



Standards et normes en SSI

Mercredi 19 octobre 2005

■ Suite de l'épisode précédent ...

- Ce que nous avons vu en novembre 2004 :

Enjeux liés à l'emploi des normes dans l'entreprise :

historiquement orientés sur des standards de sécurité informatique on arrive progressivement à la certification des systèmes de management de la sécurité

Cartographie des normes : les sources des normes de la SSI sont multiples, les définitions elles-mêmes de la sécurité sont variées. Il existe un réel « fond documentaire » sur la SSI mais qui prête à confusion.

Présentation des labels de sécurité : savoir lire entre les lignes les déclarations des fournisseurs concernant des certifications FIPS, ITSEC et Critères Communs.

■ Suite de l'épisode précédent ...

- Ce que nous vous proposons aujourd'hui :

Qu'est ce que la politique de référencement intersectorielle de sécurité de l'administration française (PRISv2) ?

BS, ISO, -1, -2, x7799, 27001 : quels préfixes et quels suffixes, pour quels usages ?

■ Philippe PERRET

- Groupe ARKOON – Directeur Technique de la gamme de produits Security BOX®
- Politique de référencement intersectorielle de sécurité : 9h-10h

■ Samuel Janin

- Ernst & Young et Associés – Manager audit et sécurité des systèmes d'information
- Point sur les normes x7799 : 10h-11h



Politique de Référencement Intersectorielle de Sécurité V2 (PRIS V2)

Mercredi 19 octobre 2005

- Rappel de l'épisode précédent
 - Les évaluations sécuritaires
 - Les qualifications administratives

- PRISv2
 - But
 - Contenu
 - Usages possibles dans le privé

- FIPS 140-1 (norme américaine)
- ITSEC (un peu ancien)
- Critères Communs (ISO 15408)

- EAL 1 : testé fonctionnellement
- EAL 2 : testé structurellement
- EAL 3 : testé et validé méthodiquement
- EAL 4 : conçu, testé et revu méthodiquement
- EAL 5 : conçu à l'aide de méthode semi-formelles et testé
- EAL 6 : conception vérifiée à l'aide de méthodes semi-formelles et testé
- EAL 7 : conception vérifié à l'aide de méthodes formelles et testé

- Il y a trois niveaux :
 - Standard
 - Renforcé
 - Élevé
- Le niveau à utiliser dépend de :
 - Le niveau de confidentialité des informations
 - Si les informations sont ou non de défense
- Les niveaux sont définis en fonction des critères communs
- Niveau standard → EAL 2+ (avec des items niveau EAL 4) mais qui va passer à EAL3+
- Niveau renforcé → EAL 4+ (avec des items EAL 6)
- Le confidentiel défense nécessite le niveau renforcé.
- Validation par la DCSSI de la pertinence de la cible.

■ Transformation de l'administration

- Modernisation des services
- Simplification des démarches
- Plus grande efficacité (Baisse des coûts)

→ Dématérialisation des procédures

- Téléservices/téléprocédures
- Sécurité des échanges (apport de confiance même si pas le choix)

- Définition d'un cadre global de SSI (pour toutes les administrations)
- C'est une sorte de cahier des charges
- La PRIS V2 porte sur :
 - Les certificats
 - Les autorités de certification
 - Les produits de sécurité
- Utilisation des produits/services privés (liberté de choix)
- Trois niveaux d'exigences : *, **, ***

- Authentification
- Signature
- Confidentialité
- Horodatage
- Archivage
- Autres

- Techniques
- Juridiques
- Organisationnelles

- Garantie de sécurité et d'interopérabilité
 - Définition de la forme des certificats (type des données, liste des extension, algorithmes...)
 - Définition de la forme des CRL (type des données, liste des extension, algorithmes...)
 - Définition du format des requêtes/réponses OCSP

- Pour chaque service, il y a :
 - Les exigences pour les AC.
 - Les exigences pour les logiciels/matériels. Exprimé notamment en terme de qualification (cf. précédemment).
- Les exigences varient en fonction des niveaux.
- Des indications guident le lecteur pour déterminer le niveau dont il a besoin.

