

Securité informatique et PME :

Agir avant que ce ne soit trop tard

Corinne Loesel
Sébastien Pineau

- Corinne Loesel
- Le CRP Henri Tudor
- Le Centre et la Sécurité en PME
- Un label et un réseau pour du conseil de qualité
- Les services de sécurité de l'information à développer
- Le projet Cassis Sécurité 2

- Sébastien Pineau
- L'initiative ISMS-PME

- Appel à intérêt

- CRP Henri Tudor (1987) : contribue à l'amélioration et au renforcement de la capacité d'innovation des entreprises et des organisations publiques

- Effectifs fin 2008 : 346
- Produits 2008 : 32,28 M€
- Budget 2009 : 35,1 M€
- Services et Activités :
 - Recherche appliquée et expérimentale
 - Recherche doctorale
 - Développement d'outils, méthodes, labels, certifications et normes
 - Assistance technologique, conseil et services de veille
 - Transfert de savoir et pré-incubation d'entreprises
 - Formation et qualification de haut niveau
- Projets de recherche : 132 / Partenaires : 319

Domaines scientifiques et technologiques :



Technologies de l'information et de la communication



Technologies des matériaux



Organisation et gestion des entreprises

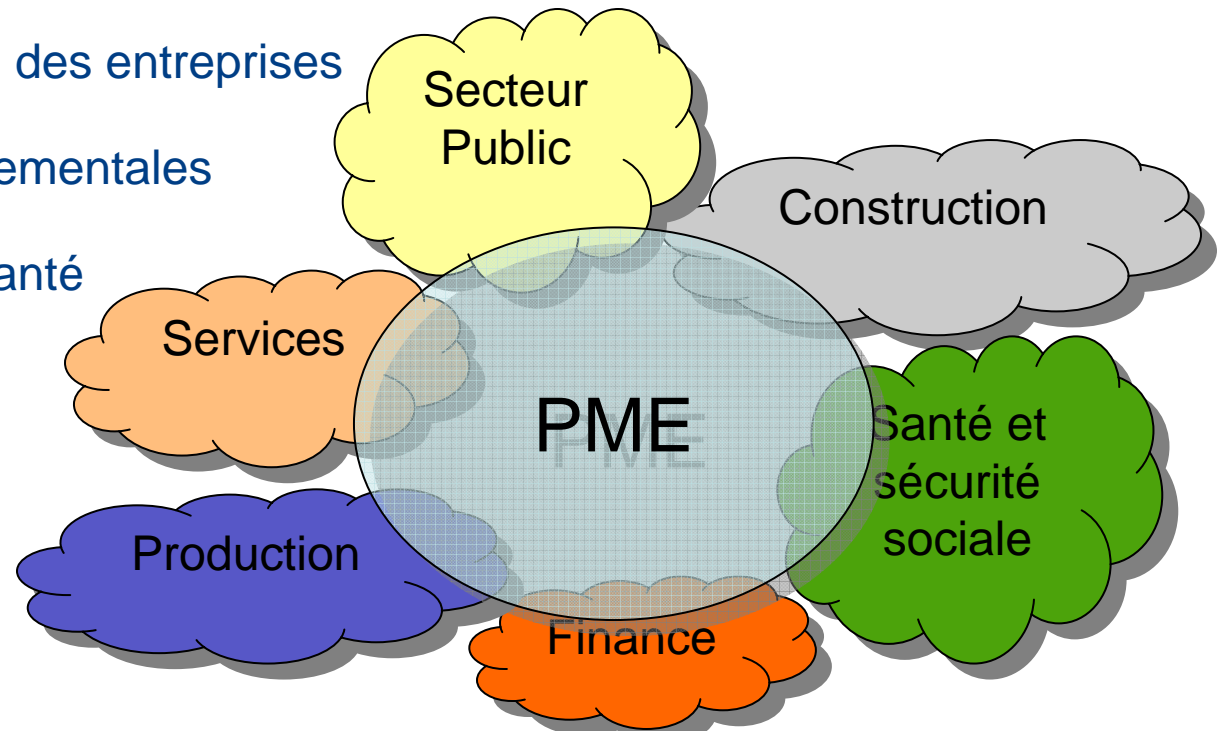


Technologies environnementales



Technologies pour la santé

Secteurs ciblés :



