

# L'approche Iso27001 au sein du Gie Systaliens de Réunion Bayard

Club Iso 27001 - Emmanuel GARNIER  
21 novembre 2007



# L'approche Iso 27001 au sein du GIE Systalians

---

## SOMMAIRE

- Systalians : le Gie de Réunica Bayard
- La sécurité au sein de Systalians
- L'ISO 27001 : de multiples raisons d'y aller
- La démarche de mise en œuvre
- Un plan d'action sur 2 ans : la certification pour début 2009
- Conclusion

# L'approche Iso 27001 au sein du GIE Systalians

---

## SOMMAIRE

- Systalians : le Gie de Réunica Bayard
- La sécurité au sein de Systalians
- L'ISO 27001 : de multiples raisons d'y aller
- La démarche de mise en œuvre
- Un plan d'action sur 2 ans : la certification pour début 2009
- Conclusion

# Systalians, le GIE informatique de Réunica Bayard

---

- **Systalians : GIE de la protection sociale**

- Né du rapprochement des groupes de protection sociale **Réunica** et **Bayard Retraite Prévoyance**
- Il a pour objet :
  - de **mettre en commun et de mutualiser**, tant sur le plan technique que financier, les différents systèmes d'informations spécifiques à chacun de ses membres ou communs à tout ou partie d'entre eux, dans le but d'en **réduire leurs coûts**,
  - de **concevoir, mettre en œuvre** et **gérer** tous systèmes d'informations pour ses membres,
  - De fournir à ses membres les **services** et **prestations de conseils** associés
- Créé en juillet 2005, Systalians est entré **en activité le 1er janvier 2006**, date à laquelle l'ensemble du personnel informatique du groupe Réunica Bayard a rejoint le GIE.

# Systalians, le GIE informatique de Réunica Bayard

---

- **Systalians, en quelques chiffres**

- Effectifs : 350 personnes (dont 150 internes)
- Localisation :
  - Courbevoie : Direction, Domaines Etudes, Intégration Usine Retraite, Achats, Contrôle de gestion, Sécurité,
  - Esvres sur Indre : Domaines Etudes, Production, Méthodes Qualité, Sécurité
- Activité :
  - Chiffre d'affaires : 65,3 millions d'euros
  - Investissements : 6,3 millions d'euros
- Volumes gérés (2006) :
  - 3 000 postes de travail standards
  - 230 serveurs Windows, UNIX, AS400, MVS de production
  - Espace disque de production : 40 To
  - 325 millions de transaction CICS sur le serveur central
  - 25 000 appels au Service Desk (centre d'accueil CATI)
  - 17 000 demandes d'intervention traitées

# Systalians, le GIE informatique de Réunica Bayard

---



- **Réunica Bayard**
  - Leader de la **retraite complémentaire**,
  - 10ème groupe français en **prévoyance**,
  - Groupe paritaire indépendant à but non lucratif
  - **2 300 collaborateurs**, répartis :
    - 3 implantations en Ile de France (Courbevoie, Levallois-Perret, Paris)
    - 4 implantations en régions (Angoulême, Esvres-sur-Indre, Lyon, Toulouse)
    - 27 délégations commerciales
    - 11 délégations sociales

# Systalians, le GIE informatique de Réunica Bayard

---



- **Réunica Bayard**

- **Retraite**

- 4 institutions de retraite complémentaire qui gèrent et redistribuent les cotisations de retraite complémentaire (en ARRCO : ANEP, IREPS ; en AGIRC : CIRCACIC, CRICA)

- **Chiffres clés : 4,6 millions d'affiliés – 1,3 million d'allocataires (retraités) – 7,2 milliards d'euros de cotisations encaissées**

- **Prévoyance**

- **2 institutions** de prévoyance : Bayard Prévoyance et Réunica Prévoyance.

- Assurent une garantie aux salariés et leur famille en cas de maladie, maternité, accident de travail, invalidité, décès

- **1 mutuelle interprofessionnelle** qui propose aux particuliers une complémentaire santé

- **Chiffres clés : 2 millions d'assurés en prévoyance, 154 000 assurés en santé, 30 000 contrats entreprises – 330 millions d'euros de cotisations encaissées**

# SYSTALIANS, le GIE informatique de la protection sociale

---

- **Deux grands axes d'activités : retraite et prévoyance**
  - Un secteur retraite en forte concentration avec des synergies entre groupes (Usine Retraite),
  - La prévoyance, un milieu qui reste concurrentiel
- **Enjeux de Sécurité**
  - Flux financier,
  - Données à caractère personnel,
  - Garantir un niveau de sécurité conforme aux exigences des membres adhérents et des fédérations AGIRC et ARRCO

