Gestion des risques et solution EGERIE RiskManager

Séminaire Confiance Numérique – Clermont-Ferrand
Jeudi 04.02.2016

Mathieu Charbois, Consultant Cyber-Sécurité
Responsable de l'agence FIDENS Auvergne / Rhône-Alpes / Suisse

Ordre du jour

- Présentation de FIDENS
- Gestion des risques : rappel des notions
- Pourquoi outiller la gestion des risques
- Solution EGERIE RiskManager

FIDENS : un positionnement clair

Cabinet de Conseil Opérationnel

- Spécialisé dans la Sécurité des Systèmes d'Information
- Une démarche ancrée sur les standards du domaine
- Maîtrise méthodologique et savoir faire technologique
- Expérience probante, riche de projets majeurs (1500 études)
- Une expertise reconnue dans les grands comptes privés et publics

Implication forte dans les Groupes de Travail

- Travaux de l'AFNOR – ISO 2700x, Club 27001, Club EBIOS, le RGS, CLUSIF Santé

Les métiers de FIDENS

- **Conseil**: de l'analyse stratégique au conseil opérationnel
- **Audit**: maitrise méthodologique et savoir-faire technologique
- **Formation**: Formations certifiantes, Transfert de compétences et retours d'expérience, Centre de formation agréé n°11 95 04268 95

Gestion des risques : rappel

- Définition (ISO/CEI 31000:2009 – Management du risque — Principes et lignes directrices) :
  - Discipline qui s'attache à identifier, évaluer et prioriser les risques relatifs aux activités d'une organisation, quelles que soient la nature ou l'origine de ces risques, pour les traiter méthodiquement de manière coordonnée et économique, de manière à réduire et contrôler la probabilité des événements redoutés, et réduire l'impact éventuel de ces événements

- Norme Internationale ISO/CEI 27005:2011 : Gestion des risques liés à la sécurité de l'information
  - Guide de mise en œuvre de l'appréciation des risques de la sécurité de l'information décrite dans l'ISO 27001
  - Processus de gestion du risque en sécurité de l'information

Gestion des risques : Démarche

- Démarche ISO/CEI 27005:
  - Etablir le contexte
    - Métriques
  - Identification du risque
    - Actifs, menaces, mesures de sécurité
  - Estimation du risque
    - Conséquences, vraisemblance des menaces
  - Evaluation du risque
    - Cartographie des risques
  - Traitement du risque
    - Choix de traitement
  - Acceptation du risque
    - Validation des risques

Gestion des risques au sein de ISO 27001

- La gestion des risques est la première étape de tout système de management de la sécurité de l'information (ISO/CEI 27001):
  - Clause 6.1.2 (ISO/CEI 27001) : L'organisation doit définir et appliquer un processus d'appréciation des risques de sécurité de l'information
  - Clause 6.1.3 (ISO/CEI 27001) : L'organisation doit définir et appliquer un processus de traitement des risques de sécurité de l'information

- A la suite de cette gestion des risques, un plan d'actions des mesures de sécurité pourront être mis en œuvre afin d'initier l'implémentation du SMSI 27001

Pourquoi outiller la gestion des risques ?

- Faciliter le pilotage de la gestion des risques dans la durée
- Faciliter l'arbitrage et la prise de décision en donnant aux donneurs d'ordre, une vision précise, compréhensible, normalisée et actualisée de la cartographie des risques et des moyens de protection
- Faciliter l'obtention et la maitrise des budgets en garantissant et en justifiant un niveau de protection et de couverture des risques
- Faciliter la responsabilisation et le contrôle des plan d'actions sur les acteurs du SI

EGERIE RiskManager

- Solution web de gestion des risques de sécurité de l'information
- Editeur : EGERIE-SOFTWARE, filiale éditrice du groupe FIDENS

MERCI

Didier SAVALLE

Responsable commercial

Agence FIDENS Auvergne / Rhône-Alpes / Suisse

50, rue de la République – 69002 Lyon

didier.savalle@fidens.fr

Mob : + 33 (6) 84 76 42 92