CLUB DE LA SECURITE DE L'INFORMATION FRANCAIS

CLUSIF

Conformité ou maîtrise des risques

Un choix nécessaire ?

La question du choix se pose-t-elle ?

- Quel choix ?
- Quelles conséquences en attendre ?
- Quels acteurs et quel pilotage implique-t-il ?
- Quelles sont les cibles visées ?
- Quelles conclusions tirer de tout cela ?

Le choix d'une politique

- Conformité à un référentiel :
  - ISO 27001 pour la mise en place d'un SMSI
  - Un cadre plus restreint tel que la sécurité des informations « privées »
  - Un référentiel métier (bancaire, santé, etc.)
- La maîtrise des risques :
  - Identifier **tous** les risques
  - Évaluer chaque risque
  - Sélectionner un plan de traitement adapté à chaque risque

Ces politiques peuvent-elles conduire à des solutions différentes ?

- Les choix techniques et les solutions pratiques seront identiques à 80 %
  - Référentiels basés sur des bonnes pratiques couvrant les risques les plus courants
  - Consensus de la profession
- Les risques spécifiques peuvent être ignorés en l'absence de méthode dédiée à la gestion des risques
  - Cas particuliers non retenus dans un compromis normatif
  - Cycle de vie et échelle de temps du contexte normatif
- Les traitements « métier » seront plus facilement identifiés et sélectionnés par une gestion de risques

Quels acteurs et quel mode de pilotage ?

- La politique de conformité :
  - Exige du commanditaire l'allocation de ressources et le plein support de la démarche
  - Fait reposer l'essentiel des actions sur la fonction sécurité (RSSI et DSI)
- La gestion des risques :
  - Exige de la Direction de l'organisme une totale implication dans le pilotage des risques
  - Ne fait appel à la fonction sécurité que pour des « éclairages » techniques (vulnérabilités, menaces, techniques d'évaluation, etc.)

Quelles cibles visent ces politiques ?

- La politique de conformité :
  - Vise à propager une image et à donner confiance
  - S'adresse aux clients et partenaires
  - Offre une ligne de défense (à la Direction) en cas d'incident de sécurité
- La gestion des risques :
  - Vise à anticiper et à maîtriser les risques
  - Est un outil de pilotage pour la Direction
  - Permet à la Direction d'anticiper la gestion de situations de crise, en cas d'incident de sécurité

Quelles conclusions ?

- Les 2 politiques de conformité et de maîtrise des risques sont bien différenciées et un choix est donc possible, voire nécessaire

- Elles sont aussi compatibles et la Direction peut choisir de suivre les deux, simultanément

- Il faut, dans ce cas, s'appuyer sur une méthode de gestion des risques, telle que Méhari

Merci de votre attention