# L'approche Iso 27001 au sein du GIE Systalians

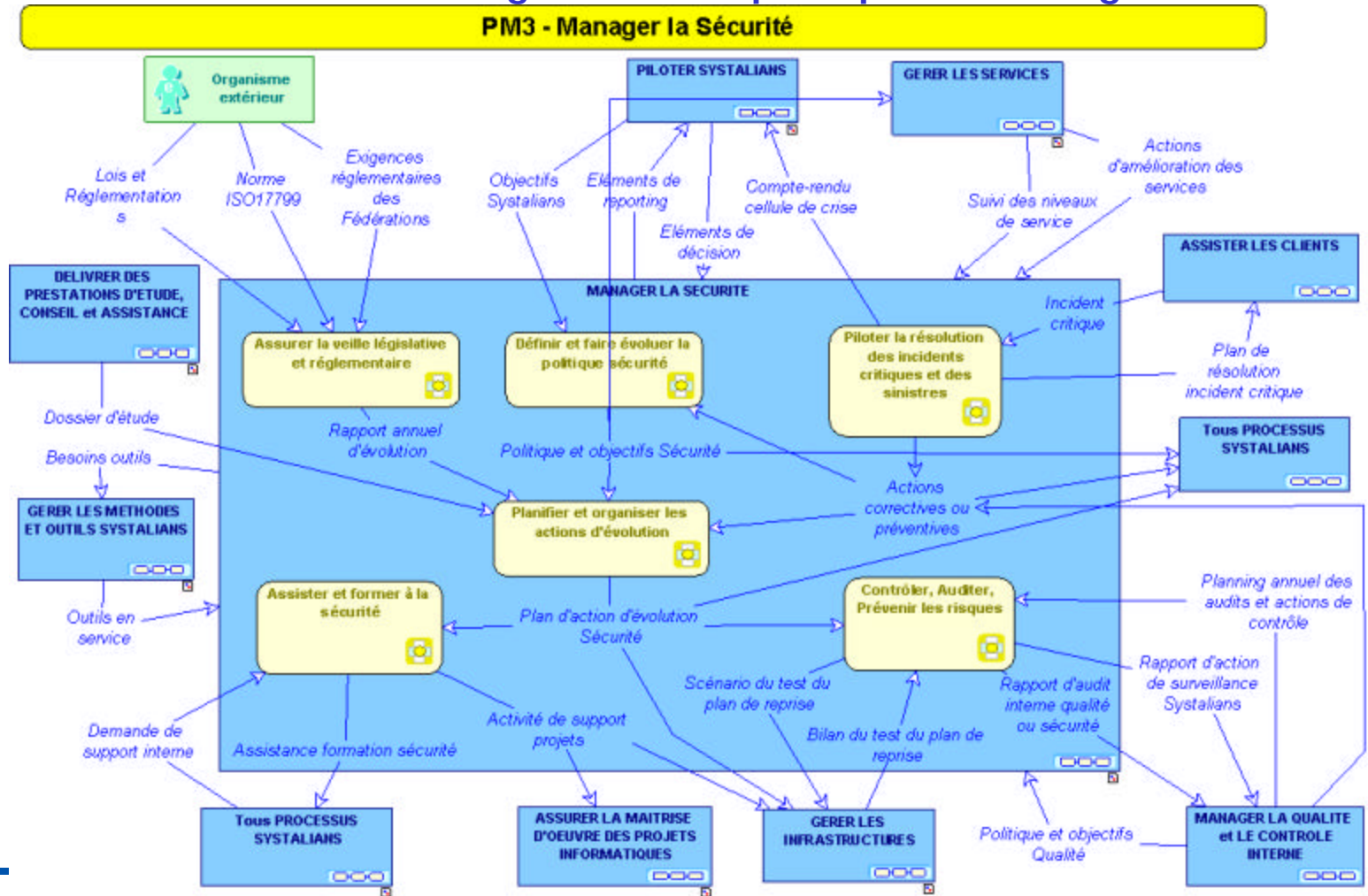
---

## SOMMAIRE

- Systalians : le Gie de Réunica Bayard
- La sécurité au sein de Systalians
- L'ISO 27001 : de multiples raisons d'y aller
- La démarche de mise en œuvre
- Un plan d'action sur 2 ans : la certification pour début 2009
- Conclusion

