Le pilotage de la SSI

Indicateurs, Tableaux de bord

Gouvernance de la SSI

- **S'assurer que la réalité du terrain est conforme aux enjeux, à la stratégie définie.**
- **Suppose une politique de sécurité avec un plan directeur et des projets de mise en œuvre.**
  - **Etude CLUSIF 2005 : 56 % ont une PSI**
- ***Mesure l'efficacité de la politique de sécurité***

Mais on ne pilote que ce que l'on mesure →

Les indicateurs

- Doivent être clairement définis ainsi que les objectifs auxquels il se rattachent.
  - Fiables.
  - Représentatifs.
  - Quantifiés (binaire du type oui /non, %, nombre).
  - Datés avec une période de validité et un processus de mise à jour.
  - Un propriétaire.
  - Le mode de présentation doit être défini ainsi que les modalités de diffusion.
  - Compréhensible, adapté à son destinataire (Technique, Métier).
  - Documenté, reproductible avec un processus de mise à jour.

Exemples →

Sécurité organisationnelle

- Nombre de risques couverts parmi les risques choisis par la direction.
- Nombre de participants aux comités sécurité
- Nombre de police d'assurance.
- Nombre de contrats commerciaux incluant un clause sécurité / nombre total de contrats.
- Nombre de documents classifiés confidentiels.
- Nombre de « fils rouges » sur la sécurité dans l'année.
- Nombre d'audit / année.
- Nombre d'exercices d'évacuation / période

Protection des locaux, des sites

- Nombre de détecteurs d'incendie par local / surface.
- Nombre de détecteurs d'humidité / surface.
- Taux de disponibilité de l'électricité de la climatisation.
- Nombre de badges perdus.
- Nombres d'effractions / période.
- Nombre de personnes externes ayant accès aux bureaux

Sécurité des réseaux, des systèmes

- Taux de disponibilité du réseau.
- Nombre de refus d'accès.
- Nombre d'intrusions détectées.
- Nombre d'accès supprimés / nombre de personnes parties.
- Nombre de personnes habilités à donner des autorisations.
- Nombre des machines protégées contre les Virus / nombre des machines installées.
- Nombre de patchs appliqués / nombre de patchs publiés.
- Nombre de mise à jour des tables de flux du pare-feu.
- Date de dernière mise à jour du câblage.
- Nombre de modification de configuration / équipement

Sécurité applicative

- Nombre des projets informatiques ayant inclus la sécurité dès la conception / nombre total de projet
- Nombre des applications avec un contrôle d'accès / nombre total des applications.
- Nombre moyen de « profile » ou « rôle » dans les applications.
- Nombre de refus d'accès applicatifs.

Sécurité de la production

- Nombre de sauvegardes testées / nombre sauvegardes total.
- Nombre de test de PRA par an.
- Nombre de mises à jour du PRA.

Projets

- Certification ISO 17799 Nombre d'objectifs atteints / 39 objectifs de la norme
- Nombre de machines Windows protégées contre les virus / nombre de machines total.
- Nombre d'étapes achevée du plan de secours / nombre total d'étapes.