Une attention particulière est accordée aux PME

Petites et Moyennes Entreprises

Monitoring de la sécurité

Continuité d'activité



Archivage numérique

Gestion des PKI

Confiance numérique

Formation



Ingénierie des exigences et modélisation de la sécurité

Standards de sécurité (ISO/IEC 2700x)



Gestion des risques



Agir avant que ce ne soit trop tard...

- Pannes
- Infection par virus
- Vols
- Attaques logiques ciblées
- Accidents physiques
- Fraudes informatiques



Perte de temps...
mais aussi

Perte de la confiance de vos clients, de vos partenaires

La sécurité OK... mais vers qui me tourner ?

- Les questions que l'on se pose souvent :
 - A qui puis-je faire **confiance** ?
 - Combien cela va-t-il me **coûter** ?
 - La solution sera-t-elle **adaptée** à mes besoins ?

- Aides étatiques :
 - Loi des classes moyennes

- ➔ Intérêt d'un **LABEL** donné aux consultants et sociétés de services



Un label pour un conseil informatique de qualité



➤ Objectif principal du label : offrir un conseil informatique **neutre** et de **qualité** en PME à **coûts maîtrisés**

➤ Avantages pour les PME :

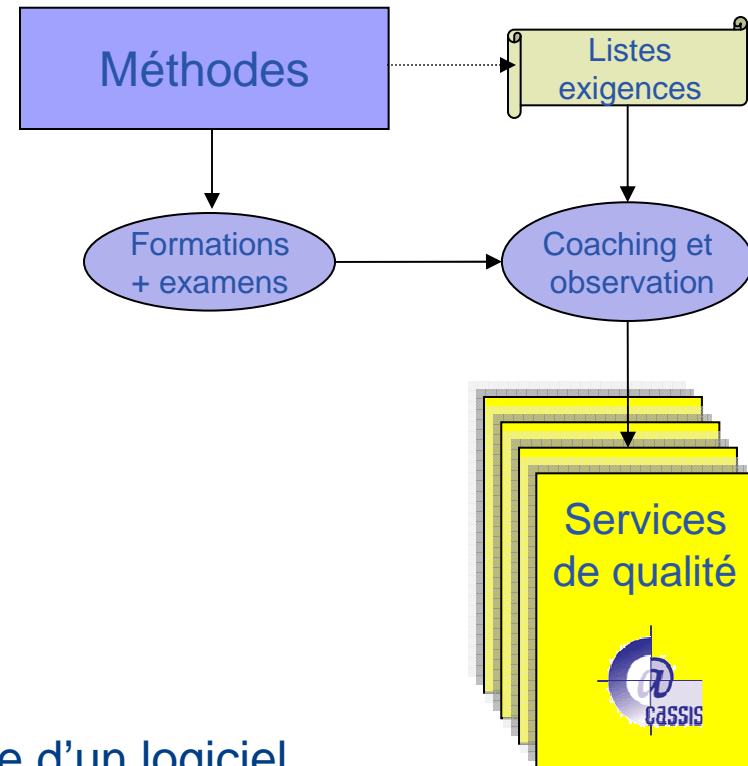
- Investissement en qualité des consultants et sociétés de services : méthodes, outils... **testés et éprouvés**
 - Garantie d'avoir un conseil le plus **adapté** à leurs besoins réels
 - Appartenance au réseau des PME gérées par des consultants et sociétés labellisés : pas seuls, **confiance**
- Support des Chambres, Ministère de l'Economie, Ministère des Classes moyennes

