Résumé de INFORMATION SECURITY MANAGEMENT – A NEW PARADIGM

Quelques termes et définitions utilisées :
ISMS = Information Security Management System
IT = Information Technologies
Inf = information
Inf Sec Mgmt = Information security Management
Ent = entreprise

Introduction :

Inf Sec Mgmt nécessite un changement de paradigme vers la protection des informations en terme d'actifs. Les Ent ont besoin d'une approche holistique de la sécurité pour créer et maintenir un environnement d'informations sécurisées.
Un ISMS est constitué d'un mix de : politiques, standards, guidelines, codes de conduite, technologie, aspects humain, légaux et éthiques. Il permet d'implémenter ISO 17799.
Approches de Inf Sec Mgmt (holistique): Perspective stratégique (corporate governance, politiques) ; humaine (culture sécurité , attentivité, entrainement, éthique,…) ; technologique (soft- et hardware)

2 approches pour implémenter un ISMS :
process security
product security

Sécurité IT comprends 5 éléments de services de sécurité (selon ISO 7498-2):

- Identification & authentification
- autorisation
- confidentialité
- intégrité
- non-repudiation (rejet)

ad 2) Definition de Process & Product ISMS (systéme de 2 phases)
Partie Processus :
ISMS but = planifier et implémenter des pratiques mgmt, procédures pour maintenir Sec Inf.
La politique de Sec Inf forme la base du processus ISMS
En premier il faut implémenter les guideline et contrôles comme dans ISO 17799
En 2.) faut contrôler l'implémentation et l'adéquation avec le standard
3.) certification externe
Principe de l'amélioration continue (donc processus itératif) → voir roue deming (plan, do,check,act)

Partie Product ISMS:
But du Systeme mgmt ici : choisir Software évaluée afin d'établir la sécurité d'information.
Sur base de besoins définis, il faut processus d'évaluation de produit et tests (blablabla…)
Review par externe serait idéal…faire audit d'évènements, analyse de canaux couverts (covert channels) → tout cela fait partie du processus de certification ISMS.
Des produits certifiés peuvent être catégorisés en 3 (bases de données, systèmes opérationnels, Réseaux) et attribuées à chacune des sections (classes de protection ou assets) de ISO 17799.

Ad 3) Combiner product et process ISMS via les classes de protection rel à ISO 17799
Chacune des 10 sections de ISO 17799 est classifiée selon 4 classes (niveaux de protection)
Tout produit ne concerne pas chaque section et toute section n'est pas importante pour l'entreprise.
Une approche section par section permet réduction de complexité et choix selon besoins.
La classification en 4 niveaux de protection est fait en fonction des dimensions/sections ISO.
- niveau de conformité avec ISO et – utilisation des produits certifiés associés à chaque section ISO.

Classe 1 : Protection inadéquate
Aucun effort est fait pour implémenter les contrôles recommandés relatifs aux besoins/situation
L'utilisation des produits certifiés ou non n'a pas d'influence à ce niveau
Classe 2 : Protection minimale
Un effort minimal pour implémenter les contrôles est fait (conformité aux contrôles est à 75%).
L'utilisation des produits certifiés ou non n'a pas d'influence à ce niveau

Classe 3 : Protection raisonnable
Pour certaines sections de ISO, exigé d'implémenter processus pour prouver que contrôles sont faits
Pour certaines sections il est exigé de utiliser produits certifiés (=>faut 1/2 des produits listés exigés)
Classe 4 : Protection adéquate
Pour classifier une section en classe 4, il faut prouver qu'un effort « considérable » est fait pour implémenter les contrôles recommandés pour cette section d'ISO. Cela implique correspondance totale aux « codes de pratiques » de la section.
Selon exigences de la section, il faut aussi avoir les produits certifiés (p.ex. BD Oracle 8i)

Les sections ISO 17799 sont :

- Security policy
- Security organisation
- Asset classification and control
- Personal security
- Physical and environmental security
- Communications and operations management
- Access control
- Systems development and maintenance
- Business continuity management
- Compliance

Table 2: Protection requirements for ISO17799 sections

ISO17799	Protection class			
	Class 1: Inadequate protection	Class 2: Minimal protection	Class 3: Reasonable protection	Class 4: Adequate protection
3. Security policy			☒	☒
4. Security organisation			☒	☒☒
5. Asset classification and control			☒	☒
6. Personnel security		☒	☒☒	☒☒☒
7. Physical and environmental security		☒	☒☒	☒☒☒
8. Communications and operations management		☒	☒☒	☒☒☒
9. Access control		☒	☒☒	☒☒☒
10. Systems development and maintenance			☒	☒☒☒
11. Business continuity management			☒	☒☒☒
12. Compliance			☒	☒

Legend:

	no requirement
☒	additional requirement based on implemented processes and procedures
☒☒	additional requirement based on implementation of certified products in at least half of the applicable product categories
☒☒☒	additional requirement based on implementation of certified products in all of the applicable product categories

Conclusion (bof !!!)

Se papier propose un framework pour fasciliter une relation entre processus et produits IT. Une implémentation de celui-ci devrait contribuer a une approche holistique du mgmt de la sécurité de l'information.

QUESTIONS pour l'assistent :
Je n'ai pas de questions, car cet article est assez théorique et peu profond, mais bon…peut-être il y a des choses pas claires justement parce qu'il reste peu profond…L'auteur a aussi tendance a rester vague et a mélanger des % de niveau de conformité par rapport aux classes comme décrites dans son article.