David BIGOT

Julien VEHENT

Etude du cas “ASSURAL”

Mise en conformité du système d'information avec la norme ISO 17799

Master Management de la Sécurité des Systèmes Industriels et des Systèmes d'Information

IRIAF, Université de Poitiers

Octobre 2006

I) Rédaction des préconisations

I.1) Préconisations liées au rapport d'audit

Thèmes	*Problèmes*	*Préconisations*
Thème 1 : Politique de sécurité	Pas de PSSI	Rédiger une PSSI dans le cadre de la création d'un ISMS
Thème 2 : Organisation de la sécurité de l'information	Situation du RSSI dans la hiérarchie (séparation MOA/MOE)	Le RSSI doit être directement rattaché à la Direction Générale (RSSI et DG sont la MOA)
|	Les administrateurs jouent le rôle d'administrateurs de la sécurité	Créer un poste “Responsable Sécurité Informatique”, rattaché au RSSI, qui aura la charge de l'administration de la sécurité informatique
|	Absence de définition précise des responsabilités	Définition des responsabilités du personnel par des procédures formalisées
|	Processus d'approbation de la DG sur l'évolution du SI est défaillant	Revoir le processus de validation MOA -> MOE
|	Absence de fondamentaux en matière de gestion de la sécurité du système d'information (audits, tableau de bord, cellule de crise, ...)	La mise en place d'un ISMS est indispensable
Thème 3 : Gestion des actifs	Les rôles de propriétaires ne sont pas définis	Définir les règles administratives et juridiques liés à la propriété de l'information au travers de la PSSI
|	Evaluation empirique de la criticité de l'information	Etablir une classification avec le concours des propriétaires, réaliser une analyse des risques pour affiner les procédures de traitement de l'information
Thème 4 : Sécurité liée aux ressources humaines	Absence de contrôles à l'embauche pour les postes sensibles	Procédure de vérification des diplômes et du casier judiciaire
|	Défault d'implication des utilisateurs dans le processus sécurité	Réalisation des actions de sensibilisation pour responsabiliser les utilisateurs
|	Pas de contrôle régulier des habilitations	Faire démarrer le Workflow depuis la DRH et réaliser un audit des habilitations deux fois par an
Thème 5 : Sécurité physique et environnementale	La politique de contrôle d'accès par badge est inefficace	Sensibiliser le personnel à l'accès aux locaux (ne pas laisser entrer de personnes non munis de badges)

	Faille dans le système de livraison	Mettre en place un sas de déchargement
Thème 6 : Gestion des télécommunications et de l'exploitation	Absence de contrôles indépendants des processus d'exploitation et de maintenance	Réaliser régulièrement des audits internes
	Gestion défaillante de la sécurité des systèmes	Procédurer, avec une définition des responsabilités, la gestion de la sécurité
	Pas, ou peu, d'analyse des fichiers journaux	Mettre en place un système de gestion des journaux en temps réel
Thème 7 : Contrôle des accès logiques	Pas de séparation des pouvoirs	Etablir une matrice des droits prenant en compte les incompatibilités de pouvoirs
	Pas de contrôle de l'utilisation des privilèges	(voir thème 4) Audit bi-annuel et gestion des habilitations par la DRH
	Absence de bonnes pratiques pour le rangement des données	Mettre en place une politique de “bureau propre, écran vide”
Thème 8 : Acquisition, développement et maintenance des SI	Les développeurs ont accès aux environnements de production	(voir thème 7) Etablir une matrice des droits prenant en compte les incompatibilités
	Jeux de test basés sur des données de production	Les jeux de tests doivent être établis à partir de données à blanc pour interdire toute fuite d'information
	Pas de centralisation de la gestion des vulnérabilités, pas de veille technologique	Centraliser la gestion des mises à jour (information, déploiement) au travers d'un outil dédié
Thème 10 : Gestion de la continuité d'activité	La continuité d'activité est limitée à des procédures techniques concernant les systèmes serveurs	Mettre en place un PCA et un PRA prenant en compte l'ensemble du système d'information (utilisateurs, ressources, données, etc...)
Thème 11 : Conformité	Aucun audit	Réaliser régulièrement des audits du système d'information, établir un suivi de ces audits dans le temps

I.2) Organisation des préconisations

Pour faciliter la mise en place des préconisations précédemment identifiées, nous pouvons regrouper ces dernières sous forme de projets. Ces projets seront organisés selon une échelle de priorités évolutive dans le temps. Ceux-ci seront plannifiés sur plusieurs années (4 à 5 ans).

