

# ***Retour d'expérience sur la mise en œuvre d'un SMSI***

***Infosecurity - 21 novembre 2007***

# Sommaire

**I. Introduction**

**II. Le projet pilote**

**III. Apports de la démarche, écueils  
à éviter**

**IV. Conclusion**

# I. INTRODUCTION

# 1. Le groupe Crédit Mutuel Nord Europe

- 289 points de vente en France et en Belgique
- Près de 4000 salariés
- Plus d'1 million de clients

Chiffres arrêtés au 31/12/2006



- Caisse de Crédit Mutuel Nord Europe
- Bureau de Crédit Mutuel Nord Europe
- Chef lieu de département (France) et de province (Belgique)
- Siège de banque régionale
- NEPB Luxembourg
- Agence du réseau Crédit Professionnel

PÔLE ENTREPRISES

PÔLE GESTION POUR COMPTE DE TIERS

  
Banque  
PME-PMI

  
Crédit-bail  
mobilier

  
  
Crédit-bail  
immobilier

  
Investissement  
immobilier  
patrimonial

  
Gestion  
patrimoniale

  
MULTIFONDS

  
NEPE  
Gestion d'actifs  
mobiliers

Réseau belge  
du Crédit Professionnel



PÔLE BANCASSURANCE BELUX

Réseau français  
des Caisses Locales









  
Prévoyance  
et retraite

PÔLE ASSURANCES

PÔLE  
SERVICES  
ET ACTIVITÉS  
DIVERSES

PÔLE BANCASSURANCE FRANCE

# 1. Pourquoi un SMSI ?

**La Direction a pris conscience de cette nécessité**

**Pourquoi ?**

- **Harmoniser les pratiques dans le groupe**
- **Pression réglementaire**
- **Pression de la commission bancaire**
- **Pression de l'environnement**

# 1. Le rôle du RSSI au CMNE

## Missions principales :

- Mettre en œuvre la politique de sécurité du groupe
- S'assurer de l'existence des PRI et des PCA
- Améliorer la sécurité des opérations, la confidentialité des données et la prévention du risque
- Déterminer le risque maximum tolérable
- Sensibiliser à l'importance de la sécurité de l'information

# **I. Le projet pilote**

# Sommaire

**1. Les objectifs**

**3. La démarche**

**5. Timing**

# 1. Objectifs

**Adopter une référence : norme ISO 27001**  
Sans vouloir obligatoirement la certification

**Pas la certification ... dans un 1<sup>er</sup> temps**

**Elaborer et mettre en œuvre une méthode**

**Se préparer à déployer un SMSI dans chaque pôle**

**Définir l'organisation générale de la sécurité**

# 1. La démarche

- **Sélectionner une société du groupe « pilote »**
- **Préparer une infrastructure commune déployée dans les autres entités**
- **Déploiement piloté par le RSSI**

# 1. La démarche

**1<sup>ère</sup> phase : Analyser les risques**

**2<sup>ème</sup> phase : Identifier et rédiger les procédures**

**3<sup>ème</sup> phase : Définir l'organisation de la sécurité**

# Phase 1 : Analyse des risques

- **Identifier les actifs**  
Source : PCA, entretien responsables métiers
- **Estimer le niveau de gravité D, I, C, P**  
Source : analyse des risques opérationnels CM CIC
- **Identifier les vulnérabilités et les menaces**  
Source : entretiens, expériences, EBIOS
- **Estimer la fréquence de survenance des menaces**  
Source : tableau des fréquences (CM CIC), expérience

# Phase 1 : Analyse des risques

- Calculer le niveau de risque

$$NR = \max (G) \times F$$

- Identifier les mesures de sécurité existantes
- Estimer la fréquence résiduelle
- Calculer le niveau de risque résiduel
- Identifier les mesures de sécurité à mettre en œuvre

Si  $NR \geq$  Risque Maximum Tolérable

# Phase 1 : Analyse des risques

## Les segments de risques :

Niveaux de risque						
Fréquence		1	2	3	4	5
Gravité		1	2	3	4	5
1		1	2	3	4	5
2		2	4	6	8	10
3		3	6	9	12	15
4		4	8	12	16	20
5		5	10	15	20	25
6		6	12	18	24	30
7		7	14	21	28	35

# Phase 1 : Analyse des risques

**Identification des mesures de sécurité en cours ou déjà réalisées :**

- **Restriction d'accès aux sites de vente par correspondance**
- **Limite des tailles des messages en envoi**
- **Filtrage des accès externes**
- **Traces des accès Internet**

