CLUB EBIOS – réunion du 17 Janvier 2008

ISO 27001

Présentation & Caractéristiques

Par Mauro ISRAEL – certifié Lead Auditor ISO27001
mise à jour janvier 2008

ISO 27001 en 6 questions

- D'où vient la norme ISO 27001 ?
- En quoi consiste la norme ?
- Comment la mettre en œuvre ?
- Les livrables de l'ISO 27001 ?
- En quoi consiste la certification ?
- EBIOS dans ISO ?

Petit historique de la certification en sécurité (1)

ISO 13335: l'évaluation des risques

- **ISO 13335:** Normaliser la sécurité à consisté tout d'abord en une analyse de risques: ISO 13335 ou « DICP »: Disponibilité – Intégrité – Confidentialité – Preuve
- L'idée est de mesurer les risques liés aux menaces sur les biens immatériels et matériels liés aux systèmes d'information.
- Une fois les menaces et les vulnérabilités recensées, une analyse en termes d'impact permet de déterminer le risque:
  - Impact financier - Impact sur l'image de marque - Conséquences juridiques
- Le risque est ensuite traité par des mesures de réduction, de transfert ou d'élimination et les risques résiduels sont évalués
- Cette norme, bien qu'intéressante, ne dit pas comment renforcer la sécurité et avec quoi…

Petit historique de la certification en sécurité (2)

ISO15408: « critères communs »

- Le besoin de certifier des produits de sécurité s'est fait sentir en complément de l'analyse de risques
- Cette norme consiste à évaluer des produits en laboratoire et leur donner une note, de EAL1 à EAL 5, par exemple EAL4+
- Très utile pour vérifier le niveau de sécurité d'un produit comme un firewall ou une carte à puce, cette norme ne préjuge en rien de la sécurité globale d'une entreprise.

Petit historique de la certification en sécurité (3)

BS7799-ISO17799: la certification « Anglo-Asiatique »

- Issue des travaux du British Standard, cette norme propose une vision globale de la sécurité des S.I. en près de 10 chapitres.
- La BS7799-1 traite des principes généraux alors que la « -2 » traite des principes appliqués.
- La norme couvre aussi bien la sécurité physique, les notions de meilleures pratiques que les réseaux, les systèmes, la classification des données, les plans de continuité etc…

Petit historique de la certification en sécurité (4)

- La norme BS7799 à été translatée en ISO17799:2000, mais uniquement le -1;
- La BS7799 a été revue en 2005.
- ISO 17799 ne permet pas de se faire certifier, en revanche BS7799-2:2005, oui
- De nombreuses entreprises UK et Asiatiques (notamment au Japon) se sont faites certifier: on a atteint le chiffre de 1000 dont 1 seule en France (Axalto)
- La BS7799-2:2005 a été référencée ISO sous le terme de ISO/IEC 27001:2005 en Novembre 2005

La certification ISO 27001

- La norme **IS27001:2005** comprend les chapitres 4 à 8 qui définissent le **périmètre de certification, le SMSI, l'analyse de risques, le traitement de ces risques ainsi que les engagements et actions à mener pour certifier un système de management de la sécurité.**
- Le système est donc **global et complet**. Il permet de faire certifier un périmètre cohérent.
- L'annexe « A » reprend les **133 contrôles** de IS17799:2005 pour choisir ceux applicables au SMSI: bientôt ISO27002
- Un SoA: **Statement of Applicability** définit ainsi les mesures de sécurité applicables et auditables par les audits de certification.
- La certification IS27001 est la première d'une **série ISO27xxx** qui reprend tous les éléments des normes précédentes ISO13335 notamment.
- Une **méthode d'audit ISO 19011** garantit la qualité et l'impartialité des audits de certification.

Méthode d’audit qualité ISO 19011

• L'ISO 19011:2002 fournit des conseils sur les principes de l'audit, le management des programmes d'audit, la réalisation d'audits de systèmes de management de la qualité et/ou de management environnemental ainsi que sur la compétence des auditeurs de ces systèmes.

