EBIOS & 27001

C. Rubat du Mérac
Enseignante IUT2

CLUSIR 14/12/2009

Sécuriser le SI d'une société : les freins

- Au niveau général
  - pléthore de lois, règlements, normes
- Individuellement :
  - Naïveté, conscience du risque insuffisante
- En Entreprise :
  - La sécurité des systèmes d'information : parent pauvre des budgets
  - Pourtant :
    - Techno de l'information ➔50% des investissements productifs des entreprises
  - Constat :
    - ☹ culture Système d'information (processus métier) faible
    - ☹ la culture « risque » des Directeurs de SI français insuffisante
    - ☹ l'utilisation de méthode de gestion du risque est encore loin d'être systématique

Méthode et Normes : Pourquoi

- Actuellement (si une sécurisation existe)
  - limitée au systèmes informatiques en place
  - responsabilité technique
  - Sauvegardes, filtres réseaux, antivirus, antispam, …
- Pannes => gestion réactive (dans l'urgence)
  - Solutions inadaptées
  - Remises en causes fréquentes

➔ Méthode : guide d'une réflexion préalable raisonnée sur les véritables vulnérabilités

EBIOS : une méthode d'analyse et de couverture du risque

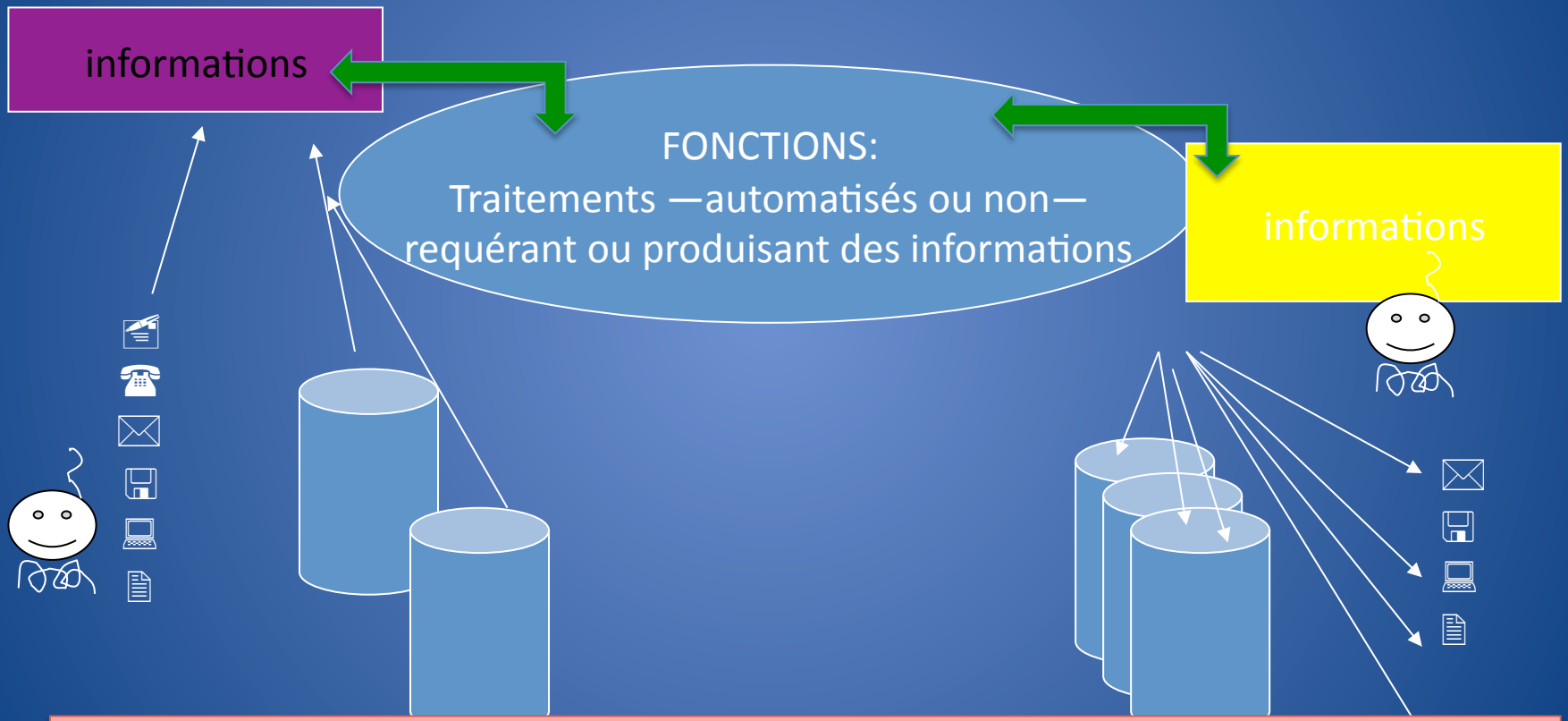
- EBIOS V2 : norme ISO-IEC-17799 /27002 (code de bonnes pratiques)
  - Définir des mesures de sécurités (moyens de couverture)
  - Associées aux exigences de sécurité (niveau de couverture à atteindre)
  - exigences demandées par les objectifs de sécurité (ce qu'on veut protéger)
- Évolution vers ISO-IEC- 27005 : en cours
  - 27005 :
    - normalisation de l'analyse de risque
    - Critères : reproductibilité et comparabilité des évaluations du risque
  - simplification des risques : Éléments redoutés
  - Etude :
    - Périmètre
    - Entités : biens informationnels