# Phase 1 : Analyse des risques

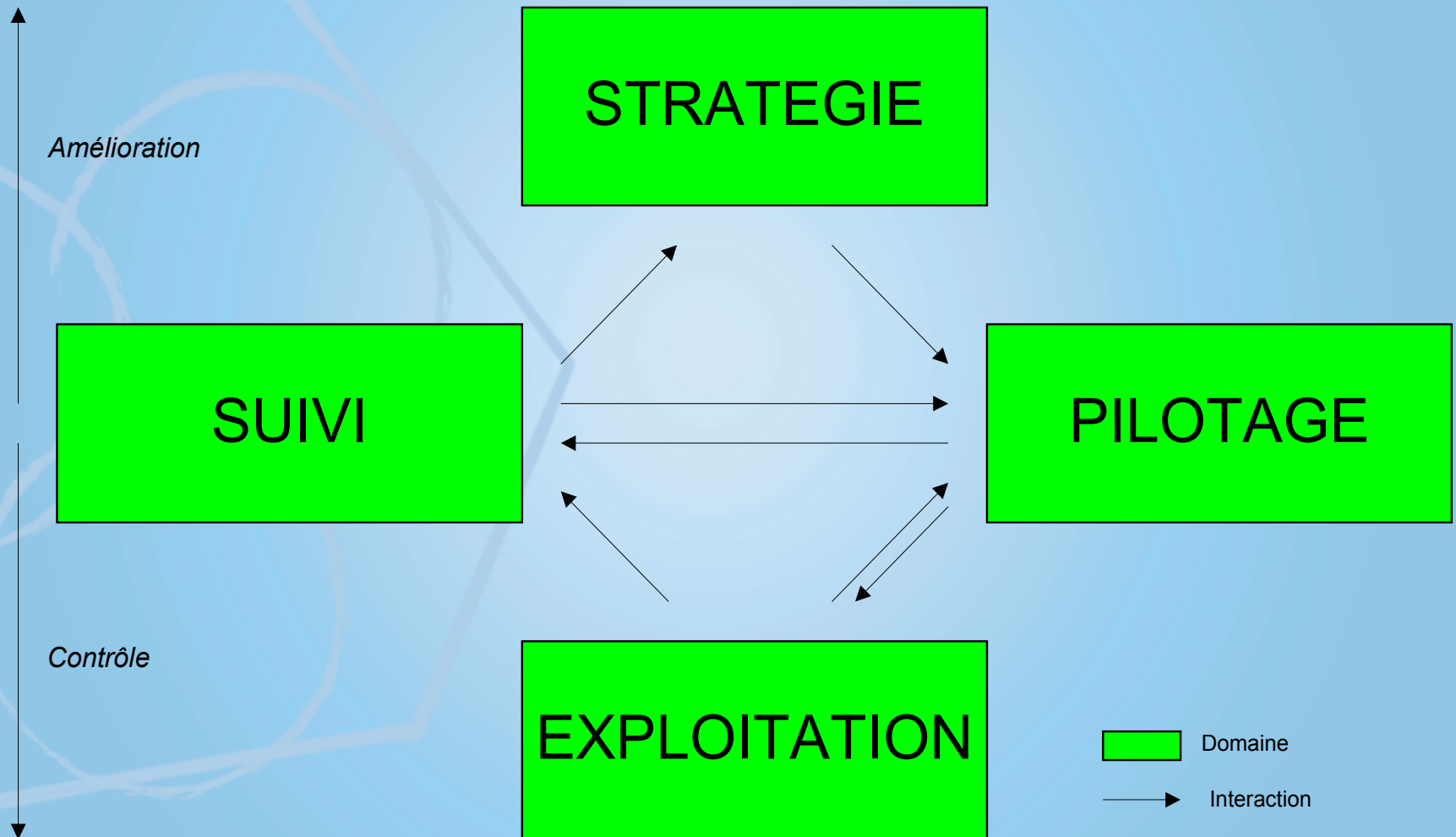
**A mettre en œuvre :**

- **Formation / sensibilisation**
- **Charte**
- **Authentification forte**

## Phase 2 : Les procédures

- Analyse de risques
- Gestion des documents
- Revue du SMSI
- Détection et remontée des incidents
- Procédure métiers : engagements
- Procédure de contrôle, etc.

# Phase 3 : Organisation



## Phase 3 : Organisation

### Le RSSI, son rôle :

- Support dans la mise en œuvre des SMSI
- S'assure de la conformité des SMSI
- Met en œuvre des process « groupe »
- S'assure de la revue régulière des SMSI

# 1. Timing

- Démarche initiée en février 2007
- Dans la filiale « pilote »
- Reste à faire (début 2008) :
  - Valider le SMSI
  - Compléter la DdA
  - Définir des indicateurs
  - Terminer de rédiger les procédures métier

# 1. Timing

- **Reste à faire :**
  - Valider le SMSI au plus haut niveau
  - Définir des tableaux de bord « sécurité »
  - Sensibiliser
  - Déployer la démarche dans chaque pôle

# **I. Apports, écueils à éviter**

# 1. Les apports

- Recenser les mesures existantes
- Les rendre cohérentes et auditables
- Justifier les mesures de sécurité à mettre en œuvre
- Démarche pérenne

# 1. Les écueils à éviter

- Faire de la procédure
- Mettre en œuvre des mesures de sécurité sans justification
- Compliquer la démarche

# I. Conclusion

- Faites vous aider de spécialistes
- Mettez en œuvre avant d'écrire les procédures
- Faites « votre marché » dans les méthodes existantes

Par exemple : l'analyse de risques

**Merci de votre attention ...**

**Avez-vous des questions ?**