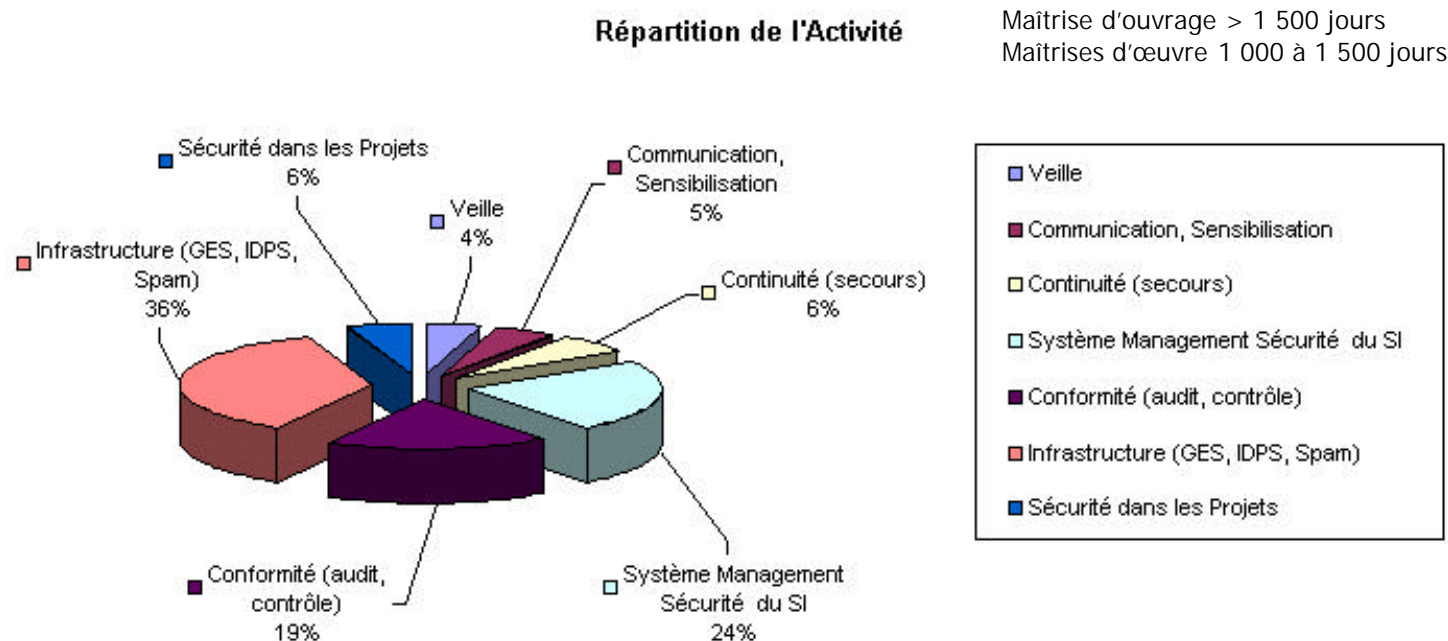
# La sécurité chez SYSTALIANS

- Une mise en œuvre en ligne avec les principes de management Qualité

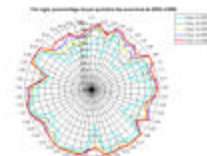


# La sécurité chez SYSTALIANS

- Revue annuel du processus dans une démarche d'amélioration continue



- Un encadrement par le règlement de sécurité des fédérations AGIRC ARRCO (basé sur l'ISO 27002)



# L'approche Iso 27001 au sein du GIE Systalians

---

## SOMMAIRE

- Systalians : le Gie de Réunica Bayard
- La sécurité au sein de Systalians
- L'ISO 27001 : de multiples raisons d'y aller
- La démarche de mise en œuvre
- Un plan d'action sur 2 ans : la certification pour début 2009
- Conclusion

# ISO 27001, de multiples raisons d'y aller

---

- **A partir d'un existant aligné sur les bonnes pratiques ...**
  - Certification ISO 9001 depuis 2001,
  - Mise en place du contrôle interne en 2006 basé sur COBIT,
  - Alignement en cours sur les pratiques ITIL
- **La volonté d'aller plus loin**
  - S'aligner sur l'ISO 27001
- **Se démarquer dans le secteur**
  - Et être attractif
- **Simplifier le dialogue**
  - Avec les métiers, les fournisseurs et les acteurs externes
  - Faciliter les démarches d'audit
- **Renforcer la confiance des clients**



