Semaine Tech 2013 : La gestion de la sécurité - ISO 27K

Pascal BOU NASSAR

Plan

1- Introduction : La gestion de la sécurité

- Défis
- Les principes à la base de la gestion de la sécurité
- Différents standards dans la gestion de la sécurité

2- Les standards ISO 27K

- Modèle PDCA
- Les domaines d'intervention du standard ISO27002

3- Conclusion

Semaine Tech 2013 : La gestion de la sécurité - ISO 27k (Pascal BOU NASSAR)

II 1- Introduction : La gestion de la sécurité

- La sécurité revient à déterminer ce qui doit être protégé et pourquoi, ce qui a besoin d'être protégé et comment le protéger tant qu'il existe [C. Alberts]
- La gestion de la sécurité est un processus permettant d'assurer la sécurité en intégrant les aspects organisationnels et technologiques. Ce processus permet d'identifier les biens à protéger et de développer des stratégies de protection contre les menaces éventuelles.
- La gestion globale de la sécurité (technologique et organisationnelle) a été élaboré dans plusieurs standards tels que : ISO, COBIT, FISMA, etc.

A 1-1 : Défis

1- Définir :

- quels sont les biens à protéger ?
- quelles sont les mesures de sécurité les plus adéquates pour le système ?

2- Faut-il choisir un des standards dans la gestion de la sécurité ou combiner plusieurs standards ?

3- Comment adapter la sécurité selon les enjeux du système étudié ?

B 1-2 : Les principes à la base de la gestion de la sécurité

Dans le cadre de la gestion de la sécurité d'un système d'information, l'agence nationale de la sécurité des systèmes d'information de France (ANSSI) a défini dans son référentiel général de la sécurité, six principes à la base de la gestion de la sécurité :

1. Adapter une démarche globale

L'objectif est la cohérence d'ensemble de la démarche de sécurisation des systèmes d'information. Il convient à ce titre de n'oublier aucun élément pertinent, pour éviter toute faille qui réduirait la sécurité globale du système d'information.

2. Adapter la sécurité du système d'information selon les enjeux

Il est recommandé que la sécurité du système d'information soit adaptée aux enjeux du système et aux besoins de sécurité, afin d'y consacrer les moyens financiers et humains juste nécessaires mais suffisants.

3. Gérer les risques

Il est obligatoire de suivre une démarche qui consiste à :

1) Identifier l'ensemble des risques pesant sur le système

2) Fixer les objectifs de sécurité, pour répondre de manière proportionnée aux besoins de protection du système et des informations face aux risques identifié

3) En déduire les fonctions de sécurité et leur niveau de mise en œuvre pour atteindre ces objectifs.

4. Élaborer une politique de Sécurité du Système d'Information (SSI)

Élaborer une stratégie globale de sécurité permet de définir le cadre d'utilisation du système d'information. Les politiques définissent entre autres les rôles et les responsabilités des différents acteurs, les règles d'utilisation des systèmes et de l'information, les règles permettant de contrôler l'accès sur l'information, les règles d'utilisation des données privées, les règles d'audit, de sauvegarde, etc.

5. Utiliser les produits et prestataires labellisés pour leur sécurité

La certification de produits ou prestataires permet d'attester de la confiance que l'on peut accorder à des produits de sécurité et à la compétence des professionnels en matière de SSI.

6. Viser une amélioration continue

Il est recommandé de chercher une amélioration constante de la SSI, par exemple en mettant en place un « système de management de la sécurité de l'information » (SMSI) pour planifier les actions de sécurisation et les mettre en œuvre puis les vérifier et améliorer la SSI.

C 1-3 : Différents standards dans la gestion de la sécurité

1-3-1 : Le standard ITSEC de l'Union Européenne

Proposé en 1991, le standard Information Technology Security Evaluation Criteria de l'Union Européenne a été développé pour réaliser une synthèse entre les travaux de certification sécurité des différents états partenaires. Les besoins en termes de « cible

de sécurité » (i.e. le niveau de certification visé) sont décrits selon 8 groupes de critères : identification et authentification, contrôle d'accès, imputabilité, réutilisation d'objets, fidélité, continuité de service, échange de données (incluant l'authentification, le contrôle d'accès, la confidentialité des données, l'intégrité des données et la non-répudiation).

1-3-2 : Les critères communs

Afin de certifier de manière unifiée dans un cadre international le niveau de sécurité atteint par les systèmes des partenaires dans un environnement distribué, le standard 'Common Criteria' (CC) définit à la fois des critères et une méthode d'évaluation.

Ce standard repose sur deux concepts principaux :

- Le profil de protection (PP) représente l'ensemble des besoins et d'objectifs de sécurité pour une catégorie de produits ou systèmes.

