

ISMS-PME : développement d'un outil de gestion des risques pour les PME conforme à l'ISO/IEC 27005

Nicolas Mayer – Product Manager Security & Continuity Management
<http://www.nmayer.eu>

- **Un centre de recherche public**
 - Recherche court / moyen terme
 - Financement privé / public
- **5 départements**
 - Santé
 - Environnement
 - Centre de veille technologique
 - Technologies industrielles et matériaux
 - **Service Science and Innovation**

➤ **Management de la sécurité**

- Risk management
- Security standards
- Security assessment / Security metrics
- Security modeling

➤ **Confiance numérique**

- Trust
- Records management
- PKI management
- Business Continuity

➤ **Monitoring d'architectures IT**

- Préparation à la certification ISO/IEC 27001
 - Préparation en grappe pour les PME
 - Accompagnement individuel

- Outils de management de la sécurité
 - **Gestion des risques**
 - Gap analysis ISO/IEC 27001
 - Micro-éval
 - Aide à l'établissement d'une PSSI

- BCP
- Archivage numérique

- **Projet de recherche ISMS-PME**
 - Ministère de l'Économie et du Commerce extérieur du Luxembourg

- **Orienté vers les TPE/PME**
 - Points faibles / ISO/IEC 27001
 - Moins de ressources
 - Moins de compétences
 - Points forts / ISO/IEC 27001
 - Plus flexibles
 - Plus réactifs

- **Résultats attendus**
 - Réalisation d'un guide d'implémentation adapté aux PME
 - Réalisation de templates et **outils supports à la démarche**

Outil de gestion des risques ISO/IEC 27005

- But de l'outil d'appréciation des risques basé sur l'ISO/IEC 27005
 - Faciliter et accélérer la réalisation d'une appréciation des risques spécialement pour des entreprises de type PME

- Pour qui?
 - L'outil se destine :
 - Aux consultants pour réaliser une appréciation des risques
 - Aux RSSI en interne pour réaliser son appréciation des risques

Couverture des exigences de l'ISO/IEC 27001

- L'outil répond aux besoins des points suivants de l'ISO/IEC 27001
 - 4.2.1 c) définir l'approche d'appréciation du risque
 - 4.2.1 d) identifier les risques
 - 4.2.1 e) analyser et évaluer les risques
 - 4.2.1 f) identifier et évaluer les choix de traitement des risques
 - 4.2.1 g) sélectionner les objectifs de sécurité et les mesures de sécurité proprement dites pour le traitement des risques.
 - 4.2.1 j) préparer une Déclaration d'Applicabilité
 - 4.2.2 a) élaborer un plan de traitement du risque

L'outil et les lignes directrices de l'ISO/IEC 27005

- L'outil permet de réaliser les points suivants :
 - Établissement du contexte
 - Définir les critères de base
 - Critères d'impact
 - Critère de vraisemblance du risque
 - Critère d'évaluation du risque
 - Critère d'acceptation du risque
 - Appréciation du risque
 - Identification des assets
 - Estimation des assets par impact
 - Identification et estimation des menaces
 - Identification et estimation des vulnérabilités
 - Identification et estimation des risques
 - Evaluation du risque
 - Traitement du risque
 - Définir le traitement
 - Définir les mesures
 - Peut servir de base pour la communication des risques

➤ Un fichier Excel

- Critères de base
- Inventaire des processus/informations
- Inventaire des ressources SI
- Mapping
- Risques
- Déclaration d'applicabilité (tirée de l'ISO/IEC 27001 annexe A)
- Plan de traitement

- Utilisé dans 4 entreprises
 - Va être utilisé dans le cadre d'un accompagnement en grappe de PME vers la certification ISO/IEC 27001

- Stratégie de transfert de l'outil en cours de définition
 - Modalités
 - Tarif

- Labellisation de consultants sur l'accompagnement ISO/IEC 27001 à l'aide notre approche et de nos outils