Constitution des projets :

1. Cartographie des processus : afin d'effectuer une analyse des risques, il faut établir une cartographie des processus du système d'information de l'entreprise.

2. Analyse de risques : utiliser les résultats globaux de l'audit sécurité pour cibler l'analyse de risque sur les points suivants : gestion des accès (logiques/physiques); classification; continuité d'activité; implication des utilisateurs; fuite d'informations. L'analyse de risque permet de connaître l'impact financier lié à la perte ou le dysfonctionnement d'un processus.

3. Définition du ISMS sur la base des résultats de l'analyse de risques avec pour périmètre la compagnie ASSURAL. On peut détailler ce projet en plusieurs sous projets :

3.1 Modification de la position du RSSI dans la hiérarchie. Création de la fonction de responsable sécurité informatique (RSI).

3.2 Rédaction de la PSSI : Définir les règles et objectifs sécurité, les projets à mener et les responsabilités des différentes entités sur ces projets.
Identification et définition des indicateurs.
Intégration des prestataires.

3.3 Attribution des moyens : en accord avec l'analyse de risques, le coût de mise en oeuvre d'un processus (et des procédés visant à le sécuriser) ne doit pas excéder l'impact financier des risques qu'il est amenés à subir. On chiffera également les frais nécessaire à la mise en place du ISMS, incluant la maîtrise des indicateurs.

3.4 Validation de la PSSI et des moyens relatifs par la Direction Générale.

4. Mise en place du ISMS : cette partie comprend la mise en place d'un certain nombre de sous-projets visant à appliquer la PSSI dans le cadre de l'entreprise.

4.1 Responsabilité du personnel : les responsabilités collectives concernant la sécurité du système d'information sont consignées dans une charte Sécurité et les responsabilités individuelles dans le contrat de travail. Dans la même optique, on réalisera des sensibilisation et formations des employés.

4.2 Classification et rôles des propriétaires : les résultats obtenus permettent d'affiner le processus de sauvegarde.

4.3 Audits et contrôles internes : ces actions permettent de surveiller le bon fonctionnement du ISMS et d'identifier les actions à corriger dans une logique de PDCA. On retrouvera les points suivants : Attribution des droits, processus d'exploitation, contrôle à l'embauche

4.4 Matrices des habilitations et des responsabilités : définit également les incompatiblités de pouvoir

4.5 Formalisation du Tableau de Bord Sécurité : mesures techniques de production des indicateurs de premier niveau, synthétisation et compression des indicateurs pour les niveaux 2 et 3.

