

# ISMS-PME

## Guide d'implémentation d'un SMSI pour les petites structures

### **Nicolas Mayer**

Product Manager – Security and Continuity Management  
*nicolas.mayer@tudor.lu*

### **Thierry Valdevit**

Ingénieur R&D  
*thierry.valdevit@tudor.lu*

## *Guide d'implémentation d'un SMSI pour les petites structures*

- Le CRP Henri Tudor
- Objectifs et contexte
- Méthode de recherche
- Expérimentation initiale
- Réalisation du guide
- Conclusions

## *Guide d'implémentation d'un SMSI pour les petites structures*

- Le CRP Henri Tudor
  - Objectifs et contexte
  - Méthode de recherche
  - Expérimentation initiale
  - Réalisation du guide
  - Conclusions

- Un centre de recherche public
  - Recherche court / moyen terme
  - Financement privé / public
- 5 départements
  - Santé
  - Environnement
  - Centre de veille technologique
  - Technologies industrielles
  - Technologies de l'information et de la communication

- Cibles prioritaires
  - Secteur PME
  - Secteur financier
- Nos activités
  - Gestion des risques
  - Standards de sécurité (ISO/IEC 2700x)
  - Ingénierie des exigences et modélisation de la sécurité
  - Formation
  - Confiance numérique
  - Gestion des PKI
  - Archivage numérique
  - BCP
  - Monitoring de la sécurité

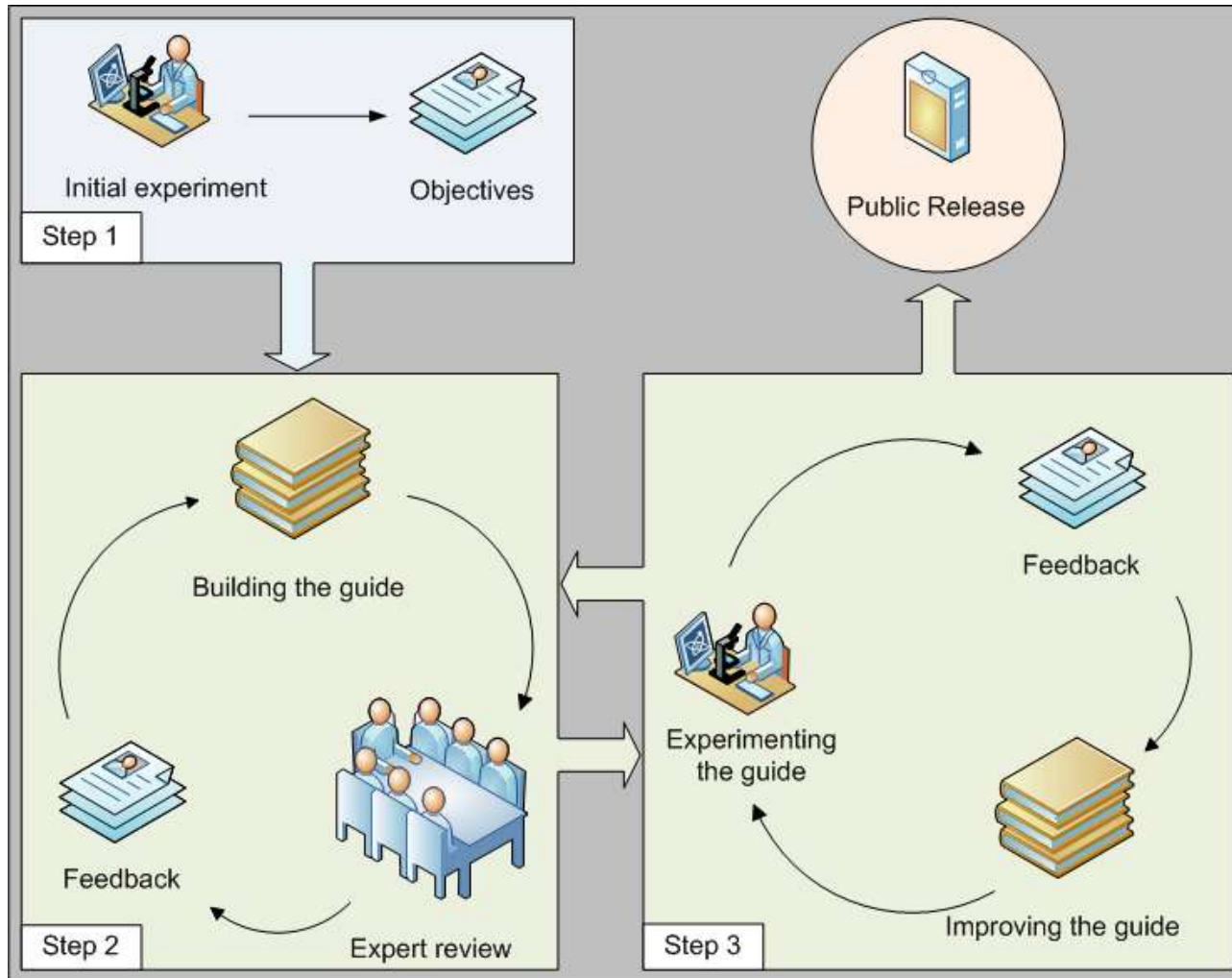
## *Guide d'implémentation d'un SMSI pour les petites structures*