➤ Labellisation CASSIS®

- De personne :
 - Formations, examen, coaching
- De société sur un service fourni :
 - Audit
- Surveillance du label
- Des **services de qualité**

➤ Les premiers **services labellisés** :

- (Diagnostic eBusiness gratuit)
- Stratégie informatique
- Conseil en choix de logiciel
- Accompagnement à la mise en place d'un logiciel
- Evaluation de la maturité informatique
- Gestion de l'informatique





PME
(productivité et innovation)

Chambres
(aide à leurs affiliés)

Consultants
(performance sur le marché des PME)

Fournisseurs
(à intégrer)

Développer une **relation gagnant-gagnant** entre les **PME** et les **Sociétés de services** en mobilisant un **réseau de professionnels** autour de **méthodes neutres et de qualité**

Sociétés services
(services de qualité)

Politiques
(développement économique par les PME)

Le CRP Henri Tudor
(qualité des services)



- Asbl : en cours création

- Relais CASSIS à venir vers la Belgique et vers la France

- Autres services à venir :
 - Cassis Stratégie en 5 jours pour les petites entreprises
 - Gestion de projet
 - Sécurité : CASSIS SECURITE 2 & ISMS-PME

- www.cassis.lu

Offre de services Sécurité de l'Information

Le CRP Henri Tudor a pour vocation d'aider et d'accompagner les PME et TPE à se poser les bonnes questions, et sa volonté est de :

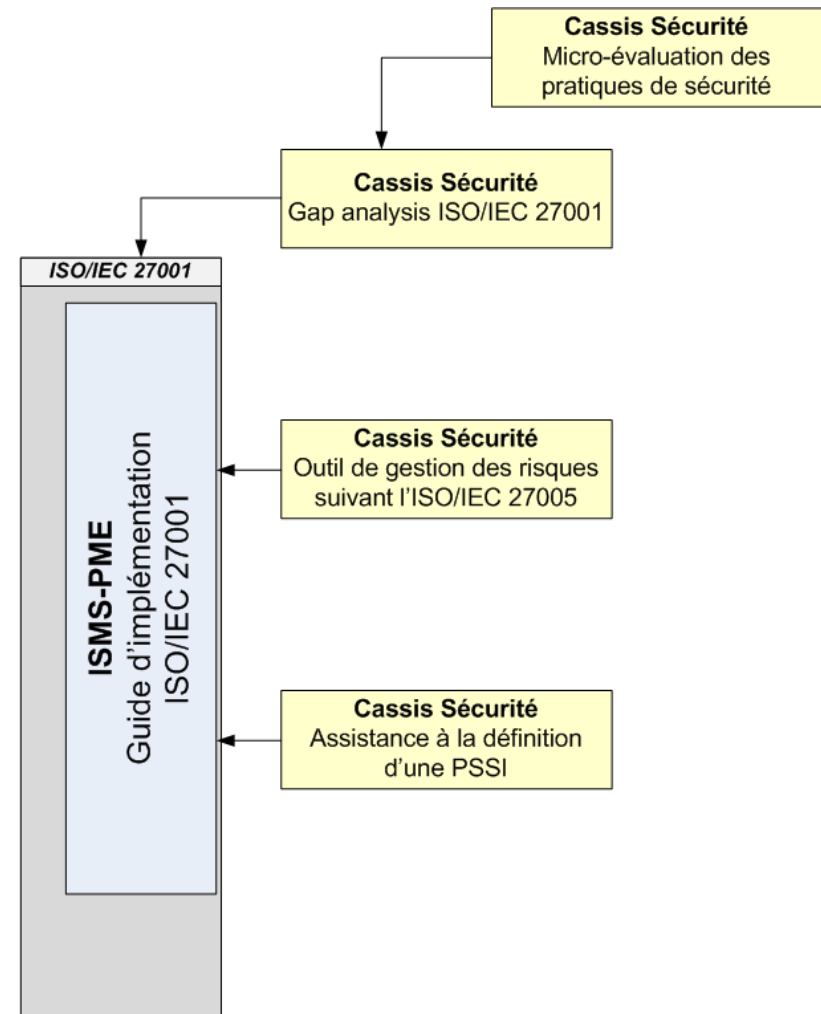
- Mieux connaître les préoccupations des PME et TPE
- Développer les services pour la sécurité informatique qui répondent aux attentes réelles du terrain
- Initier une collaboration avec les entreprises pour favoriser l'amélioration continue des services au travers du réseau CASSIS®