# L'approche Iso 27001 au sein du GIE Systalians

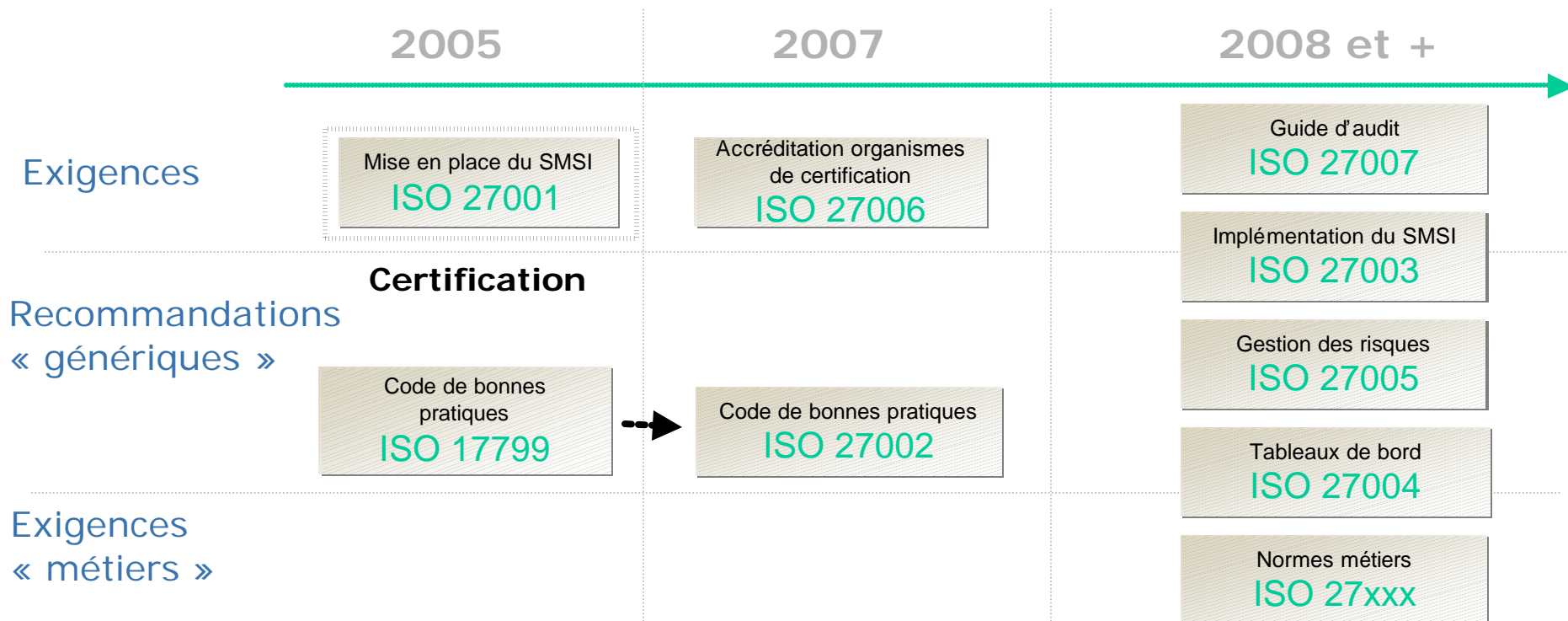
---

## SOMMAIRE

- Systalians : le Gie de Réunica Bayard
- La sécurité au sein de Systalians
- L'ISO 27001 : de multiples raisons d'y aller
- La démarche de mise en œuvre
- Un plan d'action sur 2 ans : la certification pour début 2009
- Conclusion



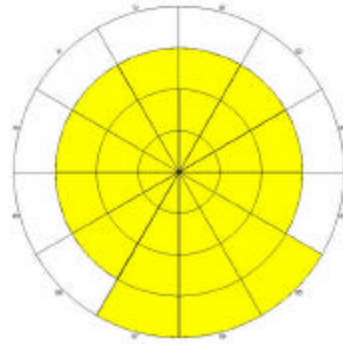
# Iso 27001 : norme certifiante



Une différence majeure par rapport aux autres systèmes de management : des mesures et des contrôles techniques

# Méhari 2004 – une conversion vers l'ISO et un périmètre modifié

**MEHARI  
2004**  
*Orientation  
risques*

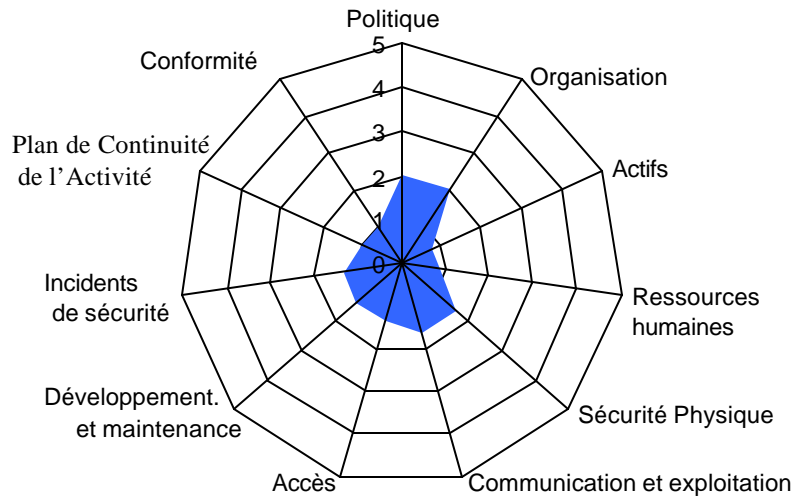


Périmètre initial

- Périmètre : Réunionica
- Population : utilisateurs, acteurs du SI, direction, métiers...
- Site : tous les sites Réunionica



**ISO 27002**  
*Orientation  
conformité*

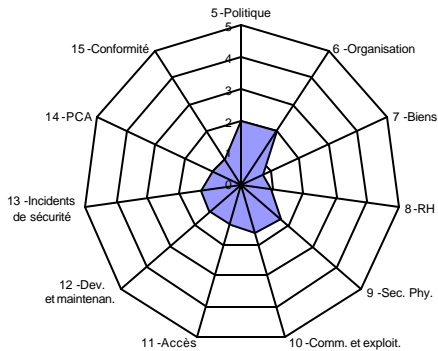


Adaptation au périmètre 2007

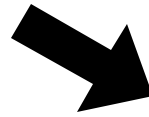
- Périmètre : Systalians
- Population : acteurs du SI  
→ naturellement plus sensibilisés
- Sites : Courbevoie et Esvres  
→ meilleure sécurité physique