- Procédure de qualification (arrêté du 26/7/4)
- Mise en place de PC (Politique de certification) types pour chaque service élémentaire de sécurité
- Les PC types sont lourdes → réservée à de grosses autorités

- Procédure de qualification (décret du 18/4/2)
- Utilisation de profils de protection certifiés par la DCSSI

- Objectifs/exigences pour un type de produits de sécurité
- Les profils sont certifiables (procédure CPP-P-01)
- La certification vérifie leur adéquation aux Critères Communs.
- On trouve un peu de tout :
 - Services bancaires ou financiers sur Internet
 - Firewall
 - Client VPN
- Liste complète sur le site de la DCSSI

- Récupération d'un travail tout fait
- Base pour le choix d'une AC
- Base pour la définition de PC. Pour une AC d'entreprise, pas besoin de tout reprendre systématiquement.
- Aide au choix de produits de sécurité

- Groupe ARKOON
- Société de service et éditeur de logiciels spécialisé dans la sécurité logique et les réseaux
- Produits : Gamme Security BOX®

- Adresse : 3 place Renaudel
69003 LYON
Tél : 04 78 14 04 10 Fax : 04 78 14 04 11
Web : <http://www.securitybox.net>

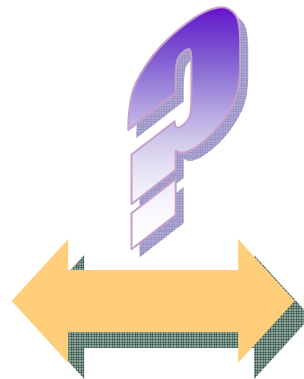
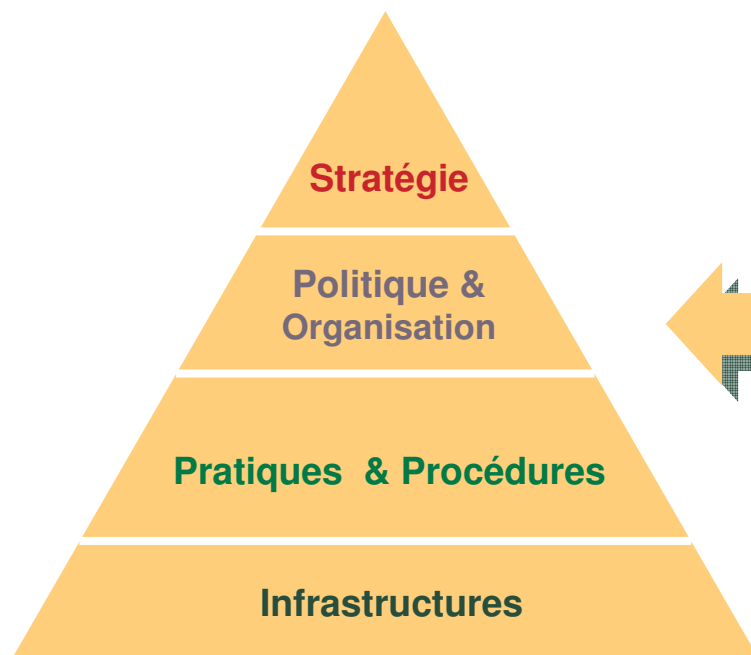
- Philippe PERRET
Directeur Technique
philippe.perret@msi-sa.fr



Point sur les normes x7799

Mercredi 19 octobre 2005

■ Rappel de l'épisode précédent ...



Identification	Désignation	Source
▪ EBIOS	Méthode	DCSSI
▪ MEHARI	Méthode	CLUSIF
▪ OCTAVE	Méthode	CERT
▪ PSSI	Guide méthodologique	DCSSI
▪ TDBSSI	Guide méthodologique	DCSSI
▪ PC2	Guide méthodologique	DCSSI
▪ DSIS	Guide méthodologique	DCSSI
▪ Memento DeP	Guide méthodologique	DCSSI
▪ sp800-60	Guide méthodologique	NIST
▪ PSC-SI	Guide de bonnes pratiques	GMSIH
▪ PAU	Guide de bonnes pratiques	GMSIH
▪ ITIL	Guides de bonne pratiques	itSMF – BSI
▪ Guide SMSI	Guide de bonnes pratiques	CNRS
▪ CobIT	Guide de bonnes pratiques	ISACA - ITGI
▪ ISF	Guide de bonnes pratiques	ISF
▪ ITSEC	Norme d'exigences	DCSSI
▪ ISO 15408	Norme d'exigences	DCSSI
▪ EESSI	Normes d'exigences	MINEFI
▪ NF Z 42-013	Normes d'exigences	AFNOR
▪ 21 CFR Part 11	Norme d'exigences	FDA
▪ ISO 13335	Norme de bonnes pratiques	ISO
▪ ISO 13569	Norme de bonnes pratiques	ISO
▪ ISO 17799	Norme de bonnes pratiques	ISO
▪ PRIS	Politique de référencement	DCSSI
▪ sp800-45	Guide technique	NIST
▪ PPnc004	Guide technique	DCSSI

- Disposer d'un référentiel pour :
 - Suivre les bonnes pratiques en termes de gestion de la sécurité de manière transverse : infrastructures, procédures, politique, organisation et stratégie.
 - Mettre en place un système de suivi et de pilotage de ces différents aspects.

