- Politique de sécurité
- Organisation de la sécurité
- Classification des Informations
- Sécurité du personnel
- Sécurité de l'environnement et des biens physiques
- Administration
- Contrôles d'accès
- Développement et maintenance
- Gestion des incidents
- Plan de continuité
- Conformité légale et audit de contrôle

Sécurité de l'information & Normalisation - Exemples

ISO/IEC 17799:2005 (Politique de sécurité) –

Les catégories :

- La structure de la norme est semblable pour chacune des 39 catégories de sécurité :

 - Un objectif de contrôle qui fait l'état sur ce qui doit être appliqué est énoncé
 - Un ou plusieurs contrôles à appliquer sont proposés pour remplir l'objectif de contrôle de la catégorie de sécurité

Sécurité de l'information & Normalisation - Exemples

ISO/IEC 17799:2005 (Politique de sécurité) –

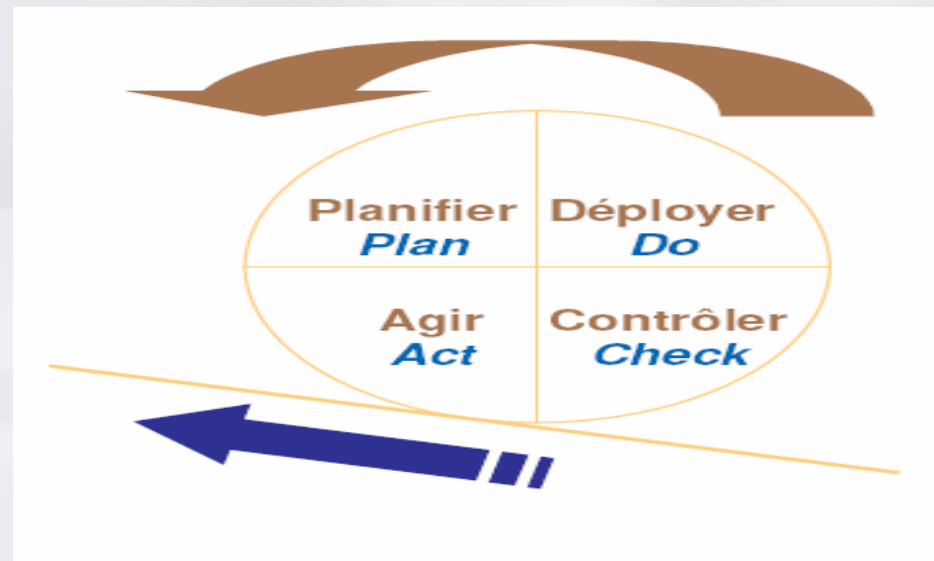
Les objectifs de contrôle :

- Au niveau inférieur, la structure de la norme est semblable pour chacun des 137 objectifs de contrôle qui ont été définis :

- **Control** : le contrôle permet de définir précisément l'état pour satisfaire à l'objectif de contrôle
- **Implementation guidance** : le guide d'implémentation propose les informations détaillées permettant d'effectuer l'implémentation du contrôle et de satisfaire à son objectif

Sécurité de l'information & Normalisation - Exemples

- IS ISO/IEC 27001:2005 : « **Information security Management systems – Requirements** » (complément de la norme ISO/IEC 17799:2005 : « Code de pratiques » pour la gestion de sécurité de l'information)
- IS ISO/IEC 27001:2005 : son application consiste en la mise en oeuvre d'un système de gestion de la sécurité de l'information selon la célèbre roue (PDCA)



Sécurité de l'information & Normalisation - Exemples

- ISO 27001 spécifie le processus permettant de :
 - établir,
 - mettre en oeuvre,
 - revoir
 - surveiller
 - gérer
 - et actualiser
- un système de gestion de la sécurité de l'information efficace

Sécurité de l'information & Normalisation - Exemples

- Permet à une organisation d'obtenir une certification qui atteste de la mise en place effective d'un Système de Management de la Sécurité de l'Information (SMSI, SGSI ou *ISMS*)
- Cette norme garantit aux parties prenantes (clients, actionnaires, partenaires...) que la sécurité des systèmes d'information :
 - a été sérieusement prise en compte
 - que l'entreprise s'est engagée sur ce sujet dans une démarche d'amélioration constante
- Toutes les tailles d'entreprises sont concernées, y compris les PME
- Tous les secteurs économiques également sans exception

Sécurité de l'information & Normalisation - Exemples

Etablir la structure ISMS : six étapes :