- CASSIS Securite 2
 - Micro-évaluation sécurité
 - Diagnostic sécurité
 - Analyse de gestion des risques
 - Politique de sécurité

- ISMS-PME

- Outillage méthodologique et logiciel pour le management de la sécurité en PME

- Respect des normes et standards du marché

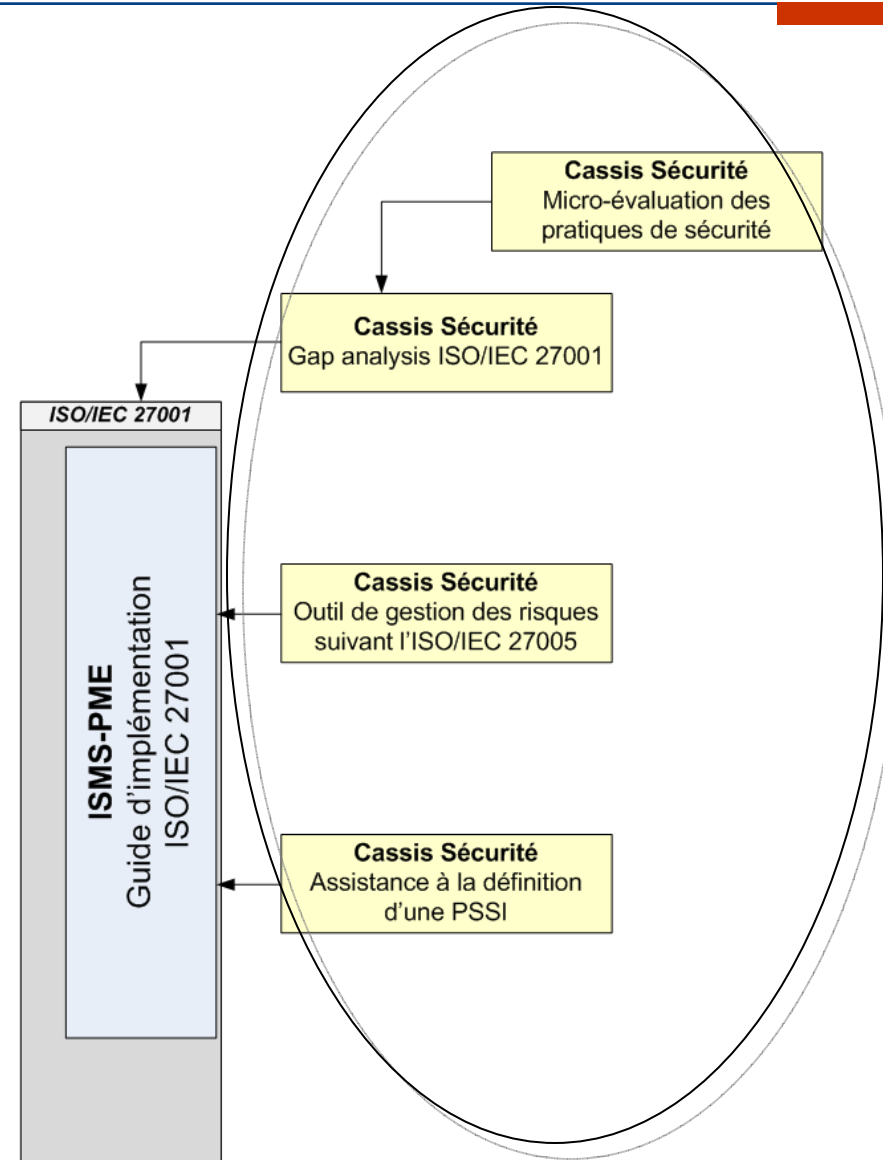


- ➔ **Projet FEDER en collaboration avec le MECO**
- ➔ **01/01/2009 – 31/12/2011**