- Quelles réponses apportées par les normes x7799 ?
 - Présentation de l'ISO 17799:2005
 - Présentation de la BS 7799-2
 - Comparaison des deux normes
 - Point sur la certification x7799

- Référentiel de bonnes pratiques découpant la mise en œuvre de la SSI suivant 11 thématiques opérationnelles

Structure de la norme ISO17799 :

- Politique sécurité
- Organisation de la sécurité
- Classification
- Sécurité et personnel
- Sécurité et environnement physique
- Réseau et administration informatique
- Contrôle d'accès au système
- Développement et maintenance informatique
- Gestion des incidents
- Plan de continuité
- Conformité légale et audits de contrôle

11 ACCESS CONTROL	→	Chapitre (1^{er} niveau)
11.1 BUSINESS REQUIREMENT FOR ACCESS CONTROL		
11.1.1 Access control policy		
11.2 USER ACCESS MANAGEMENT	→	Thème (2^{eme} niveau)
11.2.1 User registration		
11.2.2 Privilege management		
11.2.3 User password management		
11.2.4 Review of user access rights		
11.3 USER RESPONSIBILITIES		
11.3.1 Password use	}	→ Mesure (3^{eme} niveau)
11.3.2 Unattended user equipment		
11.3.3 Clear desk and clear screen policy		
11.4 NETWORK ACCESS CONTROL		
11.4.1 Policy on use of network services		
11.4.2 User authentication for external connections		
11.4.3 Equipment identification in networks		
11.4.4 Remote diagnostic and configuration port protection		
11.4.5 Segregation in networks		
11.4.6 Network connection control		
11.4.7 Network routing control		
11.5 OPERATING SYSTEM ACCESS CONTROL		
11.5.1 Secure log-on procedures		
11.5.2 User identification and authentication		
11.5.3 Password management system		
11.5.4 Use of system utilities		
11.5.5 Session time-out		
11.5.6 Limitation of connection time		
11.6 APPLICATION AND INFORMATION ACCESS CONTROL		
11.6.1 Information access restriction		
11.6.2 Sensitive system isolation		
11.7 MOBILE COMPUTING AND TELEWORKING		
11.7.1 Mobile computing and communications		
11.7.2 Teleworking		

10.5.1 Information back-up

Control

Back-up copies of information and software should be taken and tested regularly in accordance with the agreed backup policy.

Implementation guidance

Adequate back-up facilities should be provided to ensure that all essential information and software can be recovered following a disaster or media failure.

The following items for information back up should be considered:

- a) the necessary level of back-up information should be defined;
- b) accurate and complete records of the back-up copies and documented restoration procedures should be produced;
- c) the extent (e.g. full or differential backup) and frequency of backups should reflect the business requirements of the organization, the security requirements of the information involved, and the criticality of the information to the continued operation of the organization;
- d) the back-ups should be stored in a remote location, at a sufficient distance to escape any damage from a disaster at the main site;
- e) back-up information should be given an appropriate level of physical and environmental protection (see clause 9) consistent with the standards applied at the main site; the controls applied to media at the main site should be extended to cover the back-up site;
- f) back-up media should be regularly tested to ensure that they can be relied upon for emergency use when necessary;
- g) restoration procedures should be regularly checked and tested to ensure that they are effective and that they can be completed within the time allotted in the operational procedures for recovery;
- h) in situations where confidentiality is of importance, back-ups should be protected by means of encryption.

Back-up arrangements for information systems should be regularly tested to ensure that they meet the requirements of the business continuity plan (see clause 14). For critical systems, the backup arrangements should include information, applications, and data necessary to recover the

118
points de
contrôle

information, and also any requirement for archive copies to be retained (see 15.1.3).

use the back-up and restore process. Such automated processes should be implemented and at regular intervals.

Mesure de sécurité

Préconisations
d'implémentation
(4^{eme} niveau)

Autre

- Pas d'exhaustivité des mesures de sécurité
- Des mesures pas toutes nécessairement applicables
- Nécessité d'une prise de recul et d'une réelle expertise
- Statique tant en termes de mesures que de procédures

0.8 Developing your own guidelines

This code of practice may be regarded as a starting point for developing organization specific guidelines. Not all of the controls and guidance in this code of practice may be applicable. Furthermore, additional controls and guidelines not included in this standard may be required. When documents are developed containing additional guidelines or controls, it may be useful to include cross-references to clauses in this standard where applicable to facilitate compliance checking by auditors and business partners.