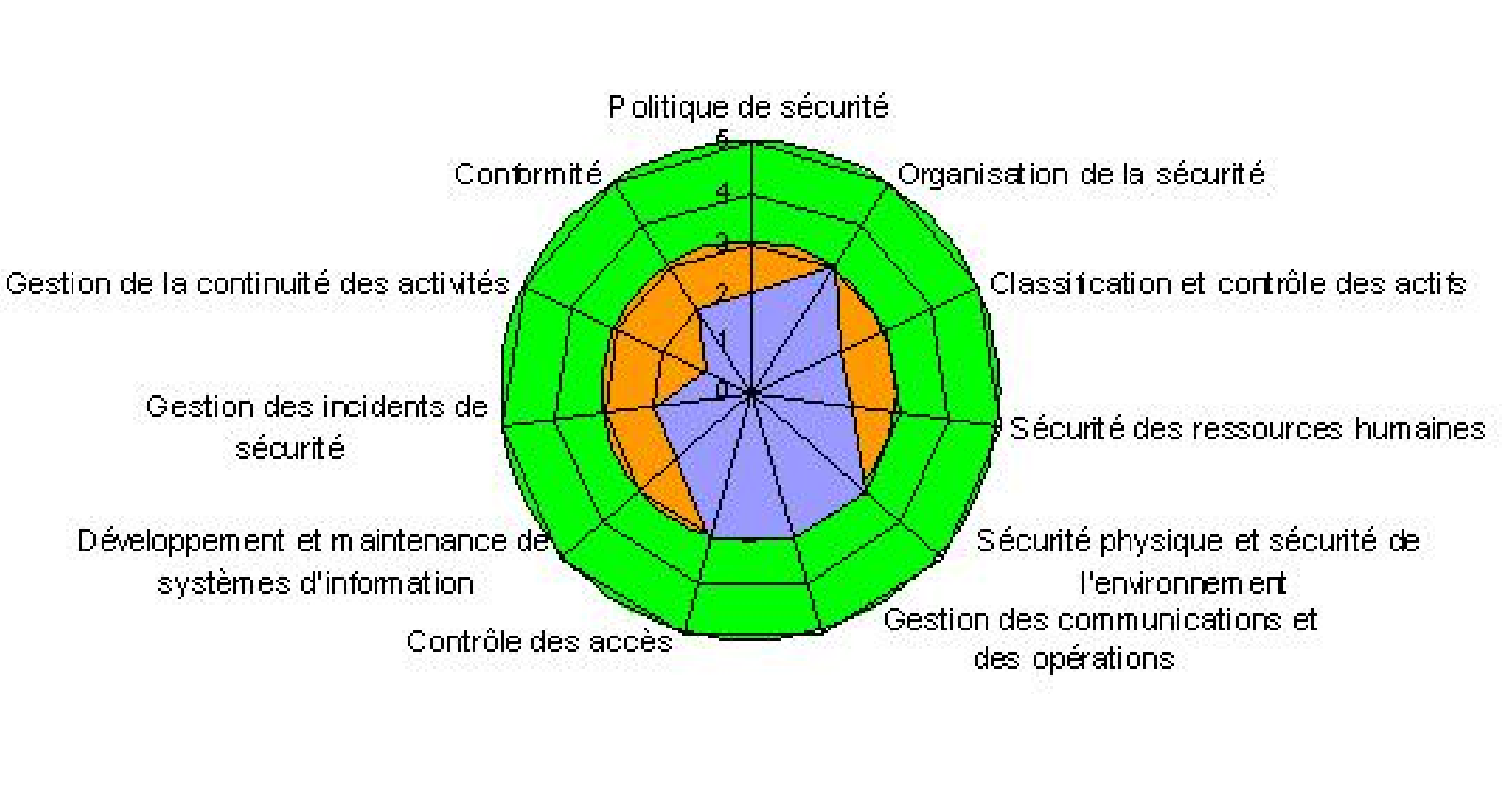
Le tableau de bord

- Outil de visualisation, de synthèse, de mise en valeur des indicateurs, il doit être court et lisible.
- Indicateur composite.
- Adapté sur le fond et la forme à ceux qui doivent les lire.
- Montre l'écart entre le niveau de sécurité attendu et celui réellement en place.
- Montre la progression des plan d'action.
- Justifie les budgets
- Il permet de faire prendre des décisions sur des faits concrets.

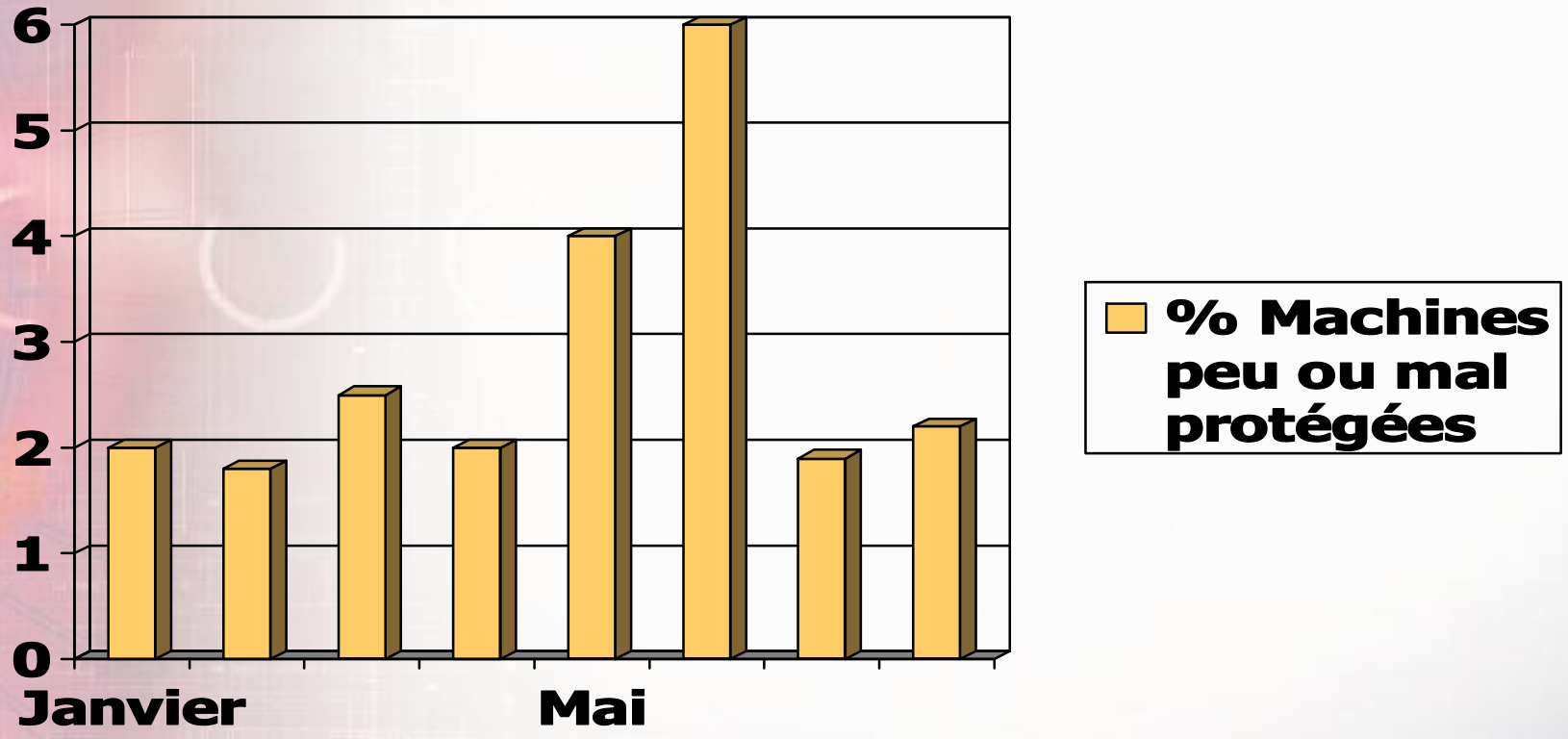
- *Assure le lien avec les enjeux métiers*

