



**alTran**  
OUEST

**La boîte à outils ISO 27001** : *retour d'expérience sur l'utilisation de l'ISO27001 pour la prise en compte de la sécurité dans l'externalisation de prestations informatiques.*



Ludovic JAMART – Consultant Sécurité

 ISO 27001:2005 Lead Auditor

**Club 27001 – Jeudi 17 janvier 2008.**

**VOYAGEURS FRANCEUROPE**  
DIRECTION DU SYSTEME D'INFORMATION VOYAGEURS

donner au train des idées d'avance



# Sommaire

1. Présentation de l'entreprise
2. Contexte
3. Objectifs
4. Description de la démarche
5. Bilan
6. Perspectives

# 1. Présentation de l'entreprise

- **Opérateur ferroviaire français**
- **Branche Voyageurs France Europe (VFE)**
  - Trois transporteurs à longue distance :
    - TGV France
    - Corail
    - Europe
  - Plusieurs types de filiales :
    - commercialisation : Voyages-sncf.com, Rail Europe,...
    - transport européen voyageurs : Lyria, Elipsos Int., Artesia, Eurostar Group, Thalys Int., ...
    - services : Sysrail Data, CRM Services, iDTGV,...
    - gares : A2C, Parvis
- **Quelques chiffres (2006) :**
  - 130 millions de voyages par an,
  - 600000 dossiers voyage créés par jour,
  - 6 Milliards d'euros de CA.
- **DSIV (Direction du Système d'Informations Voyageurs)**
  - Système central de réservation et de distribution,
  - Un SI complexe, interdépendant et de + en + vital,
  - Un SI orientée vers la distribution et les services.

## 2. Contexte

- De plus en plus de prestations de développement et de Tierce Maintenance Applicative sont externalisées chez des prestataires externes (français...pour le moment).  
↳ *Les frontières du Système d'Information s'étendent.*
- Le choix des prestataires se fait par rapport à des critères tels que l'expertise, la taille critique, ou encore la notoriété. Il est réglementé par le processus « contrat cadre » régi par la Direction des Achats.  
↳ *Centre de compétences / centre de services.*
- Cependant, la confiance (au sens de la maturité dans les pratiques de sécurité de l'information) n'est pas un critère de sélection et reste difficile à évaluer (pas de certification sécurité par exemple).  
↳ *Comment garantir la sécurité du Système d'Information externalisé ?*

### 3. Objectifs

- **Disposer d'une assurance** dans la sécurité des prestations externalisées.
- **Avoir la garantie d'une gestion pérenne de la sécurité** des prestations externalisées.
- **Suivre dans le temps le niveau de sécurité** de la prestation externalisée.
- **Répondre au besoin de visibilité et de confiance** souhaité de la part de la direction dans les prestations externalisées.

## 4. Description de la démarche (1/6)

### 1. Etat des lieux des pratiques d'externalisation de prestations informatiques :

- Focus sur la spécification des « besoins de sécurité »
- Identification des points forts et des points faibles,
- Proposition de solution.

### 2. Définition d'un cadre méthodologique :

- Pour la prise en compte de la sécurité dans l'externalisation des prestations informatiques,
- L'audit sécurité des prestations informatiques externalisées.

### 3. Expérimentation :

- Un cas de prise en compte de la sécurité,
- Un cas d'audit sécurité.

## 4. Description de la démarche : étape 1 (2/6)

### PLAN

- Visite préalable et interview du prestataire,
- Analyse de risques,
- Rédaction d'un Plan d'Assurance Sécurité.

DSIV initie la démarche de prise en compte de la sécurité :

- **Définition du périmètre**
  - Inventaire des actifs (serveurs, postes de développement, locaux, équipes de développement,...)
  - État des lieux sécurité du prestataire,
- **Analyse de risques** des applications externalisées,
- **Validation de la direction** du projet des risques identifiés,

### Contractualisation

- Définition d'un **Plan d'Assurance Sécurité (PAS)**
  - Rôles et responsabilités des acteurs,
  - Contrôles/mesures issues de l'ISO 27002 et des directives de la PSSI SNCF.
- **Sensibilisation et accompagnement** du prestataire sur l'application du PAS,
- **Signature du PAS par le DSI** et son homologue chez le prestataire.