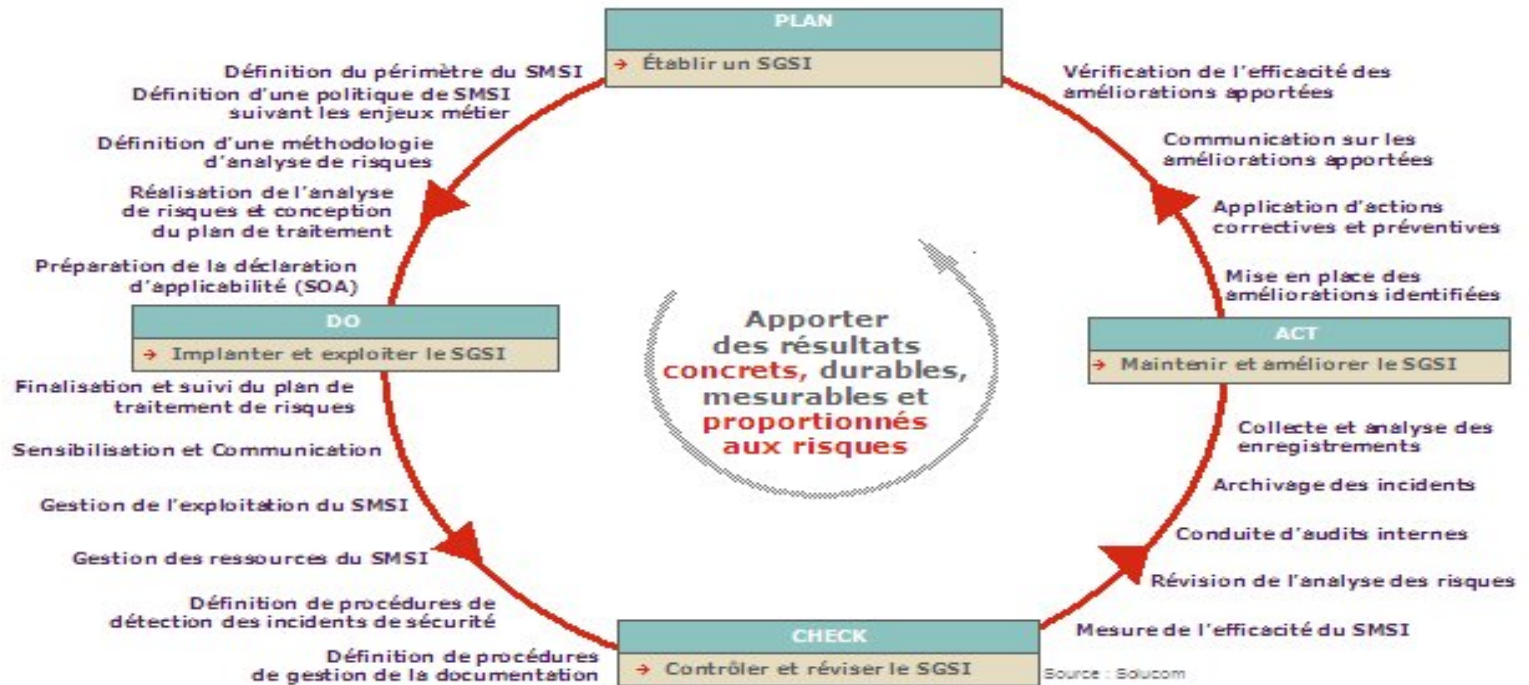
- Définir le *scope* ISMS
- Entreprendre une analyse de risque de sécurité
- Gérer le risque de sécurité
- Définir le document politique de sécurité (en fonction de l'analyse de risque de sécurité)
- Sélectionner des objectifs de contrôles et des contrôles à établir
- Préparer une déclaration d'applicabilité (documentation détaillée)

Sécurité de l'information & Normalisation - Exemples

- Comment mettre en place un ISMS conforme à la norme ISO 27001 ?
 - Implication nécessaire de la direction
 - Définir un responsable projet
 - Définir les budgets, les ressources humaines
 - Analyse de risques de sécurité
 - Rédaction/mise à jour de la politique de sécurité
 - Construction du système de management
 - Sensibilisation ou formation des collaborateurs
 - Audits internes
 - Mise en oeuvre du PDCA

Sécurité de l'information & Normalisation - Exemples

- Le cycle de vie de l'ISMS :