10.5.1 Information back-up

Control

Back-up copies of information and software should be taken and tested regularly in accordance with the agreed backup policy.

Implementation guidance

Adequate back-up facilities should be provided to ensure that all essential information and software can be recovered following a disaster or media failure.

The following items for information back up should be considered:

- a) the necessary level of back-up information should be defined;
- b) accurate and complete records of the back-up copies and documented restoration procedures should be produced;
- c) the extent (e.g. full or differential backup) and frequency of backups should reflect the business requirements of the organization, the security requirements of the information involved, and the criticality of the information to the continued operation of the organization;
- d) the back-ups should be stored in a remote location, at a sufficient distance to escape any damage from a disaster at the main site;
- e) back-up information should be given an appropriate level of physical and environmental protection (see clause 9) consistent with the standards applied at the main site; the controls applied to media at the main site should be extended to cover the back-up site;
- f) back-up media should be regularly tested to ensure that they can be relied upon for emergency use when necessary;
- g) restoration procedures should be regularly checked and tested to ensure that they are effective and that they can be completed within the time allotted in the operational procedures for recovery;
- h) in situations where confidentiality is of importance, back-ups should be protected by means of encryption.

Back-up arrangements for individual systems should be regularly tested to ensure that they meet the requirements of business continuity plans (see clause 14). For critical systems, the backup arrangements should cover all systems information, applications, and data necessary to recover the complete system in the event of a disaster.

The retention period for essential business information, and also any requirement for archive copies to be permanently retained should be determined (see 15.1.3).

Other information

Back up arrangements can be automated to ease the back-up and restore process. Such automated solutions should be sufficiently tested prior to implementation and at regular intervals.

- Un référentiel d'audit (par exemple) :
 - Données sauvegardées ?
 - Documentation des sauvegardes ?
 - Fréquence et mode de sauvegarde ?
 - Stockage ?
 - Sécurité des sauvegardes ?
 - Tests des supports ?
 - Tests de restauration ?
 - Confidentialité des sauvegardes ?
 - BCP sous-jacent ?
 - ...

■ ISO17799 (ou BS7799-1): norme de recommandation

- Énumère un catalogue de « bonnes pratiques » de sécurité de l'information
- Couvre tous les domaines de la sécurité
- Définit un « vocabulaire » commun
- Indique « quoi faire » sans pour autant dire « comment faire »

■ BS7799-2 : norme d'exigences

- Définit le Système de Management de la Sécurité de l'Information
- Apporte une dynamique (cycle « PDCA »)
- Fait référence à des mesures de sécurité dont l'implémentation est obligatoire
- Base d'une normalisation internationale à horizon 2006 (ISO 27001)

Ne dites pas « Je devrais » mais « Je dois »

7.2 Equipment security

Objective: To prevent loss, damage or compromise of assets and interruption to business activities.

Equipment should be physically protected from security threats and environmental hazards. Protection of equipment (including that used off-site) is necessary to reduce the risk of unauthorized access to data and to protect against loss or damage. This should also consider equipment siting and disposal. Special controls may be required to protect against hazards or unauthorized access, and to safeguard supporting information systems, electrical supply and cabling infrastructure.

7.2.1 Equipment siting and protection

Equipment should be sited or protected to reduce the risks from environmental threats and hazards, and opportunities for unauthorized access. The following controls should be considered.

- Equipment should be sited to minimize unnecessary access into work areas.
- Information processing and storage facilities handling sensitive data should be positioned to reduce the risk of overlooking during their use.
- Items requiring special protection should be isolated to reduce the general level of protection required.
- Controls should be adopted to minimize the risk of potential threats including:
 - theft;
 - fire;
 - explosives;
 - smoke;
 - water (or supply failure);
 - dust;
 - vibration;
 - chemical effects;
 - electrical supply interference;