EBIOS : le Système d'Information

« ENSEMBLE D'ENTITÉS ORGANISÉ POUR ACCOMPLIR DES FONCTIONS DE TRAITEMENT D'INFORMATION »

- **Fonctions : opérations associées aux « métiers » de l'entreprise**
- **Entités : constituants techniques ou organisationnels**
  - **Matériels, logiciels, infrastructures**

La notion de Système d'information

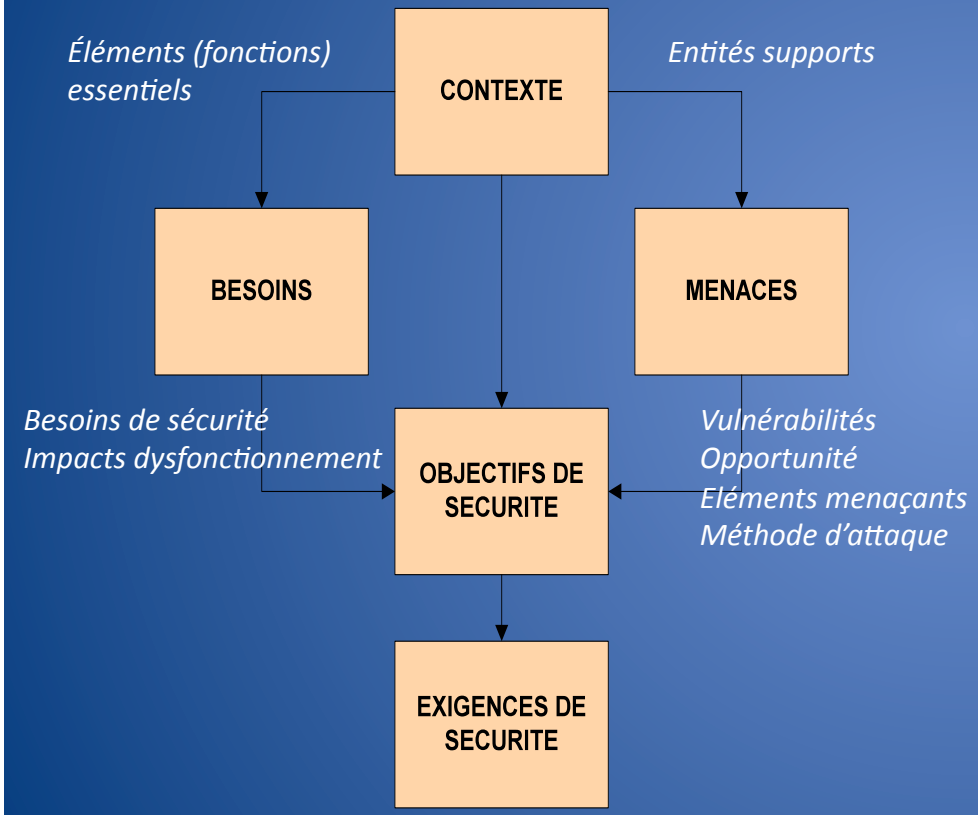


➔Entité : (porteuse des vulnérabilités)

La méthode EBIOS

- Objectif :
  - Protéger l'organisme
  - À travers son fonctionnement global
  - … en maîtrisant les risques
- Base de la méthode :
  - Examiner le contexte SI : organisation , enjeux et objectifs de la société
  - Vue métier : fonctions essentielles /entités support
  - Exposition des entités /vulnérabilités exploitables
  - Objectifs : quelles entités protéger
  - Exigences : la couverture (type et niveau)

EBIOS V2 :
5 modules pour évaluer et couvrir le risque



- Cerner le risque
  - À travers une vue métier du SI:
    - Éléments essentiels (fonctions)
    - Exprimer besoins de sécurité
    - Identifier les menaces et les vulnérabilités exploitables
  - Apprécier son importance
- Que doit-on protéger (objectifs)
- Quel niveau de couverture
  - Le traiter : le refuser
  - Le réduire : optimiser
  - Le différer : assurance
  - L'ignorer : prise de risque

➔PSSI, Schéma directeur SI, Plan de Reprise d'Activité

EBIOS V2 : bons et mauvais points

- Exhaustif : appréciation détaillée du risque
- ☺ Exploitation des résultats: guides pour documents divers
  - Politique SSI
  - Un schéma directeur SI : Moyens à mettre en face des exigences
  - Plan d'action : mise en œuvre