Sécurité de l'information & Normalisation - Exemples

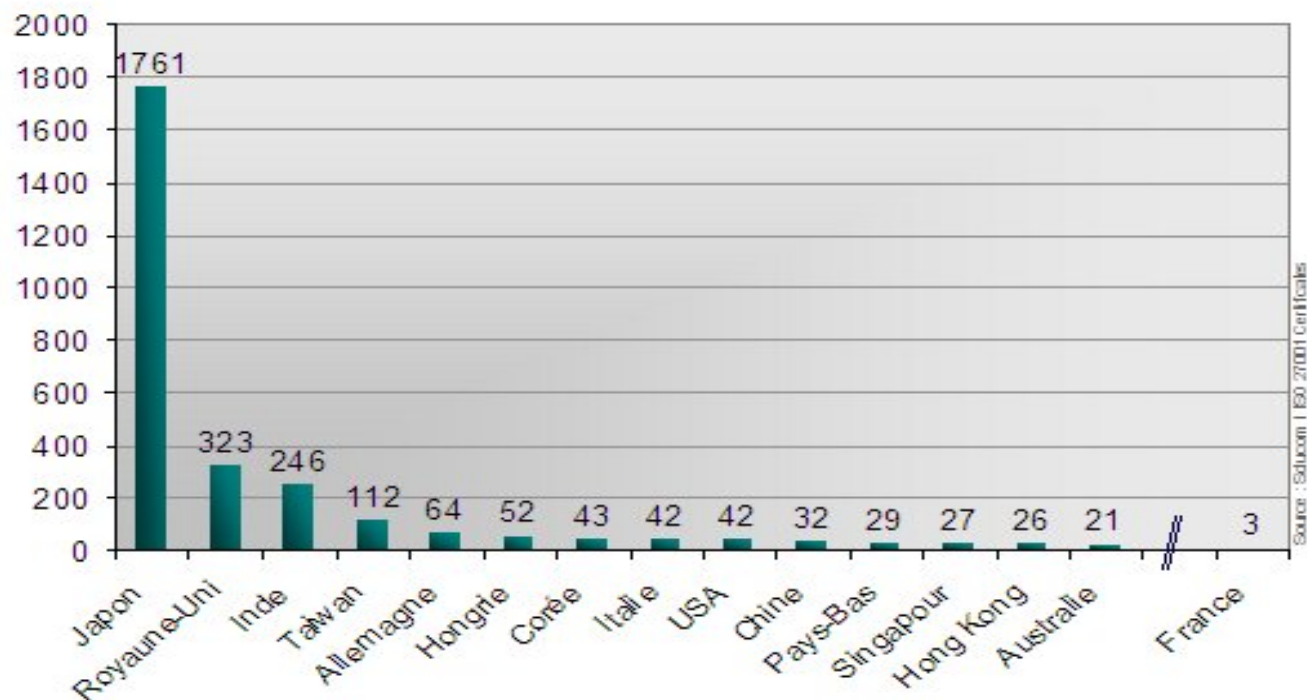
- Comment auditer un ISMS selon les critères de l'ISO 27001 ?
- Un organisme de certification vérifie la conformité du système de management au référentiel ISO 27001
- À l'issue de cet audit, et si l'entreprise répond aux exigences de la norme, l'organisme de certification délivre un certificat valable pour une durée de trois ans

Sécurité de l'information & Normalisation - Exemples

- Principes équivalents à tout audit :
 - Analyse ISMS selon un plan d'audit pré-établi
 - Analyse des pratiques de l'entreprise en fonction des procédures et des exigences du référentiel
 - Détection des écarts significatifs (Non conformité ou Remarque)
 - Deux audits de suivis durant la période de 3 ans

Sécurité de l'information & Normalisation - Exemples

- Nombre de sociétés certifiées par pays :



Normalisation ISO

- Actuellement la meilleure boîte à outils pour la sécurité de l'information organisationnelle
- Accès facilité au Grand-Duché de Luxembourg
- Permet de croiser les besoins, connaissances et avis par consensus
- Permet d'accroître les compétences des entreprises au Grand-Duché de Luxembourg

Normalisation ISO

- *" Standardization provides an important linkage between an idea and its transformation into economic success. To support a swift and smooth transformation from knowledge into products, all stakeholders have to work hand in hand "*

Günter Verheugen, Vice-President of the European Commission

Sécurité de l'information & Normalisation

Merci pour votre attention

Questions ?

jean-philippe.humbert@olas.etat.lu