5. Projets Sécurité :

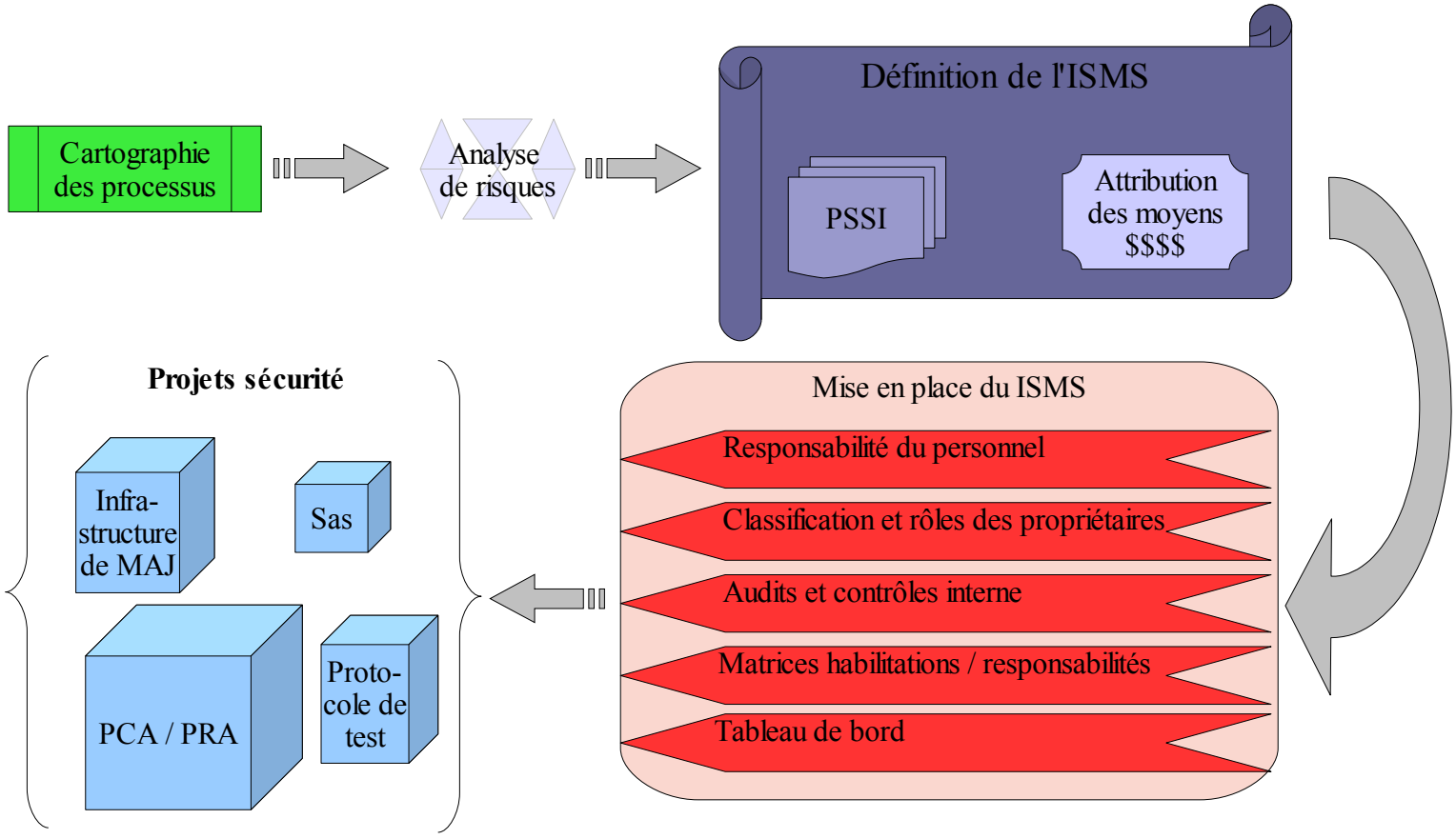
5.1 Sécurisation des accès de livraison

5.2 Etablir un protocole de test et de montée en charge des applications

5.3 Infrastructure de gestion des mises à jour

5.4 Plan de continuité d'activité et plan de reprise d'activité

Les différentes phases vues ci-dessus peuvent être schématisée :