# Diagnostic ISO 27002

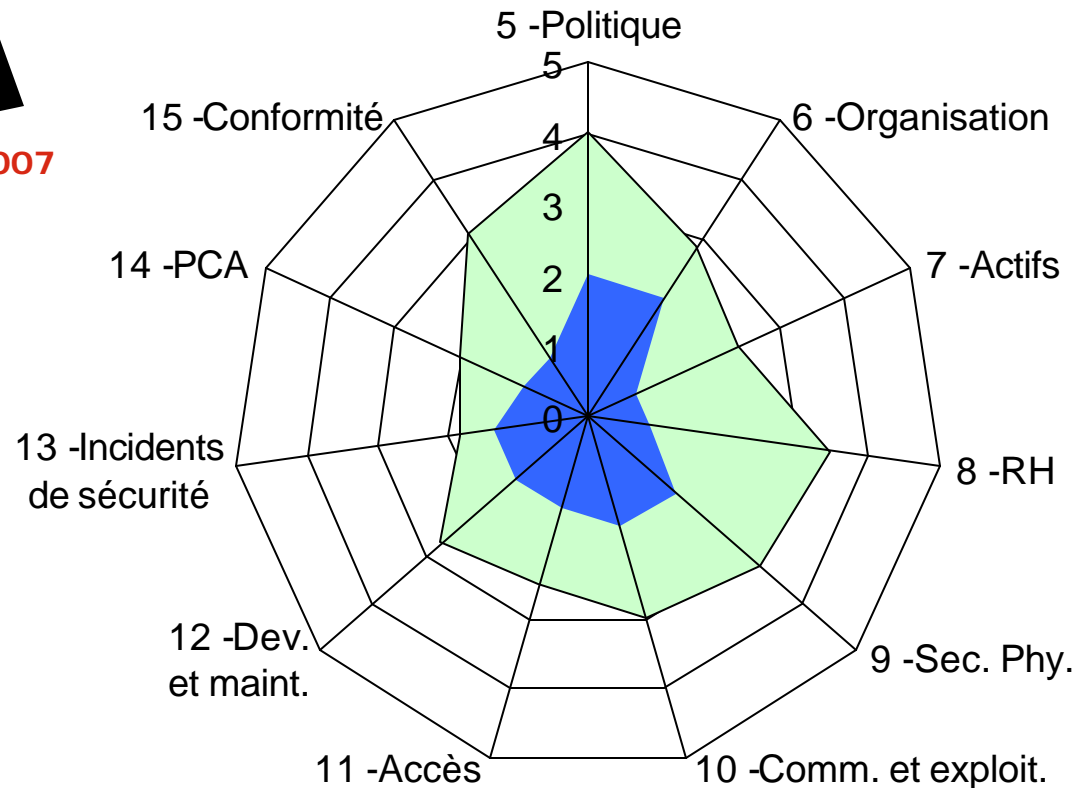
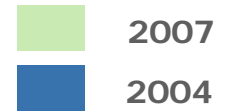
## Des pratiques sécurité en forte évolution depuis 2004



2004 ...



...2007



### Echelle

0-Inexistant

1-Pratique existante mais non alignée, effort important

2-Pratique existante mais non alignée

3-Pratique alignée mais non mise en œuvre

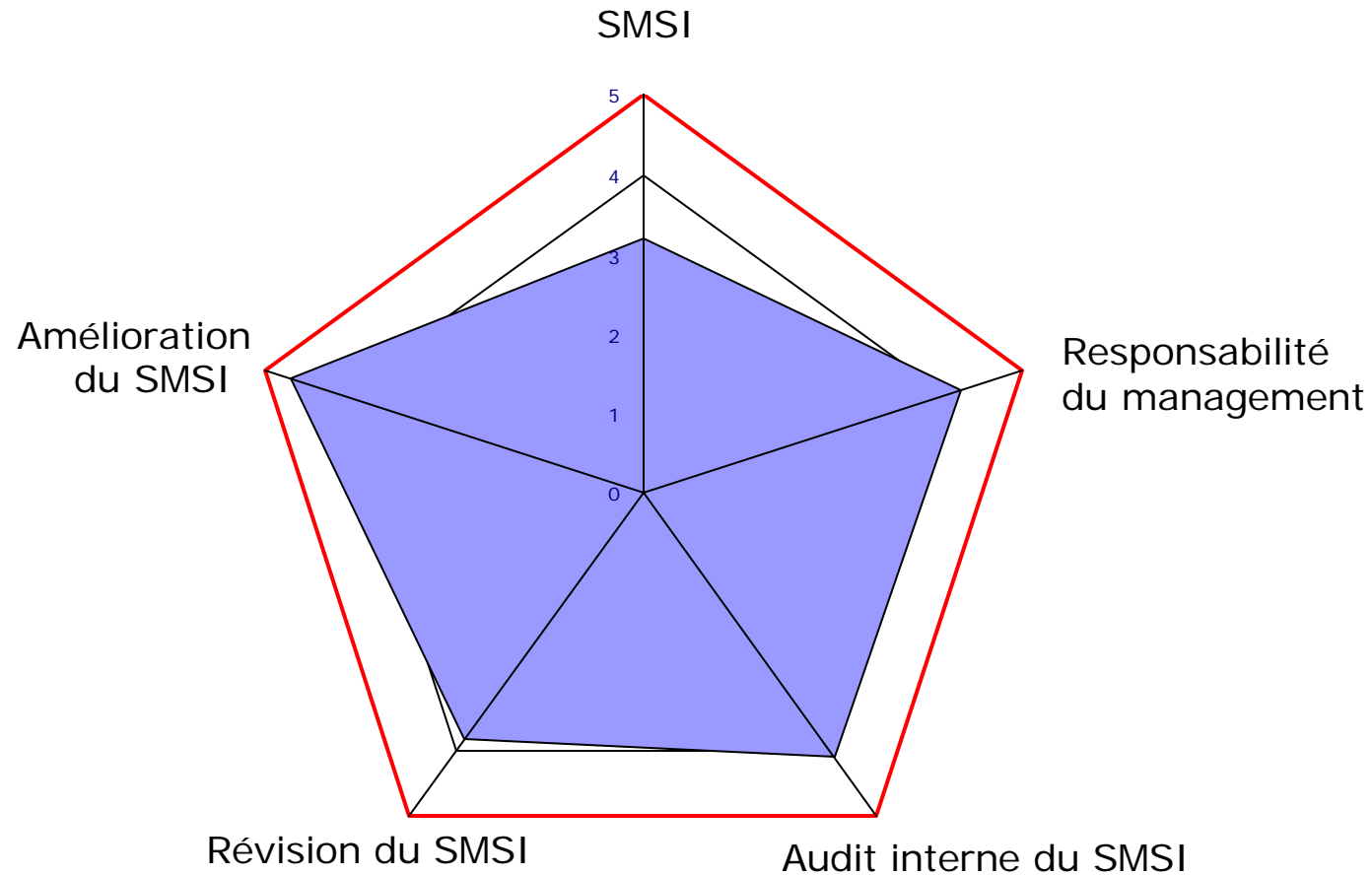
4-Pratique mise en œuvre et demande un ajustement