## 4. Description de la démarche : étape 2 (3/6)

DO

- Application du PAS par le prestataire,
- Communication périodique d'indicateurs de sécurité opérationnels.

### Le prestataire met en oeuvre le PAS :

- **Application et exploitation de mesures techniques:**
  - Sécurité physique des locaux,
  - Gestion des anti-virus et correctifs de sécurité,
  - Sauvegarde et restauration,
  - Gestion des accès et habilitations,
  - Cloisonnement réseau,
  - ...
- **Rédaction de procédures:**
  - D'exploitation (gestion des comptes d'accès, sauvegarde, ...)
- **Sensibilisation du personnel:**
  - Charte d'utilisation des ressources informatiques,
  - Engagement de confidentialité, ...
- **Communication périodique d'indicateurs de suivi:**
  - Mise à jour anti-virus,
  - Tests de restauration,
  - Revue des accès et habilitations, ...

## 4. Description de la démarche : étape 3 (4/6)

### CHECK

- Audit du prestataire,
- Définition d'un plan d'actions éventuel en fonction des écarts constatés.

La DSIV audite la conformité du prestataire au PAS :

- **Audit annuel du prestataire :**
  - Selon les termes du PAS (clause d'audit et exigences de sécurité),
  - Collecte de preuves en fonction des points de contrôle,
  - Analyse des écarts.
- **Définition d'un plan d'actions en fonction des écarts constatés :**
  - Remarques (écart mineur)
  - Risques (écart majeur).

*Dans un souci d'indépendance, la règle suivante a été définie au sein de DSIV:  
« celui qui audite le PAS ne doit pas être celui qui l'a écrit ».*