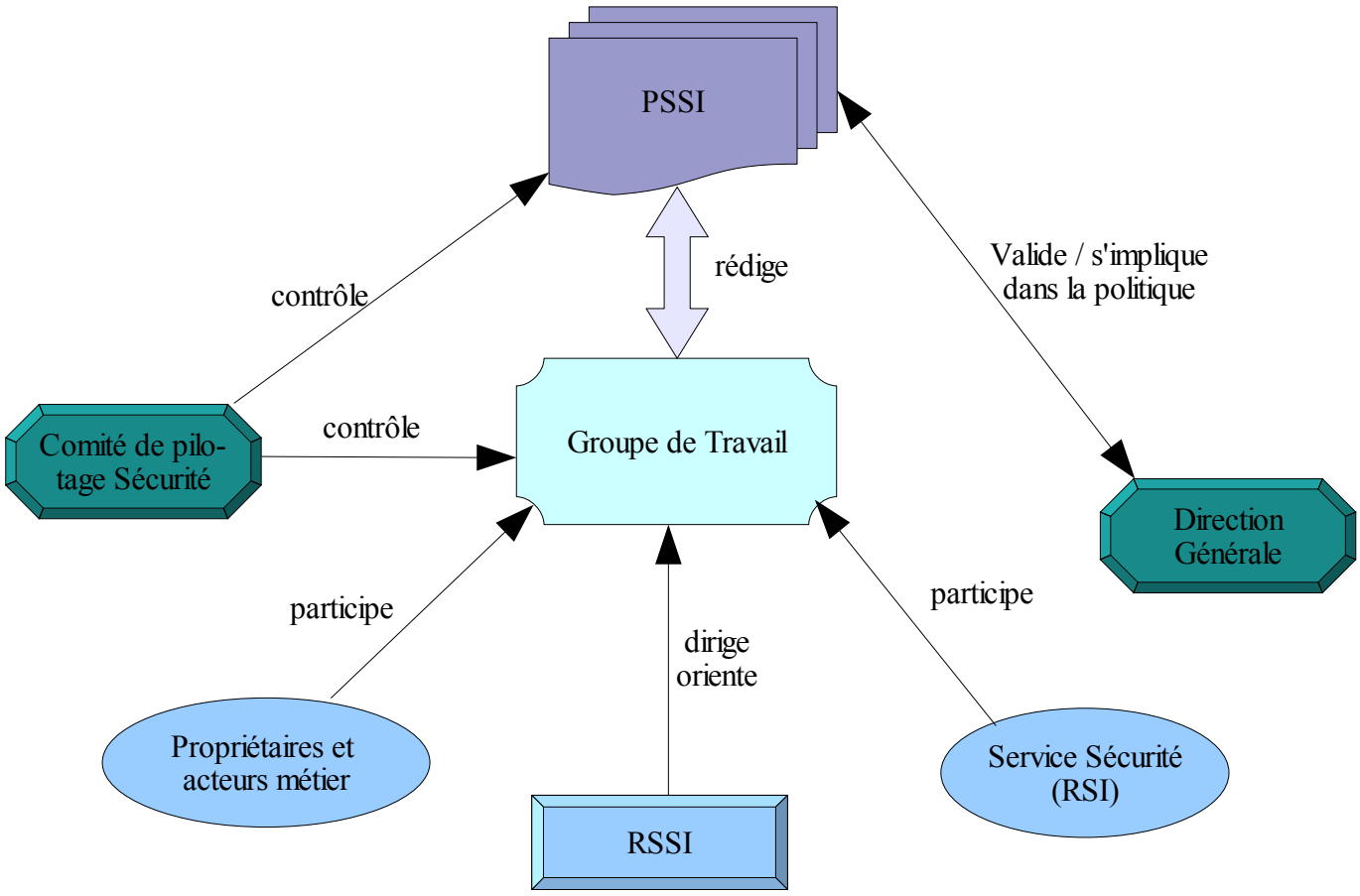


II) Elaboration de la politique de sécurité de l'information

II.1) Méthode de travail

La politique de la sécurité du système d'information permet de définir la stratégie Sécurité de l'entreprise et de présenter les actions qui seront à mener. Ce document nécessite la participation du responsable de la sécurité du système d'information et de toutes les personnes qui seront acteurs de cette politique.

On peut identifier un certain nombre d'acteurs en charge de la rédaction de la politique de Sécurité.



Le RSSI prend la direction du groupe de travail qui rédige la PSSI. Ce dernier est une structure temporaire créé pour la rédaction de la PSSI.

Afin d'assurer un maximum de cohérence avec le métier de l'entreprise, le rôle joué par le groupe “Propriétaires et acteurs métier” est primordial. Ce dernier apporte une vision pragmatique permettant à la PSSI de se détacher d'un modèle potentiellement théorique est inapplicable.

Les aspects techniques sont apportés par le RSI (et éventuellement son équipe).

Le Comité de pilotage Sécurité a un rôle de relecture et de validation de premier niveau. Il peut, si la structure le permet, participer à la rédaction du document final et est, dans tous les cas, impliqué dans les discussions.

Enfin, la Direction Générale a la charge de la validation de la PSSI et en particulier de l'attribution des moyens qui l'accompagne.