5-Pratique existante, alignée, contrôlée et boucle de progrès

**Des bonnes pratiques à sélectionner et à appliquer en fonction de l'analyse de risques**

# Situation : un SMSI récent, aligné sur les bonnes pratiques ISO 9001

| Echelle   |
|---|
| 0-Inexistant  |
| 1-Pratique existante mais non alignée, effort important       |
| 2-Pratique existante mais non alignée                         |
| 3-Pratique alignée mais non mise en œuvre                     |
| 4-Pratique alignée, mise en œuvre et demandant un ajustement  |
| 5-Pratique existante, alignée, contrôlée et boucle de progrès |



**Un alignement obligatoire du système de management par rapport à la norme ISO 27001**

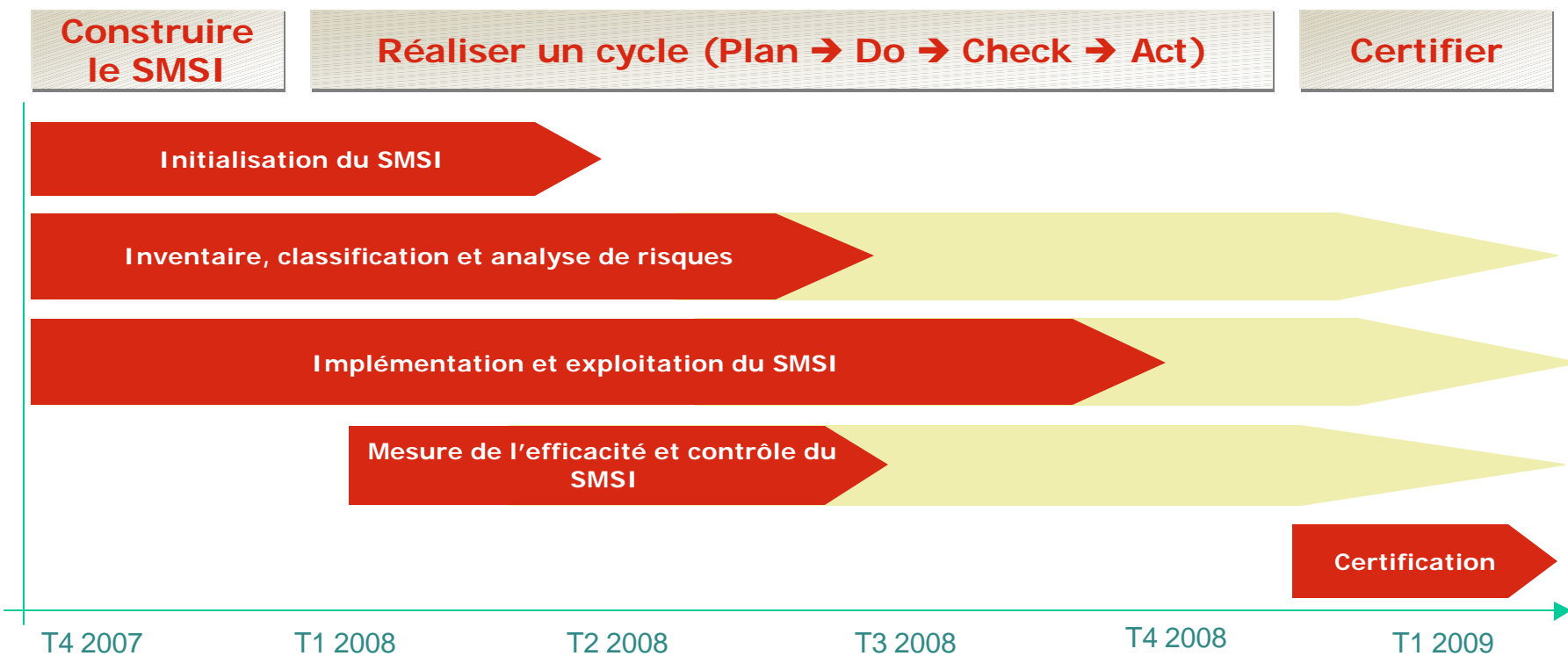
# L'approche Iso 27001 au sein du GIE Systalians