BS 7799-2:2002

A.7 Physical and environmental security

A.7.1 Secure areas		BS ISO/IEC 27002
<i>Control objective:</i> To prevent unauthorized physical access, damage to business premises and information.		
<i>Controls</i>		
A.7.1.1	<i>Physical security perimeter</i>	Organizations shall use security perimeters to protect areas that contain information processing facilities.
A.7.1.2	<i>Physical entry controls</i>	Secure areas shall be protected by appropriate entry controls to ensure that only authorized personnel are allowed access.
A.7.1.3	<i>Securing offices, rooms and facilities</i>	Secure areas shall be created in order to protect offices, rooms and facilities with special security requirements.
A.7.1.4	<i>Working in secure areas</i>	Additional controls and guidelines for working in secure areas shall be used to enhance the security of secure areas.
A.7.1.5	<i>Isolated delivery and loading areas</i>	Delivery and loading areas shall be controlled, and where possible, isolated from information processing facilities to avoid unauthorized access.
A.7.2 Equipment security		7.2
<i>Control objective:</i> To prevent loss, damage or compromise of assets and interruption to business activities.		
<i>Controls</i>		
A.7.2.1	<i>Equipment siting and protection</i>	Equipment shall be sited or protected to reduce the risks from environmental threats and hazards, and opportunities for unauthorized access.
A.7.2.2	<i>Power supplies</i>	Equipment shall be protected from power failures and other electrical anomalies.
A.7.2.3	<i>Cabling security</i>	Power and telecommunications cabling carrying data or supporting information services shall be protected from interception or damage.
A.7.2.4	<i>Equipment maintenance</i>	Equipment shall be correctly maintained to enable its continued availability and integrity.
A.7.2.5	<i>Security of equipment off-premises</i>	Any use of equipment for information processing outside an organization's premises shall require authorization by management.

- Notion de système de management introduite par l'ISO au travers de l'ISO9000 et l'ISO14000
- Système de management
 - Ensemble d'éléments corrélés ou interactifs permettant d'établir une politique et des objectifs et d'atteindre ces objectifs
 - Éléments = politiques, procédures, moyens humains, moyens techniques.
- Système de management de la sécurité
 - Système de management, basé sur une approche de gestion des risques, visant à définir, mettre en œuvre et continuellement vérifier / maintenir / améliorer la sécurité de l'information au sein d'un organisme
- Formalisation de la mise en œuvre d'une démarche de management de la sécurité de l'information

■ ISO9000 : SMQ

- Approche PDCA
- Sur un périmètre défini
- On écrit ce qu'on fait
- On le fait

■ BS7799-2 : SMSI

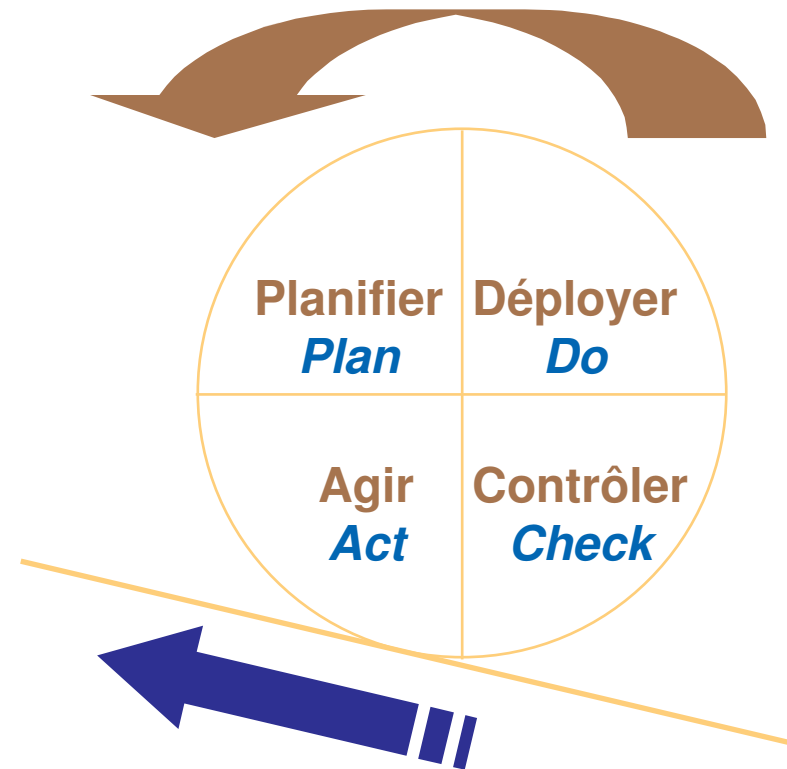
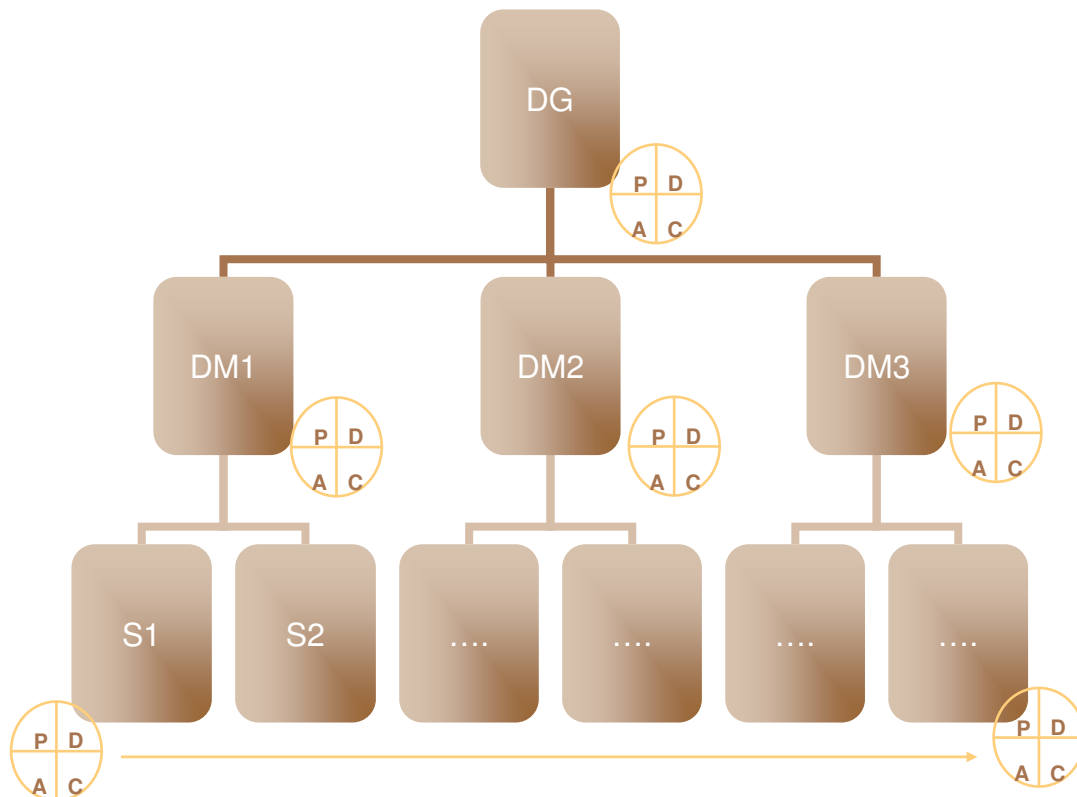
- Approche PDCA
- Sur un périmètre défini
- Existence d'un ensemble de mesures normatives
- Ce qu'on doit faire est dicté par :

