



### EBIOS et normes internationales

Présentation pour le colloque ARS sur la gouvernance de la sécurité des systèmes d'information

7 juin 2011



## Quelques réflexions sur les normes



- Les normes sont avant tout des guides, des recommandations ou des exigences qui visent à assurer la confiance dans un système.
- Elles constituent une aide pour sécuriser les systèmes d'informations

Attention toutefois au piège de la bible, de ses exégètes et de ses intégristes



La sécurité nécessite réflexion, inventivité, que les normes ne doivent pas « tuer »



Application intelligente des normes



## Repartir des fondamentaux (1)



## Qu'est ce que je souhaite protéger ?

Actifs primordiaux ou Patrimoine informationnel

Composante informationnelle

Le système d'information

**Actifs Support** 

Organisation, moyens humains

**Composante humaine** 

systèmes informatiques systèmes de télécommunication, autres

Composante technique

Source : Denis Virole Société Telindus Que cherche-t-on à sécuriser?



## Repartir des fondamentaux (2)



### Comment se protéger ?

Limites des approches par les bonnes pratiques et le tout technique S'intéressent principalement aux actifs supports;

Ne peuvent pas appréhender le risque dans toutes ses dimensions

Approche globale

Nécessité d'appréhender le risque au travers de ses composantes, de sa complexité, de ses évolutions ;

Utilisation de méthode de gestion de risques EBIOS.



## Repartir des fondamentaux (2)



### Pourquoi se protéger ?

- Respect des obligation réglementaires et légales (loi informatique et liberté, LCEN, RGS),
- Évolution des menaces (attention toutefois aux raisonnements basés sur la menace),
- → Modernisation de l'administration,
- Conception de service public : la sécurité n'est pas une fin en soi mais un moyen qui concourt à la confiance entre usagers et administration.



Apport indéniable du RGS



## Repartir des fondamentaux (3)



### Approche analytique proposée par EBIOS

Actifs informationnel Données et processus

Impact

Potentialité

Événements redoutés
Erreur
Accident
Malveillance

Étude de risque de l'application



Appréciation du risque

(Risque = Impact \* Potentialité)

Objectifs de sécurité

Mesures de sécurité adaptées à l'application et son contexte



Compréhension des composantes du risque

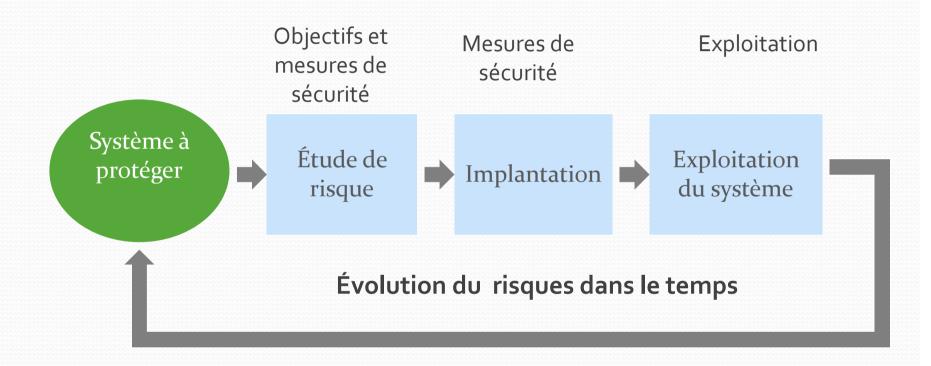


## Repartir des fondamentaux (3)





### Approche dynamique



Compréhension de la nature évolutive du risque



## Repartir des fondamentaux (3)

### Approche globale

approche globale de la sécurité des systèmes d'information Jémarche d'amélioration continue Étude risque pour toutes applications sensibles Système d'information ou application sécurisée Homologation Surveillance et réexamen du risque