---

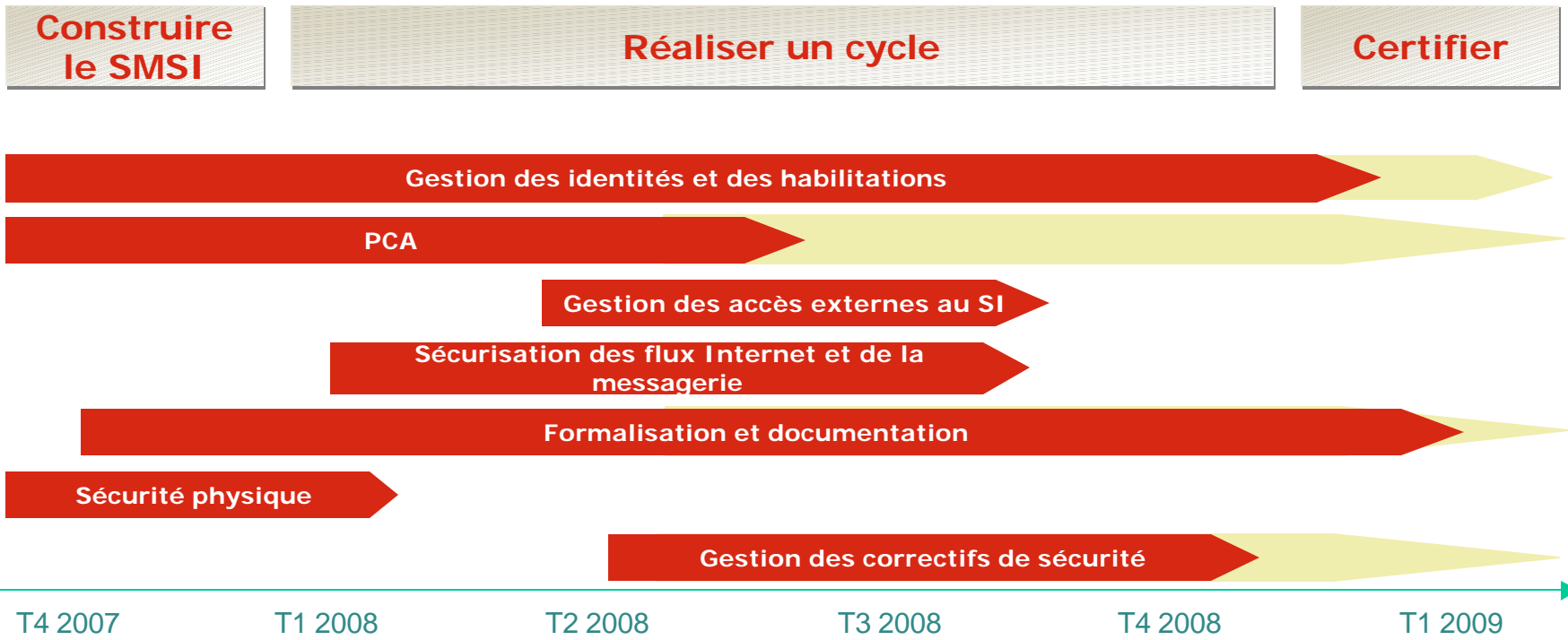
## SOMMAIRE

- Systalians : le Gie de Réunica Bayard
- La sécurité au sein de Systalians
- L'ISO 27001 : de multiples raisons d'y aller
- La démarche de mise en œuvre
- Un plan d'action sur 2 ans : la certification pour début 2009
- Conclusion

# Un SMSI à construire progressivement



# De nombreux projets à intégrer dans l'existant



# L'approche Iso 27001 au sein du GIE Systalians

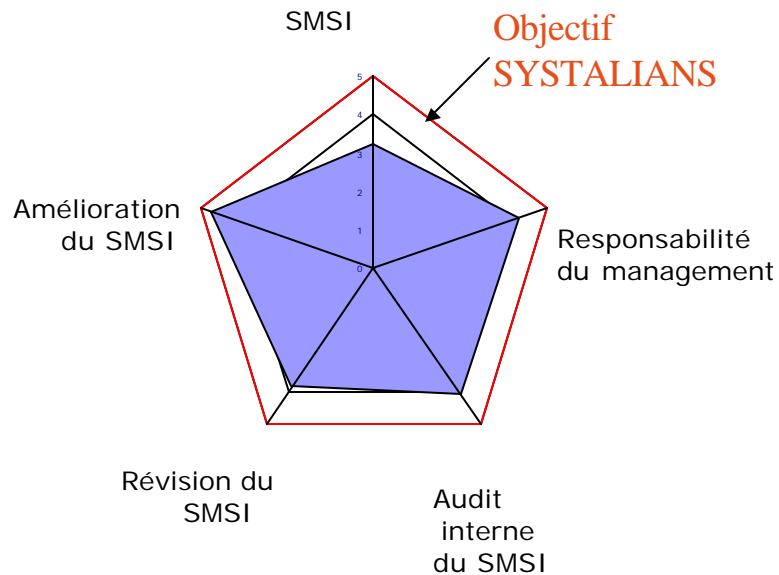
---

## SOMMAIRE

- Systalians : le Gie de Réunica Bayard
  - La sécurité au sein de Systalians
  - L'ISO 27001 : de multiples raisons d'y aller
  - La démarche de mise en œuvre
  - Un plan d'action sur 2 ans : la certification pour début 2009
- Conclusion