- Le CRP Henri Tudor
- Objectifs et contexte
- Méthode de recherche
- Expérimentation initiale
- Réalisation du guide
- Conclusions

- **Projet de recherche**
  - Ministère de l'Economie et du Commerce extérieur du Luxembourg
- **Orienté vers les TPE/PME**
  - Points faibles
    - Moins de ressources
    - Moins de compétences
  - Points forts
    - Plus flexibles
    - Plus réactifs
- **Objectifs**
  - Réalisation d'un guide d'implémentation adapté aux PME
  - Alléger le temps nécessaire et les coûts pour implémenter un ISMS
  - Rester aligné avec l'ISO/IEC 27001 pour servir d'étape préliminaire dans une optique de certification

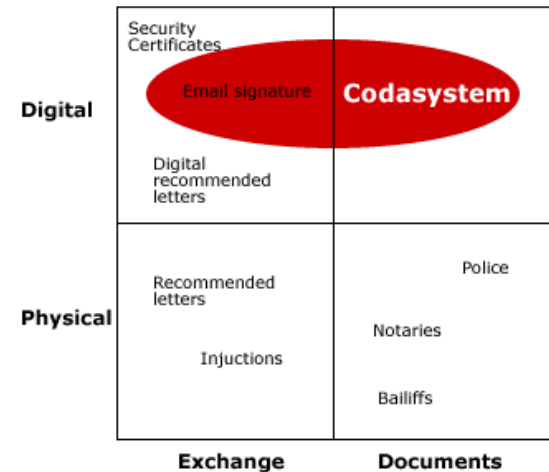
## *Guide d'implémentation d'un SMSI pour les petites structures*

- Le CRP Henri Tudor
- Objectifs et contexte
- Méthode de recherche
  - Expérimentation initiale
  - Réalisation du guide
  - Conclusions



## *Guide d'implémentation d'un SMSI pour les petites structures*

- Le CRP Henri Tudor
- Objectifs et contexte
- Méthode de recherche
- **Expérimentation initiale**
  - Réalisation du guide
  - Conclusions



- Projet pilote
- Entreprise : Codasystem
- Objectifs du CRPHT
  - Maîtrise de la norme ISO/IEC 27001
  - Développement de compétences sur l'implémentation d'un ISMS
- Durée - coût
  - De Juin 2006 à Mai 2008
  - Accompagnement : environ 100 jours/homme
- Résultat : une première entreprise privée certifiée à Luxembourg
  - Capacité d'accompagnement démontrée
  - Ébauche d'outils et de modèles
  - Expérience initiale pour la réalisation d'un guide orienté PME
  - Définition des objectifs du guide

- Appropriation de la norme
  - Difficile et lente
  - Manque de maturité organisationnelle
  - Besoins de formation
- Mise en place
  - Gap important au regard de la norme
  - Pas de procédures formalisées
  - Déploiement du SMSI
- Suivi
  - Amélioration du SMSI
  - Correction des non conformités
  - Accompagnement à l'audit
- Certification
  - Mai 2008

## *Guide d'implémentation d'un SMSI pour les petites structures*

- Le CRP Henri Tudor
- Objectifs et contexte
- Méthode de recherche
- Expérimentation initiale
- Réalisation du guide
- Conclusions

- Objectifs pour le guide
  - Avoir une approche moins abrupte
    - Saisir l'intérêt et les enjeux réels d'un système de management
    - Faciliter la compréhension d'une approche processus
    - Assimiler la logique PDCA
  - Correspondre aux attentes d'une PME
    - Charge réduite, coûts maîtrisés
    - Permettre de faire la première itération en quelques mois
    - Retour sur investissement clair
    - Se concentrer sur les tâches essentielles
  - Faciliter la compréhension
    - Définir en amont les actions et recommandations transversales
    - Simplifier la présentation des différentes étapes
  - Assurer la cohérence et l'efficacité
    - Maintenir un fort alignement avec la norme
    - Certifier par le biais d'experts
    - Fournir un ensemble d'outils et de modèles

