



# Retour d'expérience de l'ISO 27001 dans une PME

Olivier LEMOINE – RSSI d'Odiso



## 1. ADISTAR EN CHIFFRES

2. POSITIONNEMENT

3. ELEMENTS DECLENCHEURS

4. DIFFICULTES / POINTS MARQUANTS

5. IMPLICATION DES COLLABORATEURS

6. BENEFICES

7. PROCHAINES ETAPES





## ADISTAR EN CHIFFRES

- Créé en 1998 à Roubaix (Métropole lilloise)
- Evolution exponentielle du nombre de salariés depuis 2 ans
- 130 collaborateurs
- Groupe : ensemble de TPE/PME spécialisées dans un domaine des nouvelles technologies
  - Solutions
  - Services
  - Edition
- Un chiffre d'affaires en augmentation de 80% par an
- Adistar n'existe plus, nouveau périmètre :
  - Odiso (possède toute l'infrastructure)
  - EMS (Service)





1. ADISTAR EN CHIFFRES

**2. POSITIONNEMENT**

3. ELEMENTS DECLENCHEURS

4. DIFFICULTES / POINTS MARQUANTS

5. IMPLICATION DES COLLABORATEURS

6. BENEFICES

7. PROCHAINES ETAPES





## POSITIONNEMENT

### *Périmètre : 2 cœurs de métier*



- Société de conseil
- Hébergement à haute valeur ajoutée
- Conseil et offres sur-mesure de l'infogérance
- Pôle de Recherche & Développement
- 200 serveurs hébergés
- 3 data centers sécurisés

- Solution de routage et tracking d'e-mailing de fidélisation

- Application pour gérer les campagnes

- Gestion et mise à jour des BDD
- Conception du message
- Analyse et report en temps réel

- 400 millions de mails envoyés par mois





1. ADISTAR EN CHIFFRES

2. POSITIONNEMENT

**3. ELEMENTS DECLENCHEURS**

4. DIFFICULTES / POINTS MARQUANTS

5. IMPLICATION DES COLLABORATEURS

6. BENEFICES

7. PROCHAINES ETAPES





## ELEMENTS DECLENCHEURS

### Problématique

- **Odiso** : hébergement de données et d'applications sensibles (B2B,B2C)
- **EMS** : nombreuses BDD clientes contenant des données nominatives
- Des contraintes imposées par nos clients
  - **Besoin de garantir la C, I, D des informations**

### L' ISO 17799 comme point de départ

- Mesures de l'ISO17799 sélectionnées et mises en place
  - Pourquoi appliquer une mesure plutôt qu'une autre ?
- ISO 27001 semble répondre à nos besoins :
  - Surveiller et contrôler la sécurité
  - Respecter la conformité aux diverses lois
  - Etude préalable pour la mise en place des mesures ISO 27002 (=ISO17799)





### Une demande de la Direction...

- Structure grandissante
  - Part non négligeable de stagiaires
  - Besoin de contrôler la sécurité
- Direction d'ODISO sensible à la problématique sécurité
  - Notre métier repose sur l'informatique
  - Positionnement sur le service de qualité
  - Besoin d'être rassurée
  - Mise en place de la norme poussée par Odiso, l'entité technique
- Suite à des incidents jusqu'alors maîtrisés
  - Peur que cela se reproduise et détruise le business (et l'image)





## ELEMENTS DECLENCHEURS

### ...et des clients

- Montrer que la sécurité est un sujet au cœur des préoccupations
  - Réelle demande de la part des clients (apporter des garanties)
  - La sécurité de plus en plus abordée dans les appels d'offres
  
- Besoin d'un standard international pour rassurer les clients
  - Crédibilité pour attaquer les marchés internationaux





1. ADISTAR EN CHIFFRES
2. POSITIONNEMENT
3. ELEMENTS DECLENCHEURS
- 4. DIFFICULTES / POINTS MARQUANTS**
5. IMPLICATION DES COLLABORATEURS
6. BENEFICES
7. PROCHAINES ETAPES





## Avant la certification

- Identification des actifs
  - Où fixer la limite ?
- Analyse des risques
  - Quelle méthode adopter ?
- Mesures à sélectionner dans le SoA
  - Un minimum à sélectionner
  - A partir de quelle limite un système peut-il être certifié ?
- Indicateurs
  - Quels indicateurs ?
  - Comment les mesurer ?
- Ecriture de procédures « adaptées »
  - Aux collaborateurs
  - Aux changements du SI
- Implication des collaborateurs
  - A la lecture et à l'application des procédures





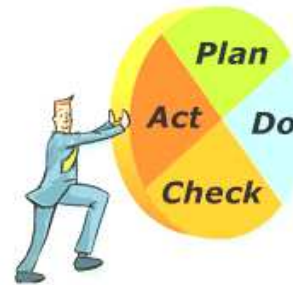
## DIFFICULTES / POINTS MARQUANTS

### Pendant la certification

- Apporter systématiquement des preuves
  - La bonne foi ne suffit pas
- Rassurer les collaborateurs
  - L'auditeur n'est pas là pour piéger !

