



we secure e-business

# EBIOS et les PSI

**Club EBIOS**

**Retour d'expérience**

**16 Mars 2004**

**JL Allard**

## **Pour des applications, des systèmes, des services, des départements d'affaire, des entreprises complètes:**

des politiques de sécurité des S.I.

des politiques de sécurité de l'information

des politiques de sécurité

et des politiques de sécurité de systèmes et réseaux.

## **+ Des plans d'action**

### **Situation:**

Informations à différents niveaux, différentes applications à exigences variables.

### **Exigence:**

Résultats rapides

## **Des informations de haut niveau**

Gestionnaires d'affaires ou de processus

Responsables techniques

Responsables sécurité

## **Des informations sur les fonctions et processus d'entreprise**

Niveau 'business'

Niveau 'technique'

## **Des 'synthèses'**

Business - technique

Processus - systèmes différents

Différentes approches et conceptions

## **Etape 1: Etude du contexte (1 jour)**

Etude rapport annuel

Discussions sur les 'Business Processes'

Détermination et sélection des 'Impacts Majeurs'

Détermination des contraintes

Préparation des 'modèles' sur les BP ou systèmes

- **Eléments non-techniques**

Analyse des risques 'A froid'

## **Etape 2: Etude des besoins de sécurité**

## **Etape 3: Etude des risques**

## **Etape 4: Objectifs de sécurité**

## **Etape 5: Exigences de sécurité**

## **Etape 1: Etude du contexte**

## **Etape 2: Etude des besoins de sécurité (1/4 jour)**

Vérification du modèle

+ **Eléments techniques**

+ **Eléments 'critiques'**

Pour chaque BP, système, application

**Les 'trois partenaires' en même temps (UNE réponse)**

**Indisponibilités 'courtes' et 'longues'**

Synthèse des BP/applications :

**Base commune**

**Variances = mesures spéciales**

## **Etape 3: Etude des risques**

## **Etape 4: Objectifs de sécurité**

## **Etape 5: Exigences de sécurité**

**Etape 1: Etude du contexte**

**Etape 2: Etude des besoins de sécurité**

**Etape 3: Etude des risques (1/4 jour)**

Pour chaque BP, système

Simplifié

Scénarios

Niveaux (potentialité, impact, risque)

Synthèse

Scénarios 'communs'

Niveaux 'communs'

**Etape 4: Objectifs de sécurité**

**Etape 5: Exigences de sécurité**

## **Etape 1: Etude du contexte**

## **Etape 2: Etude des besoins de sécurité**

## **Etape 3: Etude des risques**

## **Etape 4: Objectifs de sécurité (1 à 3 jours)**

Comparaison 'besoins de sécurité - risques'

'Compromis' opérations - sécurité

Analyse de la norme de référence (BS7799, loi, etc.)

Objectifs communs et 'spécifiques'

Signification des 'valeurs'

**Besoin, potentialité, impact, risque**

Stratégie

**Objectifs, prioritisation, idée de 'manoeuvre'**

... Ce que l'on demande

## **Etape 5: Exigences de sécurité**

**Etape 1: Etude du contexte**

**Etape 2: Etude des besoins de sécurité**

**Etape 3: Etude des risques**

**Etape 4: Objectifs de sécurité**

**Etape 5: Exigences de sécurité (2 à 5 jours)**

Traduction des objectifs  
génériques et finaux

... en termes 'actifs', proportionnés et modulés

**Pour contrer les risques**

**Pour combler les besoins**

Trois axes

Les TIC

La Sécurité (hors TIC)

Le personnel

Le 'plan d'action'



## **Formalisation des questions 'Contexte'**

- Modèle (matrice fonctions/entités avec indication de criticallité)
- Impacts majeurs (importance relative)
- Valeur des systèmes et informations
- Valeur du 'processus' (ou des applications)
- Impact sur l'extérieur de l'entreprise
- Contraintes

## **Les besoins**

- Le 'temps d'indisponibilité maximal acceptable'
- La perte maximale d'information

**... Outils pour le "BIA"  
dans le cadre de 'la continuité des affaires'**

## **L'ordre des choses**

- 1° Survie de l'entreprise, ses processus critiques
- 2° La vie de tous les jours, la sécurité

**Les possibilités 'Continuité des affaires'**

**Les informations 'Récupération après désastre'**

**La nouvelle version**