- La cible de sécurité (Security Target : ST) décrit les objectifs de sécurité et les besoins associés à une 'cible d'évaluation'.

1-3-3 : Le cadre FISMA du NIST

Le NIST (National Institute of Standards and Technology) a développé des standards pour l'implémentation de la gestion de la sécurité (FISMA : Federal Information Security Management Act).

FISMA est un cadre de gestion qui fait référence à de nombreux documents élaborés par le NIST dans la sécurisation des systèmes d'information. L'objectif du cadre FISMA est la mise en œuvre d'un plan de gestion de la sécurité.

Le cadre couvre des :

- Standards pour la catégorisation de l'information et des systèmes d'information
- Standards des exigences de sécurité minimales pour l'information et les systèmes d'information
- Directives pour la sélection des contrôles de sécurité appropriés aux systèmes d'information
- Guide pour l'évaluation des contrôles de sécurité dans les systèmes d'information et de la détermination de l'efficacité du contrôle de sécurité.
- Directives pour la certification et l'accréditation des systèmes d'information

Les standards de l'ISO : Section Suivante ....

III 2- Les standards ISO 27K

L'ISO et l'IEC (International Electrotechnical Commission) ont publié les standards ISO27001/ISO27002 (anciennement ISO 17799).

Ces standards établissent les lignes directrices et les principes pour préparer, implémenter, maintenir et améliorer la gestion de la sécurité. Le Tableau suivant liste les fonctions offertes par ces standards:

ISO 27001	Gestion de la responsabilité Audit Interne Amélioration de l'ISMS (Information Security Management System)
ISO 27002	Elaboration d'une politique de sécurité Organisation de la sécurité des informations Gestion des biens et des actifs Sécurité physique et environnementale Communications et la gestion des opérations Contrôle d'accès Systèmes d'acquisition de l'information Développement et maintenance Gestion des incidents de sécurité des informations Gestion de la continuité Conformité

Les standards ISO27001/ISO27002 font partie d'une série de standards publiés par l'ISO sur la gestion de sécurité:

- Le standard ISO27003 fournit une aide et des conseils dans la mise en œuvre d'un système de gestion de la sécurité. Il s'agit notamment de mettre l'accent sur la méthode PDCA (Plan, Do, Check, ACT) pour l'établissement, la mise en œuvre, le contrôle et l'amélioration du système de gestion.
- Le standard ISO27004 fournit les directives pour l'évaluation d'un système de gestion de sécurité.
- Le standard ISO27005 fournit les directives pour la gestion des risques dans une entreprise.
- Le standard ISO27006 fournit les directives pour l'accréditation des organismes qui offrent la certification ISO.

A 2-1 : Modèle PDCA

Dans l'ISO 27001, le modèle PDCA est appliqué à la structure de tous les processus d'un Système de gestion de la sécurité de l'information (SGSI,SMSI ou ISMS).

L'approche proposée est une approche processus pour :

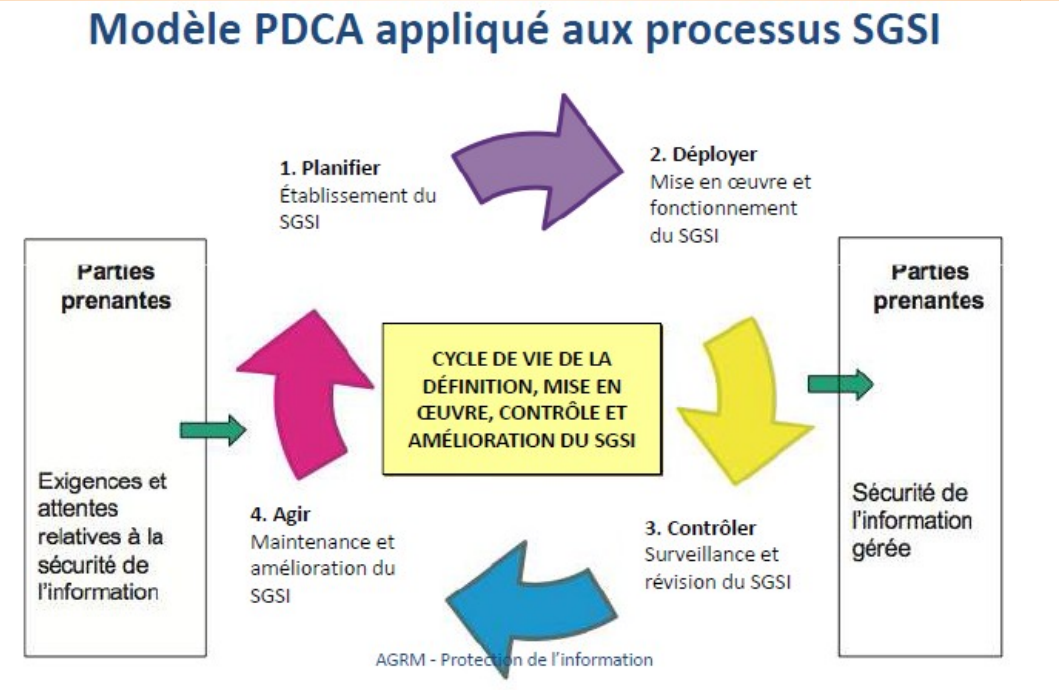
• l'établissement (Planifier)