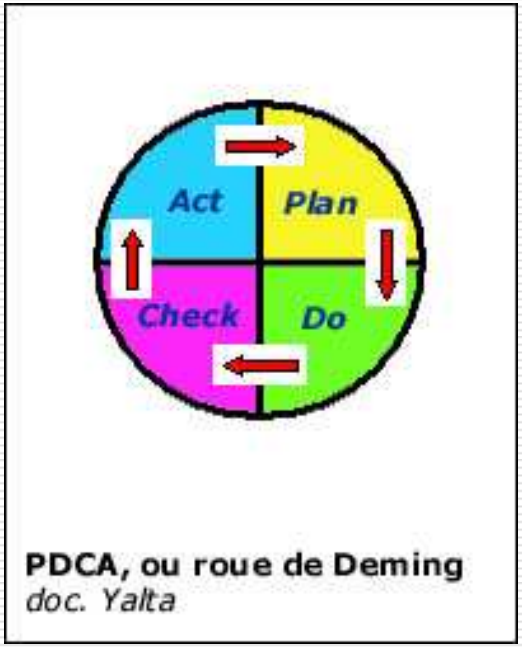
• Elle est applicable à tous les organismes qui doivent réaliser des audits internes ou externes de systèmes de management de la qualité et/ou de management environnemental ou manager un programme d'audit.

• L'ISO 19011 peut, en principe, s'appliquer à d'autres types d'audits, à condition toutefois d'accorder une attention particulière à l'identification des compétences requises pour les membres de ces équipes d'audit.

PDCA, ou roue de Deming
doc. Yalta

L'amélioration de la sécurité: un cycle permanent

- Améliorer la sécurité consiste tout d'abord à une analyse de risques: ISO 13335 ou DICP: Disponibilité – Intégrité – Confidentialité – Preuve
- L'idée est de mesurer les risques liés aux menaces sur les biens immatériels et matériels liés aux systèmes d'information.
- Une fois les menaces et les vulnérabilités recensées, une analyse en termes d'impact permet de déterminer le risque:
  - Impact financier - Impact sur l'image de marque - Conséquences juridiques
- Le risque est ensuite traité par des mesures de réduction, de transfert ou d'élimination, et les risques résiduels sont évalués…
- **Le processus d'amélioration suit 4 phases: PLAN – DO – CHECK - ACT**



PDCA, ou roue de Deming
doc. Yalta

Les chapitres de la norme IS27001:2005

Chapitres 1 à 3: Définition de la norme

Chapitres 4 à 8: Définition du SMSI – Périmètre – Analyse de risques - Engagements de la Direction – Définition de la documentation -Définition du programme d'audit

Annexe A: Description des 133 contrôles

par exemple: 9.1.2 Contrôle physique des accès;

- Mesure: protéger les accès des zones sécurisées
- Modalités de mise en œuvre:
  - *consigner la date d'arrivée et de départ des visiteurs*
  - *limiter l'accès aux personnes habilitées*
  - *porter un moyen d'identification visible*
  - *Réexaminer les droits d'accès de manière régulière*

Pourquoi se faire certifier ?

- La norme ISO27001 constitue un excellent référentiel de sécurité des systèmes d'information:
  - Amélioration réelle de votre sécurité
  - Perception améliorée par les partenaires et clients.
- Cette norme propose 133 critères concrets à travers le document ISO27002.
- De nombreuses recommandations et règlementations, notamment dans le domaine financier, vont exiger une évaluation de la sécurité des systèmes d'information: BALE II, LSF…

Les éléments nouveaux à intégrer

- Il est possible de se faire certifier en France à partir du document ISO/IEC 27701 en couvrant les aspects:
  - Techniques
  - Organisationnels
  - Ressources humaines
  - Juridiques
- **On peut se faire certifier uniquement pour un site ou bien un processus ou un département fonctionnel.**
- L'annexe A de la norme ISO27001 (bientôt ISO27002) contient les **133 mesures concrètes** à intégrer dans sa politique de sécurité
- La notion de **Lead Auditor 27001** établit une reconnaissance, et un langage commun entre les parties et les partenaires.

EBIOS avec ISO 27001 ?

- La série ISO 27000 cherche à définir une norme de certification d'un système de management des systèmes d'information, à l'instar d'ISO 9000 pour certifier le management d'un système qualité, et ISO 14000 pour le management d'un système environnemental.
- **EBIOS** (Expression des Besoins et Identification des Objectifs de Sécurité) permet de proposer une méthode d'analyse de risques, car la norme ISO n'oblige pas le choix d'une méthode déterminée, pourvu que celle-ci soit auditable et reproductible à différents endroits avec des résultats semblables.

EBIOS ?