- ➔ **Sécurité des systèmes d'information**
 - ➔ **Micro-évaluation sécurité**
 - ➔ **Diagnostic sécurité**
 - ➔ **Analyse de gestion des risques**
 - ➔ **Politique de sécurité**

- ➔ **eCommerce certified**

- ➔ **Sensibilisation à la sécurité**



- Analyse produits / services

- « Expérimentations » terrain
 - PME / CRP valeur ajoutée
 - PME / experts / CRP

- Transfert dans CASSIS : vers un label...

- Appel à intérêt / participation

ISMS-PME

Information Security Management System pour PME

Guide d'implémentation d'un Système de Management de la Sécurité de l'Information pour les PME

Sébastien Pineau

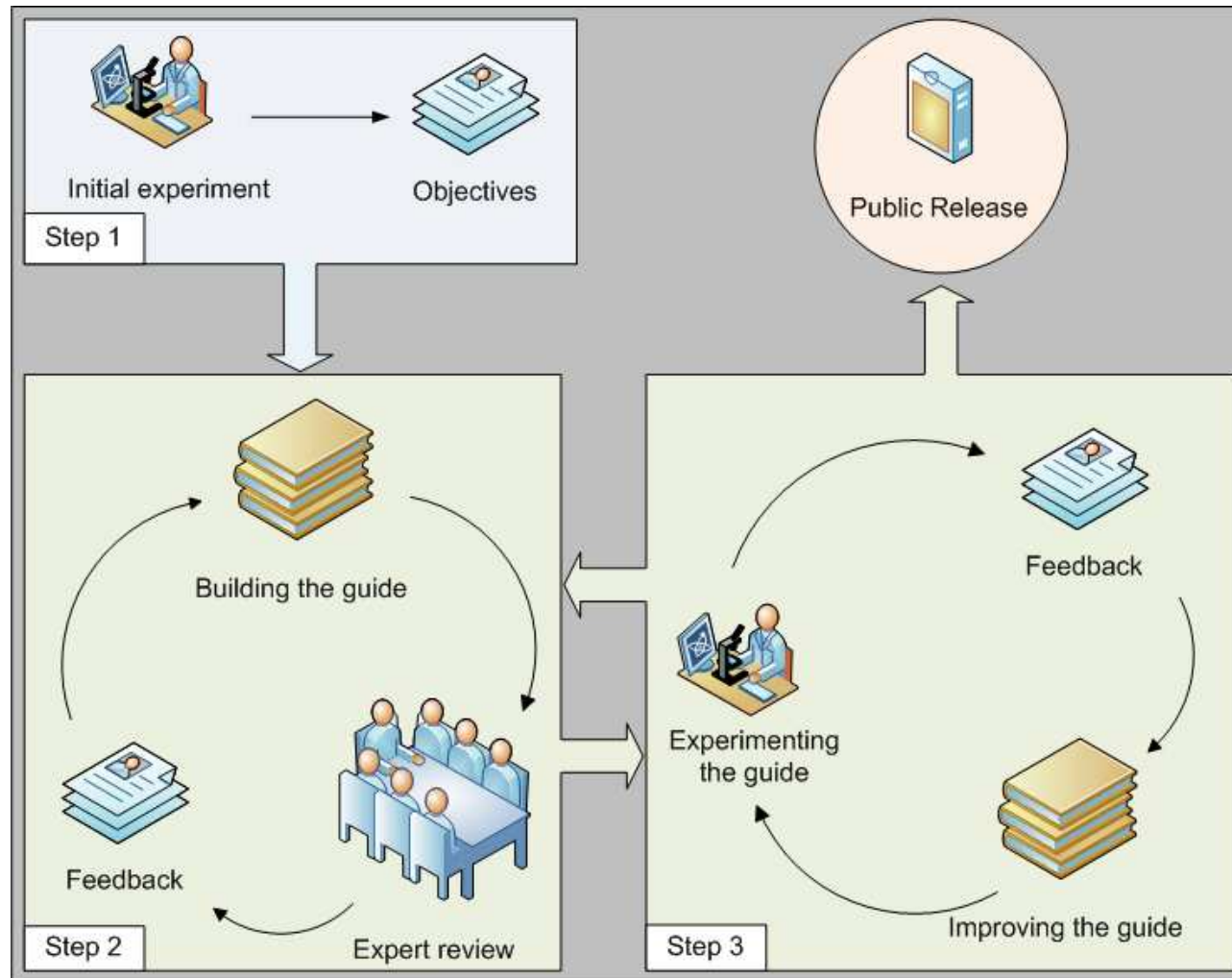
sebastien.pineau@tudor.lu

ISMS (SMSI) : Système de Management de la Sécurité de l'Information

Guide d'implémentation d'un ISMS pour les PME

- Objectifs et contexte du projet
- Méthode de recherche
- Expérimentation initiale
- Réalisation du guide
- Conclusion

- **Projet de recherche**
 - Ministère de l'Économie 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



- **Entreprise : Codasystem Benelux SA**
Preuve par l'image : développement d'un outil intégré de gestion de photos et d'information pour les activités terrain où les photos sont horodatées, géolocalisées, indexées, stockées, certifiées et facilement partageables.
- **Objectifs**
 - Apporter une réponse aux forts enjeux de l'entreprise pour manager la sécurité de ses informations
 - Développer une expertise sur les normes de référence (ISO/IEC 27001 et ISO/IEC 27005)
 - Identifier les facteurs critiques de succès
 - Développer la méthodologie
- **Durée - Investissement**
 - De Juin 2006 à Mai 2008 (dont 14 mois de développement effectif)
 - Investissement : environ 100 jours/homme
- **Résultat : une première entreprise privée certifiée au Luxembourg**
 - Mise à l'épreuve et formalisation de la méthode d'implémentation
 - Développement d'outils et de modèles
 - Ajustement des objectifs et du périmètre d'utilisation du guide