- → *Construire un TDB est un véritable projet*

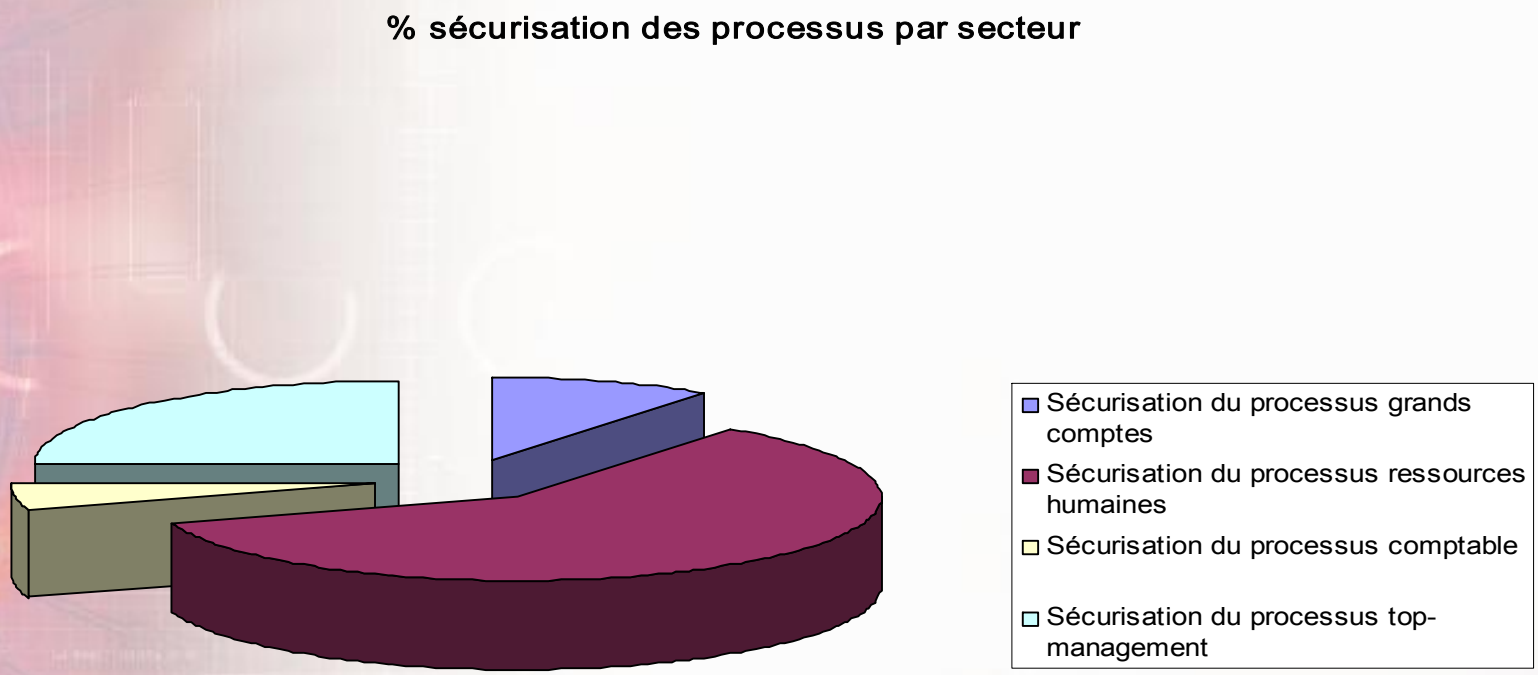
Exemple d'élément de tableau de bord (ISO 2700X)



Exemple d'élément de tableau de bord
Politique anti-virale : taux de machines non protégées



Exemple d'élément de tableau de bord
Approche par processus sensibles



Conclusion

- Un pilotage de qualité donne à la SSI la crédibilité nécessaire de la direction générale.

- Associé à un bonne connaissance des risques de l'entreprise, il permet d'assurer la pérennité de la politique de sécurité et d'éviter un effet de type « balancier ».