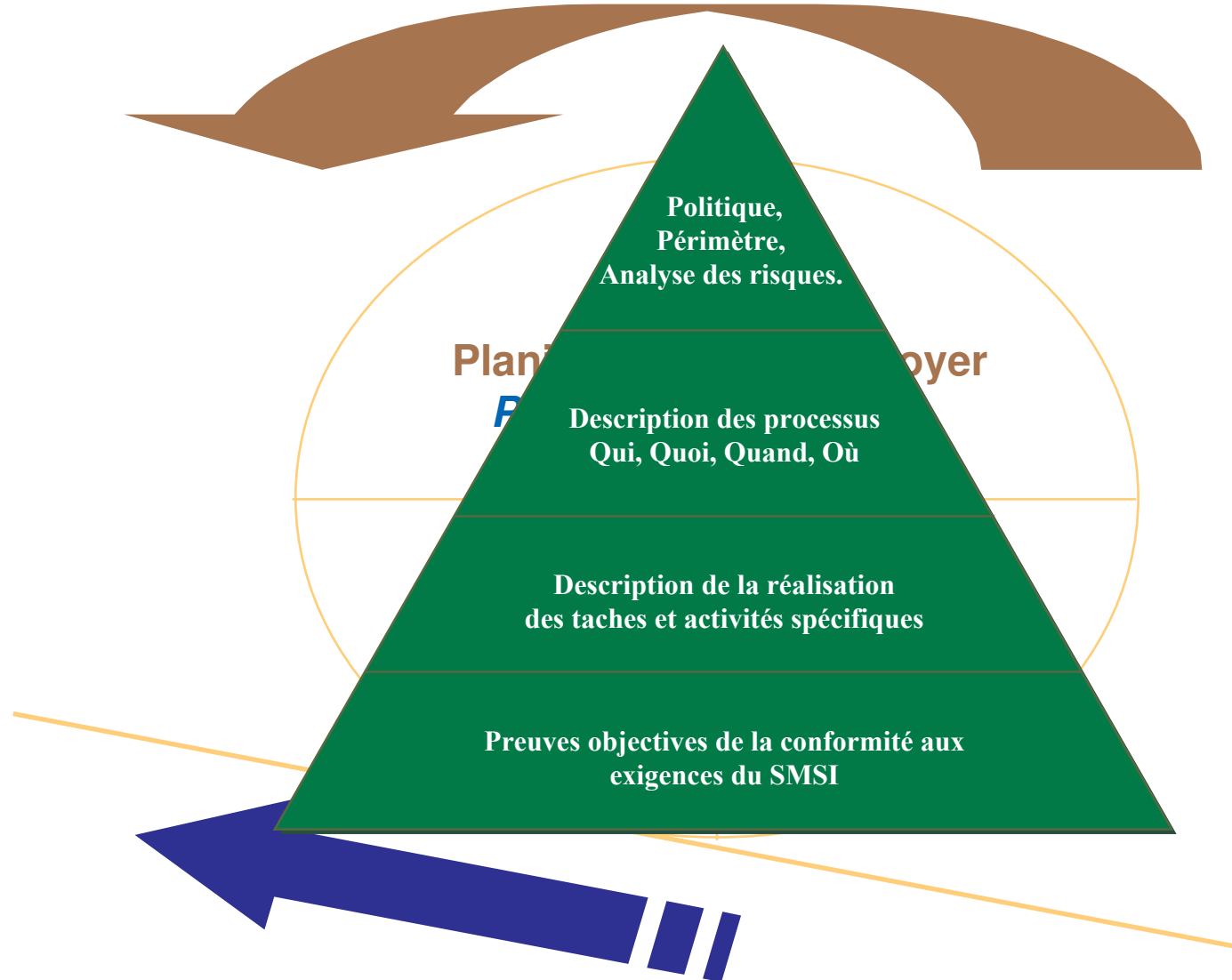
Une analyse des risques
Les mesures normatives