- **Appropriation et préparation**
 - Nécessité de composer une équipe
 - Importance de la gestion de projet
 - Besoin de formations
 - Engagement et association de la direction
- **Déploiement**
 - Ecart important au regard de la norme
 - Mise en place des procédures, gestion des enregistrements, formations/sensibilisations
 - Mise en œuvre des mesures de sécurité
- **Revue et suivi**
 - Audit interne et Revue de direction
 - Correction des non conformités
 - Accompagnement à l'audit
- **Conclusion et certification**
 - Retours d'expérience pour l'élaboration du Guide
 - Certification

- Bénéfices pour l'entreprise
 - Mise à plat (identification et formalisation) des processus
 - Prise de conscience et identification de la multiplicité et de la complexité des risques
 - Sélection et priorisation des mesures
 - Développement des compétences
 - Implication de la direction dans le management de la sécurité

- Un ISMS très simple et cohérent avec la taille et les capacités de l'entreprise
- La capacité à transférer les compétences pour manager l'ISMS
- La volonté de continuer de développement de compétences et l'amélioration de l'ISMS
- La reconnaissance de ses clients

- Objectifs pour le guide
 - Assimiler les concepts clés
 - Saisir l'intérêt et les enjeux d'un ISMS
 - Faciliter la compréhension d'une approche processus
 - Assimiler la logique PDCA (Plan – Do – Check – Act)
 - S'adapter aux attentes et aux spécificités d'une PME
 - Réduire la charge et les coûts
 - Permettre de faire la première itération en quelques mois
 - Se concentrer sur les tâches essentielles
 - Apporter des outils très simples à adapter à son entreprise
 - Faciliter la compréhension
 - Vulgariser les exigences de la norme l'ISO/IEC 27001
 - Assurer la cohérence et l'efficacité de la démarche
 - Maintenir un fort alignement avec la norme l'ISO/IEC 27001
 - Fournir un ensemble d'outils et de modèles