• la mise en œuvre et le fonctionnement (Déployer)

• la surveillance et la révision (Contrôler)

• la maintenance et l'amélioration (Agir)

du SGSI d'un organisme.



(Ref : *AGRM*[1])

Exemple : Audit de pare-feu

• Le pare-feu assure la segmentation du réseau au moyen de règles de filtrage.

• Des nouvelles règles sont ajoutées régulièrement.

- Pour de nouveaux réseaux
- Pour de nouvelles applications

1 - https://www.google.com.lb/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&ved=0CCwQFjAA&url=http%3A%2F%2Fwww.agrmpi.ca%2Fdocuments%2F1_PDCA_ISO_27001.pdf&ei=Pk4kUt3-G8up0AXM84CwBw&usg=AFQjCNGNzq_aZJEm_pMLywJUM-Cd3tiH4Q&sig2=sGSFWXnYOnJS4rUAWya4xw&bvm=bv.51495398,d.d2k

- Pour des tests

• Une équipe compétente s'occupe de gérer le pare-feu.

• Les règles commencent à s'accumuler un peu trop...

• Nécessité de protéger les données sensibles par filtrage du réseau

• La quantité de règles rend la gestion du pare-feu ardue.

• Beaucoup de règles maintenant obsolètes sont toujours présentes.

• Applications qui n'existent plus

• L'objectif de protection réseau n'est plus atteint.

--> Remédier à ce problème avec le PDCA

(Ref : *AGRM*[2])

PLANIFIER

• Identifier les flux autorisés.

• Formaliser une liste de règles.

DÉPLOYER

• Configurer le pare-feu et le routeur.

CONTRÔLER

• S'assurer que les règles présentes dans le pare-feu et le routeur sont cohérentes avec la liste de règles.

AGIR

• Si ce n'est pas le cas, modifier la liste de règles ou la configuration.

(Ref : *AGRM*[3])

B 2-2 Les domaines d'intervention du standard ISO27002

1. Politique de sécurité

Procurer des directives et des conseils de gestion pour améliorer la sécurité des données. La politique de sécurité, définissant la stratégie globale de la sécurité devra être signée par la haute direction.

2 - https://www.google.com.lb/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&ved=0CCwQFjAA&url=http%3A%2F%2Fwww.agrmpi.ca%2Fdocuments%2F1_PDCA_ISO_27001.pdf&ei=Pk4kUt3-G8up0AXM84CwBw&usg=AFQjCNGNzq_aZJEm_pMLywJUM-Cd3tiH4Q&sig2=sGSFWXnYOnJS4rUAWya4xw&bvm=bv.51495398,d.d2k
3 - https://www.google.com.lb/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&ved=0CCwQFjAA&url=http%3A%2F%2Fwww.agrmpi.ca%2Fdocuments%2F1_PDCA_ISO_27001.pdf&ei=Pk4kUt3-G8up0AXM84CwBw&usg=AFQjCNGNzq_aZJEm_pMLywJUM-Cd3tiH4Q&sig2=sGSFWXnYOnJS4rUAWya4xw&bvm=bv.51495398,d.d2k

Exemple de politique de sécurité :

Les informations traitées au sein de l'AuF nécessitent une protection particulière, permettant d'en maîtriser et d'en limiter la diffusion, dans des conditions définies dans la présente politique. Il existe trois niveaux de classification : Secret, Confidentiel, Public.

Peuvent faire l'objet de ces classifications les procédés, objets, documents, informations, données informatisées ou fichiers dont la divulgation est de nature à nuire à l'Agence.

.....

2. Organisation de la sécurité des informations

- Implication de la direction de la sécurité de l'information : Définir les objectifs de la sécurité qui assurent l'alignement métier / Sécurité de l'info
- Impliquer les responsables métier des différents départements dans la définition des besoins de sécurité
- Définir Les rôles et les responsabilité
- Définir les accords de confidentialité
- Élaborer la liste des contacts des autorités nécessaire dans le cas d'une atteinte physique ou logique à l'information (ex : pompier, police, ISP (dans le cas d'une attaque par Internet), etc.
- Adresser les aspects de la sécurité avec les clients et les fournisseurs (droits d'accès, contrats, durée de contrats, etc)

3. Gestion des biens et des actifs

- Création de l'inventaire des biens à protéger (ex : peronnes, logiciels, matériel, services, données, contrats, documentation métier et tech, procédure, plan de continutié, etc.)
- Identification des propriétaire des biens (personnes responsables de la classification des biens et de la définition des droits d'accès)
- Classification des biens : Attribution d'un niveau de protection.