Quelques mots sur l'analyse de risques

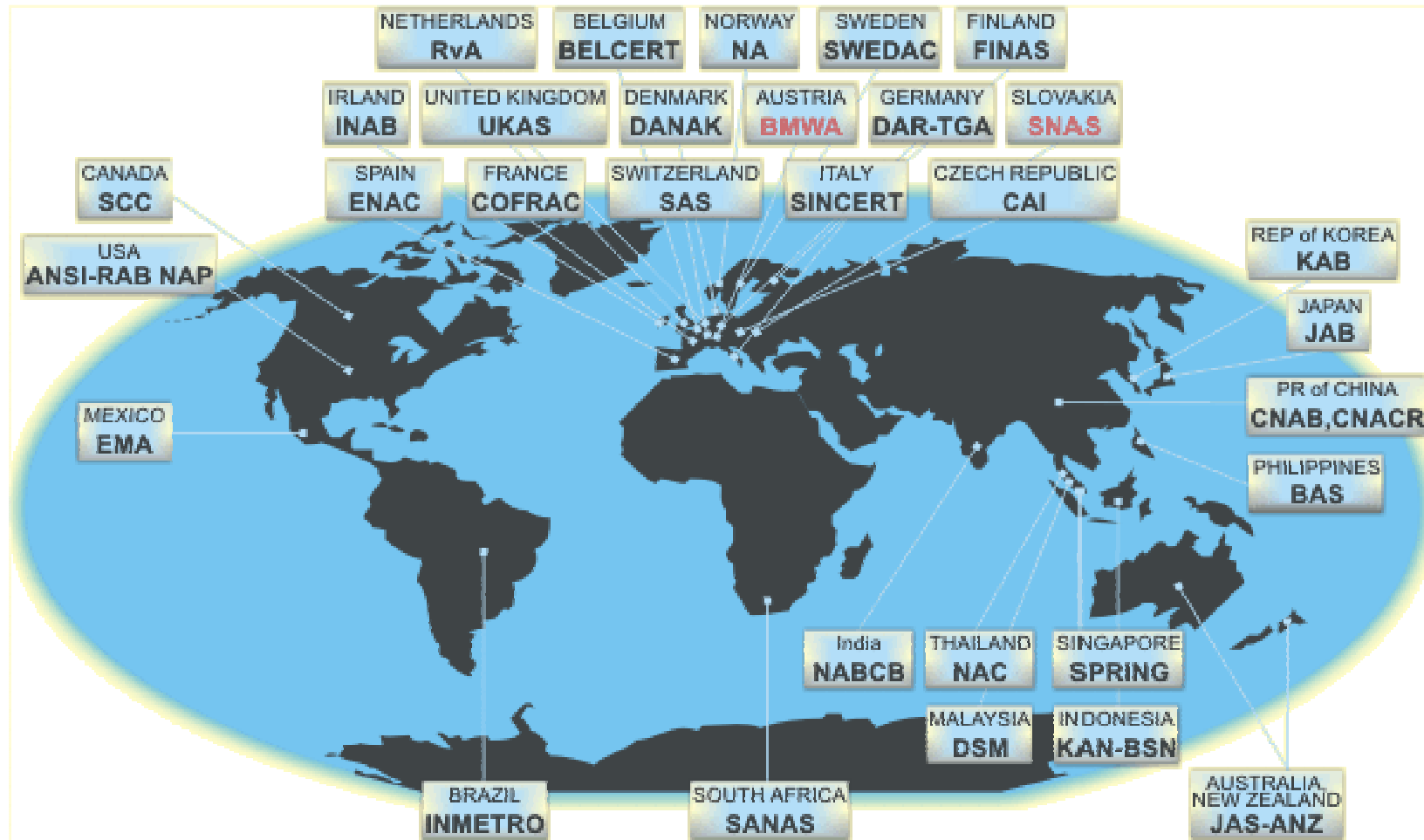
- Il n'y a pas d'obligation à employer une méthode d'analyse des risques spécifique
- Les outils & référentiels sur le sujet en France sont nombreux : MARION, MEHARI, MELISSA, EBIOS, ...
- L'objet de la gestion des risques suivant un SMSI repose davantage sur des principes applicables par le management que sur des outils employés par les équipes informatiques :
 - Disposer d'une vue complète de l'environnement business (compréhension des menaces et connaissance de la sensibilité des actifs)
 - Comprendre les « forces » qui sont contre l'organisme et celles qui le protègent (analyse des vulnérabilités)
 - Trouver le bon équilibre qui permette de supporter « un certain niveau de risque » (analyse des risques)
 - Comprendre les facteurs d'influence qui conduiront à repenser cet équilibre
 - S'organiser pour suivre et prendre en compte ces changements de manière cyclique