### Après la certification

- Continuer à appliquer :
  - Les mesures de sécurité
  - Les procédures... et les améliorer
- Respecter le plan de traitement du risque
  - Planification, délais
- Une revue constante de la documentation
  - D'où l'intérêt de procédures adaptées





1. ADISTAR EN CHIFFRES
2. POSITIONNEMENT
3. ELEMENTS DECLENCHEURS
4. DIFFICULTES / POINTS MARQUANTS
- 5. IMPLICATION DES COLLABORATEURS**
6. BENEFICES
7. PROCHAINES ETAPES





## Comment ?

### ■ Expliquer les bénéfices de manière pragmatique

- Donner des exemples en expliquant les risques

### ■ Communiquer :

- Jeux, questionnaires, sorties, organisation d'évènements
- Mémo des bonnes pratiques sécurité
- Mise en place de correspondants sécurité (= responsables)
- Présentations (formations, annonces exceptionnelles)

### ■ Auditer

- Pour rassurer
- Pour identifier les points à améliorer

### ■ Demander que certaines procédures / mesures soient rappelées par la Direction





1. ADISTAR EN CHIFFRES
2. POSITIONNEMENT
3. ELEMENTS DECLENCHEURS
4. DIFFICULTES / POINTS MARQUANTS
5. IMPLICATION DES COLLABORATEURS
- 6. BENEFICES**
7. PROCHAINES ETAPES





## BENEFICES

### Avant

- Objectif à atteindre pour la Direction, les collaborateurs et le RSSI

### Pendant

- Réduire les risques de sinistralité
- Mettre en œuvre un plan de continuité d'activités
- Responsabiliser les collaborateurs
- Légitimité de la Sécurité : un but à atteindre
- Structurer la méthode de travail





## BENEFICES

### Après

- Présenter un gage de confiance à nos clients et à nos partenaires
- Conformité aux exigences légales pour la qualité du SI et aux processus de CI (CNIL)
- Permet de générer des budgets pour les chantiers induits d'amélioration (tout en maîtrisant les couts)
- Disposer d'un langage commun
- Bénéficier d'un argument concurrentiel
- Valorisation
  - du business
  - de la valeur de l'entreprise





1. ADISTAR EN CHIFFRES
2. POSITIONNEMENT
3. ELEMENTS DECLENCHEURS
4. DIFFICULTES / POINTS MARQUANTS
5. IMPLICATION DES COLLABORATEURS
6. BENEFICES

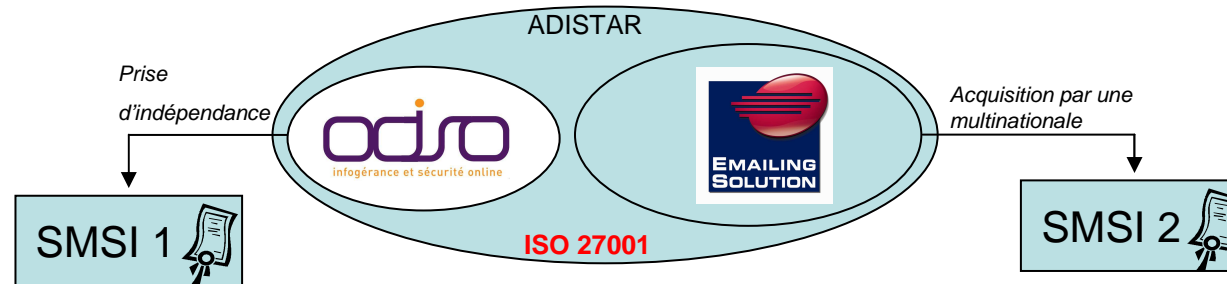
**7. PROCHAINES ETAPES**





## PROCHAINES ETAPES

### Changement d'organisation depuis le 02/05/07



- Actuellement Odiso est prestataire de service pour EMS
  - SMSI à actualiser car indépendance totale entre Odiso et EMS
  
- SMSI distincts qui vont naître de cette séparation
  - 2 SMSI
  - 2 certificats
  - 2 audits de suivi
  
- Réduction du périmètre des 2 SMSI
  - Permet de se recentrer sur le métier de chacun





## QUESTIONS

***Merci de votre attention***