  - PRA
  - …
- ☹ Mais : compléter par d'autres
  - Audit des besoins
  - TDB
  - Évaluation de la SSI
  - Formations et sensibilisation

EBIOS V2 : Ce qui me manque encore

- La notion de périmètre :
  - Alléger le démarrage
  - Adapter ensuite : démarche progressive
- Assurer le suivi de l'exploitation des dispositifs techniques :
  - Tableau de bord
- Gérer les évolutions nécessaires :
  - Évolutions dans l'organisme :
    - Restructuration ou évolution de l'activité
  - Gestion de crise :
    - risque résiduel : sous-estimé, non couvert
    - Un risque non recensé : oubli ou évolution de la société

La norme 27001

- Définit la démarche a suivre pour élaborer et mettre en place un SMSI
  - Périmètre
  - pilotage
  - Analyse et évaluation de risques : recours à 27002
    - Identification, analyse et évaluation du risque, couverture
  - Indicateurs
  - Engagement politique dans la démarche : charte d'applicabilité
  - certification

➔ Sans obligation sur le choix de la méthode

ISO 27001 et ISO 27002

	27001	27002
Système de management SI	OUI	NON
Modèle PDCA	OUI	NON
Actions à entreprendre	On DOIT (ANNEXE A.9.2.2)	Il convient 2 (CH 9.2.2)
Obligation	Clauses (chapitres) 4 à 8	aucune
Certification	Possible (personnes ou SMSI)	Impossible : Aucun sens

D'après Alexandre Fernandez – Toro (HSC) : Management de la sécurité de l'information, Implémentation ISO 27001

Complémentarité des deux normes et choix de méthode

ISO 27001

OJECTIFS :

À ATTEINDRE

obligatoires

Clauses 4à 8

Annexe A :

Mesures à mettre en œuvre

ISO 27002

Conseils de mise en œuvre

Clause 5 à 15

EBIOS

SMSI➔ PDCA et méthode EBIOS