- Suivre et prendre en compte les changements de manière cyclique : **PDCA**





- La certification est prononcée par un Organisme de Certification (*Certification Body*), ce peut être une entreprise privée
- L'organisme de certification est accrédité :
 - L'accréditation c'est la reconnaissance qu'il dispose d'auditeurs compétents et qualifiés pour conduire les audits BS7799-2
 - L'accréditation des compétences en sécurité et systèmes d'information suit l'EN45012 et l'EA-7/03
 - L'accréditation des compétences en audit suit l'ISO 19011
- L'audit suit 6 étapes :
 - Définition du périmètre de certification (défini par l'audité et revu par le CB)
 - Revue de la documentation du SMSI
 - Visites de sites pour contrôle de la mise en œuvre du SMSI
 - Délivrance et remise du certificat
 - Audits de surveillance
 - Re-certification



Nombre de certificats par pays (source xisec)

Japan	1023	Czech Republic	6	Bahrain	1
UK	215	Poland	5	Chile	1
India	131	Spain	5	Colombia	1
Taiwan	57	Brazil	4	Egypt	1
Germany	48	Greece	4	France	1
Korea	34	Iceland	4	Lebanon	1
Italy	31	Argentina	3	Lithuania	1
USA	26	Kuwait	3	Luxemburg	1
Netherlands	22	Mexico	3	Macau	1
Australia	17	Saudi Arabia	3	Macedonia	1
Hong Kong	17	UAE	3	Morocco	1
Finland	15	Belgium	2	Qatar	1
China	14	Canada	2	Romania	1
Hungary	13	Croatia	2	Russian Federation	1
Ireland	11	Denmark	2	Slovenia	1
Norway	11	Isle of Man	2	South Africa	1
Singapore	11	Malaysia	2	Turkey	1
Austria	8	Philippines	2	Relative Total	1802
Switzerland	8	Slovak Republic		Absolute Total	1790
Sweden	7	Thailand			

Seule boîte à outils utile de la SSI ?

- Une boîte à outils très complète pour gérer la sécurité de l'information d'entreprise
 - ISO 17799 : contrôler ma conformité aux bonnes pratiques
 - BS7799-2 : mesurer et améliorer mon efficacité au quotidien et sur le long terme
- Le JTC1/SC 27 de l'ISO propose un corpus de norme très complémentaires sur les sujets de la sécurité :
 - WG1 : Management de la sécurité
17799, 13335 (GMITS), 18028 (réseaux), 18044 (gestion d'incidents), 18043 (détection d'intrusions), 14516 (tiers parties de confiance)
 - WG2 : Techniques cryptographiques
9796 & 14888 (signature), 9798 (authentification), 18033 (algorithmes), 11770 (gestion de clés)
 - WG3 : Evaluation de la sécurité de produits et systèmes IT
15408 (critères communs), 15446 & 15292 (profils de protection), TBD (modules crypto & biométrie)
- Le JTC1 est « doté » d'autres comité techniques :
 - SC37 : biométrie
 - SC6 : réseaux