## 4. Description de la démarche : étape 4 (5/6)

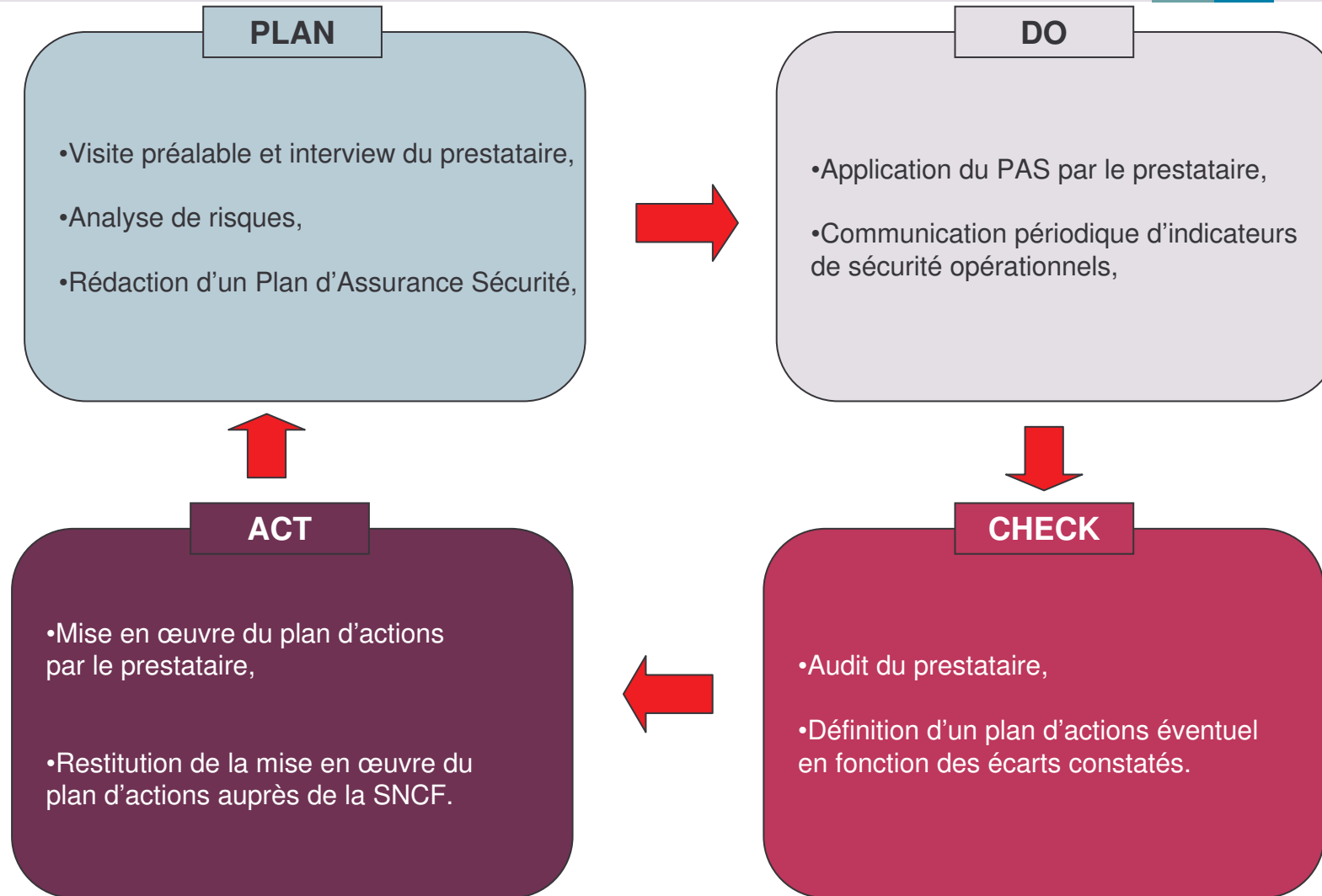
### ACT

- Mise en œuvre du plan d'actions par le prestataire,
- Restitution de la mise en œuvre du plan d'actions auprès de la SNCF.

Le prestataire applique le plan d'actions :

- Mise en œuvre des mesures de correction et d'amélioration,
- Information sur l'avancement et l'application effective des mesures.
- Une mise à jour du Plan d'Assurance Sécurité peut être opérée en fonction des événements survenues durant l'année (ex : modification du périmètre de la prestation, modification de l'architecture technique du prestataire,...).

## 4. Description de la démarche (6/6)



## 5. Bilan

### *Ce qui a été fait :*

- Définition d'une méthodologie PAS formalisée avec documents types,
- Définition d'une méthodologie d'audit formalisée avec documents types,
- Expérimentation sur un centre de services et un centre de compétences.

### ✓ **Apports ou gains obtenus**

- Une démarche basée sur **quatre étapes structurées, formalisées, dépendantes et systématiques** grâce à l'ISO 27001.
  - « Pas de risque d'oubli, on retombe toujours sur nos pieds »
  - L'ISO 27001 a permis de faciliter la définition de la démarche grâce au modèle incontournable, exhaustif et rigoureux de la norme.
- Une confiance mesurable des prestations externalisées.

### ✗ **Difficultés rencontrées**

- Un fort accompagnement nécessaire auprès des prestataires, cependant un investissement « gagnant gagnant ».
- Prise en compte de la dimension juridico-contractuelle qui limite la marge de manoeuvre.

## 6. Perspectives

- Systématisation de la démarche avec une caution «achats » (travail conjoint avec la Direction des Achats, contrat cadre),
- Généralisation de la démarche dans les autres DSI du groupe,
- Évolution vers une exigence de certification 27001 comme critère de choix du prestataire externe.

*Convaincre de l'exigence ISO 27001 par l'ISO 27001.*



Fin

Des questions, des remarques :

[ludovic.jamart@altran.com](mailto:ludovic.jamart@altran.com)