Politique de sécurité

choix de produits de confiance

choix de prestataires de confiance

Compréhension du risque dans sa complexité



# Comment utiliser les normes ? Approche boite à outils



### Connaître les normes pour les utiliser

Guide Recommandations

> 27000 Vocabulaire

27002 Les bonnes pratiques

27003 Implémentation

> 27004 Métriques

27005 Gestion de risques

> 27007 Audit

Normes certifiables

15408 Critères communs

> 27001 SMSI

Guides pour l'accréditation ou la certification

17021 Accréditation

27006 Audit SMSI

19011 Audit SMSI

17024 Certification individuelle

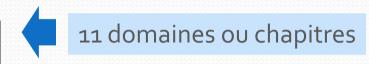


### Norme ISO/IEC 27002



Vue d'ensemble d'une mesure

Domaine	
Sous-domaine:	objectif
Définition de la mesure	la mesure 2
1	
Guide d'implémentation	nentation
Informations	
complémentaires	es







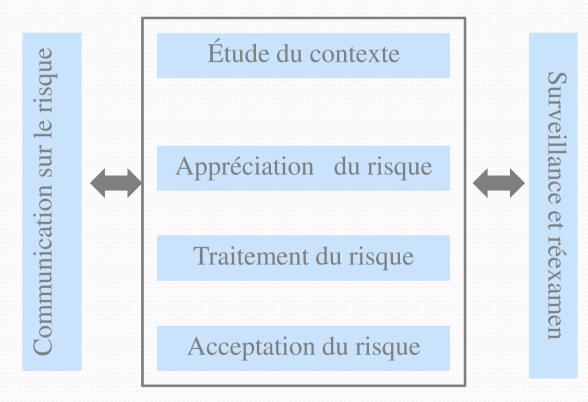
Les mesures portent essentiellement sur les actifs supports

# \$3

## **Utilisation des normes**

### Norme ISO/IEC 27005

- Démarche de gestion de risque
- Vue simplifiée de la démarche 27005



Appréciation du risque sur les actifs informationnels supports



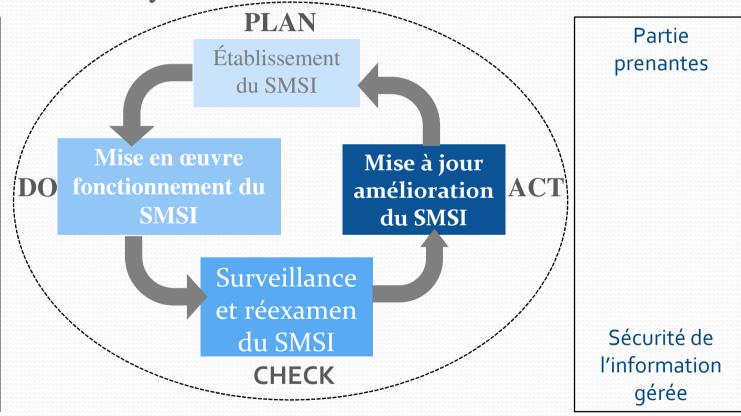
### Norme ISO/IEC 27001

Système de management de la sécurité de l'information

Vue d'ensemble du cycle PDCA

Partie prenantes

Exigences et attentes vis-àvis de la sécurité de l'information



Approche focalisée pour l'essentiel sur les actifs informationnels

## \$

## Utilisation des normes

### Norme ISO/IEC 15408



Critères communs



Vue simplifiée de la démarche de certification



Porte exclusivement sur la composante technique des actifs supports



## Tentative de synthèse

Confiance de l'usager dans les applications mises en œuvre par l'administration

EBIOS, 27005, 27002

Utilisation de produits qualifiés dont critères communs ou CSPN

Rendues obligatoires par le RGS pour les télé services approche globale de la SI

Étude de risque sur les applications sensibles

Confiance de l'usager dans l'administration

Concerne
l'administration dans
son ensemble

Démarche ISO 27005, Adoption de certains principes de la 27 001, PSSI

Préconisée dans le §2.2 du RGS