- EBIOS permet d'apprécier et de traiter les risques SSI, de contribuer à leur acceptation et de communiquer à leur sujet
- C'est un outil de négociation, d'arbitrage et de sensibilisation
- Créée en 1995 et maintenue par la DCSSI,
- EBIOS est compatible avec les normes internationales (Guide ISO 73, ISO 15408, ISO 17799, ISO 13335…)

EBIOS dans ISO 27001

- EBIOS représente une aide à la mise en place d'un SMSI:
  - Une méthode structurée identifiant les besoins réels de l'organisme en matière de SSI
  - Le soutien de la démarche spécifiée dans IS27001:2005 Chapitre 4, pour choisir des objectifs et une analyse de risque pertinente
  - La justification du choix des objectifs et mesures de contrôle de l'ISO 27002
  - Une description pratique et détaillée de la mise en œuvre des objectifs et mesures de contrôle de l'annexe A de IS27001:2005 sous la forme d'exigences de sécurité fonctionnelles
  - Une méthode et des résultats réutilisables en vue des itérations successives SMSI (Plan – Do – Check - Act)
    - Traçabilité entre les risques initialement identifiés, les mesures prises et les risques nouveaux ou mis à jour
    - Mesure de l'efficacité des mesures prises par des démonstrations de couverture rigoureuses

Analyse de risques

- EBIOS couvre les principaux risques pertinents:
  - incendie, dégâts des eaux - pollution - accidents majeurs - phénomène climatique, sismique, volcanique, météorologique, crue - défaillance de la climatisation - perte d'alimentation énergétique, des moyens de télécommunications - rayonnements électromagnétiques, thermiques - impulsions électromagnétiques (iem) - interception de signaux parasites compromettants espionnage à distance, écoute passive - vol de supports ou de documents, vol de matériels - divulgation interne, divulgation externe - panne matérielle, dysfonctionnement matériel, saturation du matériel - dysfonctionnement logiciel - destruction de matériels - atteinte à la maintenabilité du système d'information - informations sans garantie de l'origine - piégeage du matériel - utilisation illicite des matériels - altération du logiciel, piégeage du logiciel - copie frauduleuse de logiciels, utilisation de logiciels contrefaits ou copiés - altération des données - abus de droit, usurpation de droit - reniement d'actions - fraude - atteinte à la disponibilité du personnel…

EBIOS dans ISO 27001

Dans le cadre d'une démarche ISO27001, les activités de la démarche EBIOS sont utilisées d'une manière spécifique:

- Étape 1 – Étude du contexte : niveau de détail cohérent avec le périmètre et la finalité de l'étude.
- Étape 2 – Expression des besoins de sécurité : cette étape doit faciliter l'évaluation des risques, l'identification des mesures pertinentes, leur mise en œuvre et la vérification de leur efficacité.
- Étape 3 – Étude des menaces : complète, sans déscendre dans le niveau de détail ultérieur
- Étape 4 – Identification des objectifs de sécurité : référence les risques et permet de sélectionner les objectifs de contrôle
- Étape 5 – Détermination des exigences de sécurité : exploite les mesures de contrôle (intégrées dans les bases de connaissances EBIOS)

CONCLUSIONS

- La certification en sécurité c'est possible et souhaitable
- La certification ISO27001 est un moteur pour l'amélioration de la sécurité au delà du périmètre de certification.
  - Les processus et les réflexes mis en place sont aisément transposables pour améliorer la sécurité dans tous les secteurs de l'entreprise
- La confiance est un axe majeur de différenciation commerciale
- La certification permet une lisibilité des budgets sécurité vis-à-vis de la Direction Générale
- La normalisation est une tendance de fond
- La certification permet d'améliorer et de faciliter - La gouvernance - Le benchmarking - La conformité
- EBIOS peut parfaitement être utilisé pour l'appréciation des risques et la définition des chantiers d'amélioration.
- EBIOS fournit un guide méthodologique précis et exhaustif, ce qui permet ensuite une liaison simple avec la déclaration d'applicabilité ISO27002.

Conclusion

« La personne qui prétend que ça ne peut pas se faire, ne doit pas interrompre la personne en train de le faire… »

-- Proverbe Chinois

Questions - Réponses ?

Merci de votre attention,

Mauro ISRAEL - *Lead AUDITOR ISO/IEC 27001 - Responsable de la Sécurité des Systèmes d'Information*

Les adresses et documents utiles

- http://www.ssi.gouv.fr
- http://www.27001-online.com
- http://17799.standardsdirect.org/
- http://www.standards-online.net/InformationSecurityStandard.htm

Pour acquérir le document de la norme (135 € environ)

- ISO/CEI 27001:2005
- ISO/CEI 19011:2002 (F)
- ISO/CEI 17799:2005 (F ou EN)