4. Sécurité du personnel

Réduire les risques d'erreur humaine, de vol, de fraude ou d'utilisation abusive des équipements.

Exemple Définition de(s) :

- la procédure de sélection des candidats (screening)
- Responsabilités
- Conditions d'embauche (signature d'un contrat de confidentialité avec le personnel)
- Terminaison d'un contrat et suppression des droits d'accès

5. Sécurité physique et environnementale.

Empêcher la violation, la détérioration et la perturbation des installations et des données industrielles.

Exemple définition / identification de(s) :

- périmètre des zones sécurisés (locaux techniques ou autres)
- Mesures de contrôle d'accès (enregistrement du temps d'entrée/sortie ; présenter un id, etc)
- Mesures de contrôle contres les menaces de types naturelles (inondation, feu, etc)
- Mesure préventives support pour l'électricité (onduleur) la température (climatisation) feu (extincteur),etc
- Sécurité du câblage (sécuriser l'accès aux câbles en particulier des systèmes critiques)

6. Communications et gestion des opérations

Développement des procédures dans la gestion de la sécurité :

- Création, mise à jour de la documentation (ex : backup, procédures d'installation, gestion des mises à jour, du changement, séparation des roles, séparation des modes de test et de production, etc)
- Gestion de l'acquisition de services (PLA et SLA avec les fournisseurs) (supervision de ces services)
- Planification des systèmes (gestion des capacités, performances, mise à jour,etc)
- Protection contre les virus
- Les sauvegardes
- La gestion de la sécurité des réseaux
- Protection des média amovibles
- Sécurisation de la documentation
- Sécurisation de l'échange d'information (politique et procédures)
- Sécurisation du transport des médias amovibles
- Gestion de la messagerie électronique
- Les services de commerce électronique
- La supervision (logs, système de logs, etc)

7. Contrôle d'accès

- Gestion des politiques d'accès aux données
- Élaboration des procédure de création des comptes utilisateurs et d'attribution des droits d'accès
- Gestion des mots de passe
- Contrôle de l'accès aux ressources réseaux et à l'utilisation de ces ressources
- Contrôle d'accès des utilisateurs externes à l'entreprise
- Gestion des rôles pour l'accès à l'information
- Filtrage du trafic réseau
- Contrôle d'accès aux systèmes d'exploitation
- Identification / authentification des utilisateurs (ID unique)

8. Acquisition des systèmes d'info, développement et maintenance

Analyse des besoins de sécurité

Traitement des données : Validation des données d'entrée, intégrité des messages, validation des données en sortie

Politique d'utilisation des contrôles de cryptographie

Sécurité des systèmes de fichier

Gestion de la sécurité du développement externalisé

Gestion des vulnérabilités.

9. Gestion des incidents de sécurité

Assurer que les événements de sécurité et les faiblesses liées aux systèmes d'information sont communiquées de manière à permettre des mesures correctives dans les meilleurs délais.

Exemple d'incidents : arrêt d'un service, erreur humaine, non-conformité aux lois, mal-fonctionnement d'un système, Accès non autorisé, etc.

- Signaler les événements de sécurité
- Gérer les événements de sécurité (les responsabilités et les procédures, Collecte de preuves, Lessons acquises suite à des incidents, etc.)

10. Gestion de la continuité

Contrer les interruptions des activités et processus métier, protéger le système d'information ou de catastrophes et assurer la reprise.

- Élaboration du plan de continuité d'activité (PCA) en fonction des besoins métier.
- Élaborer une étude de gestion des risques
- Implémenter le PCA et le tester (les procédures devront être cohérentes et répondent aux besoins)

11. Conformité

Se conformer aux lois et aux obligations légales.

- Identifier les lois applicables au contexte de l'entreprise
- Se conformer aux droits de propriété intellectuelle
- Protection des données organisationnels
- Protection des données privées
- Conformité avec les politiques et les normes de sécurité

IV 3- Conclusion

La sécurité de l'information n'est pas la responsabilité des Techs uniquement mais la responsabilité de tout le personnel de l'AuF

Afin de protéger l'information, il ne suffit pas de prendre en compte la dimension technique mais organisationnelle aussi.

Plusieurs standards de gestion de la sécurité existent de nos jours ... il est important de les connaître et de les adapter au contexte de l'AuF