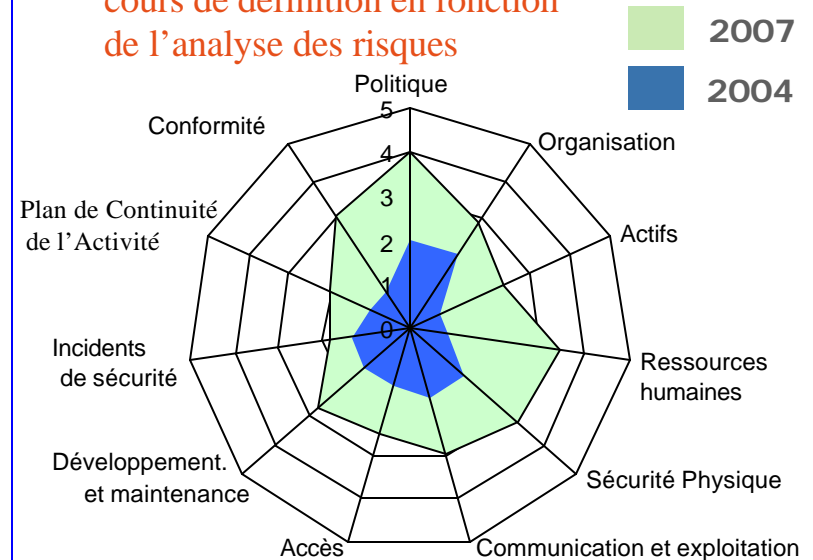
# Globalement, comment se situe le GIE SYSTALIANS du point de vue des exigences des référentiels de sécurité ?

- **Iso 27001 : norme pour la mise en place d'un Système de Management de la Sécurité de l'Information (SMSI)**



- **Iso 27002 : un ensemble de bonnes pratiques à sélectionner et à appliquer en fonction de l'analyse de risques**

Objectif SYSTALIANS en cours de définition en fonction de l'analyse des risques



# Points clés pour obtenir la certification

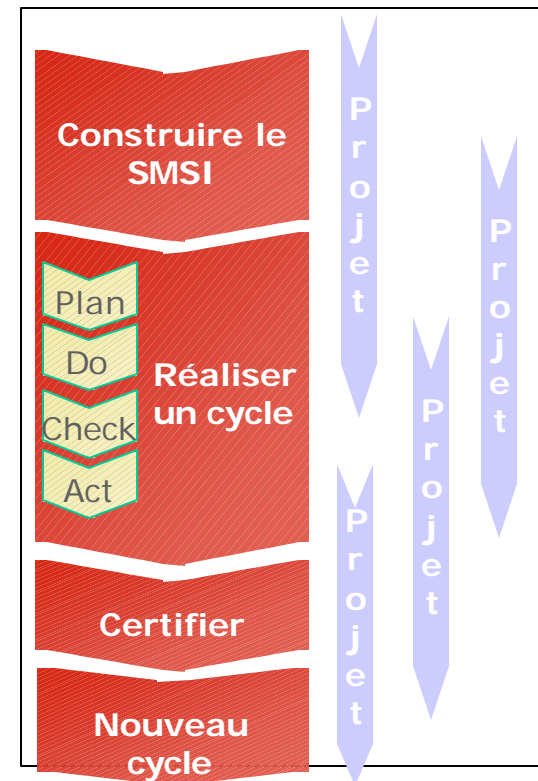
---

- **Réaliser un diagnostic : mesurer la conformité, identifier les manques**
  - Outiller la démarche et prendre en compte la difficulté d'évaluation par rapport à l'ISO 27002
- **Définir le périmètre : ni trop ambitieux, ni pas assez, aligné sur celui de l'ISO 9001**
- **Construire sur l'existant**
  - Construire un SMSI s'insérant dans la structure de l'organisation
  - Démarche qualité : gestion des documents et des enregistrements
  - Analyse de risques : réutiliser la démarche de l'analyse de risques COBIT existante
  - Processus : s'insérer avec ITIL
- **Avoir l'appui du management au plus haut niveau et valoriser**
- **Prévoir dès la construction les efforts de maintien dans le temps**
  - Alignement continu du SMSI : revue annuelle et suivi des risques
  - Mesure de l'efficacité : contrôle et indicateurs
  - Maintenir et exploiter le domaine sécurité des infrastructures

## Un point clé pour maintenir la certification

Réaliser un cycle complet avant d'envisager la certification

- ▶ Une décision importante pour ne pas prendre de risque sur le maintien du certificat
- ▶ Et qui n'est pas bloquant pour l'avancement des projets



L'implication de tous et à tous les niveaux est un pré-requis à la réussite de la certification

# Les apports déjà ressentis

- **La capacité de se mobiliser** sur un projet dans un objectif de **planning déterminé**, et **d'accélérer** ainsi la démarche de Sécurité
- **Suivi simplifié** de la démarche Iso 27001
  - Insertion dans la démarche qualité
  - Réalisation d'un outillage
    - Lors du diagnostic
    - Adaptation lors de la conception du SOA



En cours :

- Définition de la méthodologie **d'analyse de risques**
  - Menant à la conception du SOA
- Sélection des **équipes d'audit** sécurité interne