- Contenu du guide
 - I. Introduction**
 - A. Objectifs et modalités d'utilisation
 - B. Concepts clefs
 - II. Initialisation**
 - A. Composition de l'équipe
 - B. Formation de l'équipe au SMSI
 - C. Domaine d'application et objectifs
 - D. Bilan de l'existant
 - E. Planification du projet
 - III. Mise en place**
 - A. Politique de l'ISMS
 - B. Appréciation et traitement des risques
 - C. Mise en place des mesures et rédaction des procédures de sécurité
 - D. Rédaction et application des procédures du système de management
 - E. Sensibilisation du personnel
 - F. Choix et déploiement des indicateurs
 - IV. Revue du système**
 - A. Revue de direction
 - B. Clôture du cycle
 - V. Conclusions**
 - A. Délai d'implémentation et régularité du cycle
 - B. Comment aller vers la certification ?

- Contenu du guide

Tâches	<p>Produire le document décrivant la politique générale du SMSI en synthétisant sur deux pages :</p> <ol style="list-style-type: none"> 1. La définition d'objectifs clairs pour le SMSI 2. Les contraintes actuelles applicables (lois, règlements, normes, standards, contraintes métier et environnementales) ainsi que les éventuelles déclarations d'intention de mise en conformité. 3. Définir le niveau de risque global acceptable par l'organisme 4. Les critères de sécurité de l'information retenus (exemple : Confidentialité, intégrité, disponibilité, traçabilité, etc.) 5. L'engagement écrit de la direction 6. La définition du champ d'action visé 7. Une description synthétique de la situation actuelle <p>Une fois complétée, la politique du SMSI doit être <u>validée par la direction et communiquée au travers de l'organisme.</u></p> <p><i>Remarque : Les exigences légales se limitent généralement aux trois points suivants :</i></p> <ul style="list-style-type: none"> ▪ <i>Respect de la propriété intellectuelle et des droits d'auteurs</i> ▪ <i>Protection des données opérationnelles obligatoires et des données à caractère personnel</i> ▪ <i>Respect de la législation sur le droit du travail</i>
Entrées	Analyse Opérationnelle + Domaine d'Application
Sorties	Politique du SMSI
Acteurs	Direction, Responsable du SMSI

- Contenu du guide

ANNEXE INFORMATIVE 1 Recommandations pour l'appréciation des risques

1. Échelle de valorisation

Un simple tableau permet de rapidement et aisément classer les besoins et donc l'importance des actifs :

Valeur	Confidentialité	Intégrité	Disponibilité
0	Public	Nulle	Aucune contrainte
1	Restreint	Altération visible	Indisponible 1 semaine / an
2	Très restreint	Altération réduite	Indisponible 1 j / an
3	Secret	Ne peut être altéré	Toujours disponible