- Contenu du guide
  - Réduction des exigences de la norme

	ISMS COMPLETION					
	1	2	3	4	5	
<b>Plan</b>						
<ul style="list-style-type: none"> <li>Sensibiliser la direction avec la législation</li> <li>Définir la portée, les objectifs de l'organisation pour le programme</li> <li>Définir la politique de la sécurité de l'information</li> <li>Identifier et catégoriser les actifs</li> <li>Identifier les menaces et vulnérabilités de l'organisation</li> <li>Évaluer les impacts d'exploitation de chaque vulnérabilité</li> <li>Identifier l'approche à utiliser pour l'analyse de risque</li> <li>Appliquer l'analyse de risque</li> <li>Identifier les mécanismes de contrôle actuellement disponibles</li> <li>Définir une méthode pour traiter les risques et déterminer le niveau de risque acceptable</li> <li>Prendre action face à tous les risques (accepter, transférer, diminuer ou éliminer)</li> <li>Proposer des mécanismes de contrôle supplémentaires</li> </ul>						Management Commitment (Business Case) Risk Register Risk assessment report (including classification and assessment) Mapping Procedures Risk assessment report (procedure details, results) Statement of Applicability (SOP) (scope & risk assessment)
<b>Do</b>						
<ul style="list-style-type: none"> <li>Formuler un plan pour le traitement du risque</li> <li>Implémenter le plan de traitement du risque</li> <li>Écrire les politiques spécifiques en fonction des actions (standards, procédures et recommandations)</li> <li>Définir les rôles et responsabilités</li> <li>Implémenter les mécanismes de contrôle</li> <li>Définir un programme de formation et de sensibilisation</li> <li>Gérer les opérations</li> <li>Gérer les ressources</li> <li>Implémenter les contrôles capables d'activer détection et réponse aux incidents</li> </ul>						Risk treatment plan Policies, guidelines, BCP, etc.
<b>Check</b>						
<ul style="list-style-type: none"> <li>Gérer les incidents (détecter, prévenir et répondre)</li> <li>Surveiller les procédures et les autres contrôles</li> <li>Revisiter le niveau de risque résiduel et le risque acceptable</li> <li>Effectuer des audits internes à des intervalles planifiés</li> <li>Entreprendre une revue de direction du SGSI au moins une fois par année (il s'agit d'un minimum)</li> <li>Valider par la réalisation d'un test d'intrusion interne et externe</li> </ul>						Incident response operations Metrics ISMS audit planning & reports Technical audit planning & reports
<b>Act</b>						
<ul style="list-style-type: none"> <li>Implémenter les améliorations identifiées à la phase précédente dans le SGSI</li> <li>Prendre les actions correctives et préventives appropriées</li> <li>Communiquer les résultats et les actions</li> <li>Assurer que les améliorations atteignent les objectifs visés</li> </ul>						

- Suppression des audits

- Contenu du guide
  - Description des enjeux d'un SMSI
  - Présentation des concepts clefs
    - Approche processus, systèmes de management, logique PDCA
  - Déroulement chronologique des tâches successives
  - Simplification de la présentation
  - Listing des enregistrements clefs en input/output des différentes activités
  - Assignation des acteurs principaux sur les différentes activités

### B. Implement anomaly management process

<b>Details</b>	The efficiency of the ISMS is insured by detection mechanisms, monitoring, records and anomaly correction.
<b>Tasks</b>	Define and apply anomaly management process including the following items: <ol style="list-style-type: none"> <li>1. Identify the anomaly (incident, non conformity, etc.)</li> <li>2. Diagnostic method</li> <li>3. Creation of anomaly ticket (synthetic record containing useful information regarding the anomaly)</li> <li>4. Possible escalation</li> <li>5. Anomaly resolution procedure</li> <li>6. Anomaly enclosing</li> </ol>
<b>Inputs</b>	Enterprise's organisation
<b>Outputs</b>	Anomaly management process Anomaly tickets
<b>Actors</b>	Every level of management ISMS accountable Employees

- Revue d'expert
  - Comité ANSIL/CNLSI
    - Association de Normalisation pour la Société de l'Information du Luxembourg
    - Comité de Normalisation Luxembourgeois pour la Sécurité de l'Information
  - Groupe responsable JTC1/SC27
  - Douzaine d'experts du domaine
  - Mandatés pour revoir le guide
    - 3 itérations
    - 156 commentaires
  - Nouvelle revue mi 2009

## *Guide d'implémentation d'un SMSI pour les petites structures*

- Le CRP Henri Tudor
- Objectifs et contexte
- Méthode de recherche
- Expérimentation initiale
- Réalisation du guide
- Conclusions

## *Conclusion*

- Expérimentation initiale du guide
  - Début 2009
  - Première expérience terrain, premiers retours pratiques
  - Nouvelle revue d'experts
- Expérimentation en grappe
  - 3 entreprises de profils différents
  - Formation groupée
  - Coaching sur site
  - Nouvelle amélioration du guide
- Transfert
  - Guide gratuit
  - Accompagnement proposé au sein du réseau Cassis
  - Framework d'outils (à l'étude)
- Label
  - Support et reconnaissance du Ministère (à l'étude)

***Merci !***