L'appui de l'ANSSI

Sept recommandations pour bien transposer une PSSI

http://www.ssi.gouv.fr
http://www.certa.ssi.gouv.fr
http://www.securite-informatique.gouv.fr

David CROCHEMORE
Mercredi 28 novembre 2012

TRANSPOSER UNE PSSI

Disposer d'un guide n'interdit pas de réfléchir :

1. Le périmètre et le contexte
2. Les biens essentiels
3. La gouvernance SSI
4. Les processus et les règles SSI
5. La communication SSI
6. Les responsabilités
7. L'hygiène informatique

1 – LE PERIMETRE ET LE CONTEXTE

Les périmètres sont tous différents !

Les contextes sont tous particuliers !

- Contraintes géographiques ;
- Nombre de sites ;
- Réglementation PPST ;
- Echanges internationaux ;
- Echanges avec l'industrie ;
- Tout référentiel réglementaire particulier ;
- Niveau actuel de maturité ;
- Etc..

2 – LES BIENS ESSENTIELS

La définition des biens essentiels est l'une des étapes-clés de l'analyse de risque :

- Ne pas confondre « Biens essentiels » et « Biens support » ;
  - Les **biens essentiels** sont immatériels (informations ou processus) ;
  - Les **biens supports** sont les biens matériels sur lesquels reposent des biens essentiels ;
- Ce sont les *métiers* qui connaissent les biens essentiels ;
- Mais il est nécessaire d'harmoniser les perceptions sur le caractère sensible des biens essentiels ;
- Certains biens essentiels ne sont pas connus, ni pris en charge par la DSI.

3 – LA GOUVERNANCE SSI

Elle doit être intégrée au maximum au sein des structures de gouvernance existantes :

- La gouvernance SSI ne doit pas être considérée comme une affaire de spécialistes ;
- Lorsque c'est possible, il est souvent préférable de s'appuyer sur les structures de gouvernance SI existantes ;
- La pérennité de l'organisation que vous mettez en place en dépend (les commissions doivent se réunir régulièrement pour être utiles) ;
- Le niveau de représentation dans les instances de gouvernance SSI doit être suffisant pour **prendre des décisions**.

4 – LES PROCESSUS ET LES REGLES SSI

Les processus SSI doivent être intégrés dans l'existant :

- La SSI doit être totalement intégrée au cycle de vie des systèmes d'information (étude, développement, déploiement, exploitation, maintien en condition de sécurité, fin de vie…)
- La SSI n'est pas au-dessus, pas en-dessous, pas à côté : elle est à l'intérieur ;
- Charte informatique - Règlement intérieur ;
- Formation SSI *dans les formations métier* / Sensibilisation des agents *dans leur contexte.*

Les règles SSI doivent être appliquées :

- Elles doivent donc être applicables (notion de « juste nécessaire ») ;
- Les règles doivent s'imposer aux prestataires !

5 – LA COMMUNICATION SSI

Le vocabulaire doit être adapté aux interlocuteurs

- Avec les métiers, parlez *métier :*
  - Scénarios de risque métier ;
  - Impact sur les missions rendues grâce au SI.
- Avec les responsables, parlez *responsabilité* :
  - Aller à l'essentiel ;
  - Macro-risques : impacts sur l'image et sur les finances et sur la responsabilité pénale.
- Avec les informaticiens, parlez *informatique* :
  - Pour l'intégration de la SSI dans les procédures informatiques ;
  - Pour l'utilisation d'outils de sécurité dans les systèmes.
- Avec les utilisateurs, parlez simplement.

6 – LES RESPONSABILITES

Les responsabilités des différents acteurs doivent être claires et explicites

- Responsabilités locales vs responsabilités nationales ;
- Les délégations doivent être formalisées ;
- Le référent SSI doit avoir des tâches connues et des moyens adaptés ;
- Pour chaque mesure de sécurité de la PSSI, un responsable du respect de son application doit être explicitement désigné ;
- On doit savoir qui a la légitimité pour organiser des audits ;

Toutes ces questions sont d'autant plus importantes en cas de tutelles multiples !

7- L'HYGIENE INFORMATIQUE

Un socle technique commun à tous les établissements

- 40 règles issues des constatations quotidiennes du COSSI ;
- Version 0.1 disponible sur http://www.ssi.gouv.fr
- 13 rubriques :
  - Connaître précisément le système d'information et ses utilisateurs
  - Maîtriser le réseau
  - Mettre à niveau les logiciels
  - Authentification et mots de passe
  - Sécuriser les équipements terminaux
  - Segmenter le réseau et contrôler l'annuaire
  - Protéger le réseau interne de l'Internet
  - Surveiller les systèmes
  - Sécuriser les postes des administrateurs
  - Contrôler l'accès aux locaux et sécurité physique
  - Organiser la réaction en cas d'incident
  - Sensibiliser
  - Faire auditer la sécurité