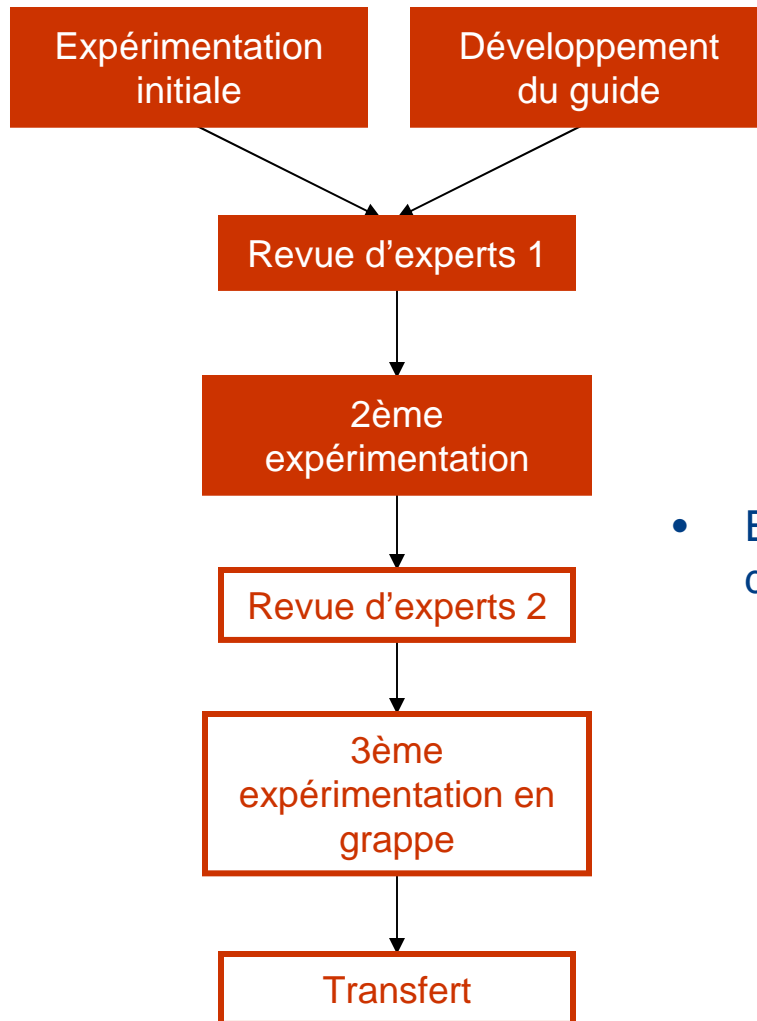
Ainsi, un actif ayant pour valorisation « Confidentialité restreinte » + « Altération réduite » + « Aucune contrainte de disponibilité » mais pas de critère de disponibilité aura une valeur maximale de 2 (altération réduite). Bien entendu, les valeurs de ce tableau sont adaptables selon l'organisme tant qu'il reste homogène et cohérent. De même, l'échelle (0 à 3) est modifiable pour plus de finesse si le contexte l'exige.

2. Étude des risques

Une notation de 0 à 4 est généralement adoptée pour pondérer chaque risque. Cependant, il est possible de faire varier l'échelle de notation pour obtenir un panel de nuances correspondant à l'organisme. On obtient donc un tableau adaptable basé sur le suivant :

Valeur	Occurrence dans l'année
0	Impossible
1	Peu probable
2	Probable
3	Très probable
4	Certaine

- Revue d'experts
 - 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 (Comité d'étude luxembourgeois pour la norme ISO/IEC 27001)
 - Une douzaine d'experts du domaine
- Mandatés pour revoir le guide
 - 3 itérations
 - 156 commentaires
- Nouvelle revue en septembre 2009



- 2ème expérimentation du guide

- Depuis début 2009
- Première expérience terrain, premiers retours pratiques

- Expérimentation en grappe d'entreprises

- 3 ou 4 entreprises de profils différents
- Formation groupée
- Coaching individualisé sur site
- Nouvelle amélioration du guide

- Transfert

- Guide gratuit
- Accompagnement proposé au sein du réseau Cassis
- Framework d'outils

- Appel à intérêt pour expérimenter les **outils sécurité** à venir :
 - Micro-évaluation sécurité
 - Diagnostic sécurité
 - Analyse de gestion des risques
 - Politique de sécurité
- Appel à candidature pour la constitution de la **grappe d'entreprises** :
 - PME uniquement
 - Lancement en septembre au plus tard
 - 9 sessions de formation et 10 sessions de coaching

Merci de votre attention

Questions ?

Corinne.Loesel@tudor.lu
Sebastien.Pineau@tudor.lu