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

↓

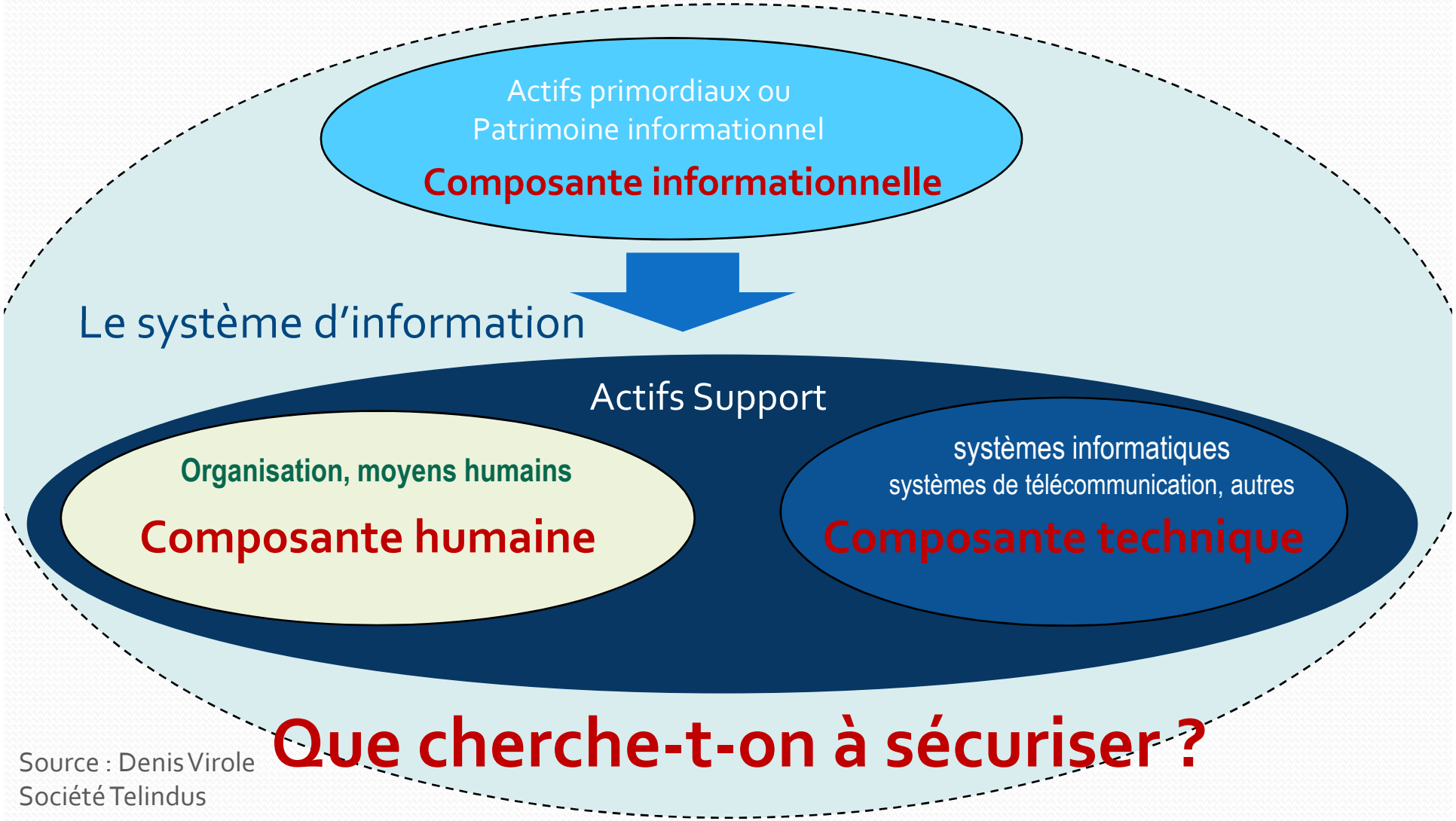
La sécurité nécessite réflexion, inventivité, que les normes ne doivent pas « tuer »

↓

Application intelligente des normes

Repartir des fondamentaux (1)

Qu'est ce que je souhaite protéger ?



Source : Denis Virole
Société Telindus

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)

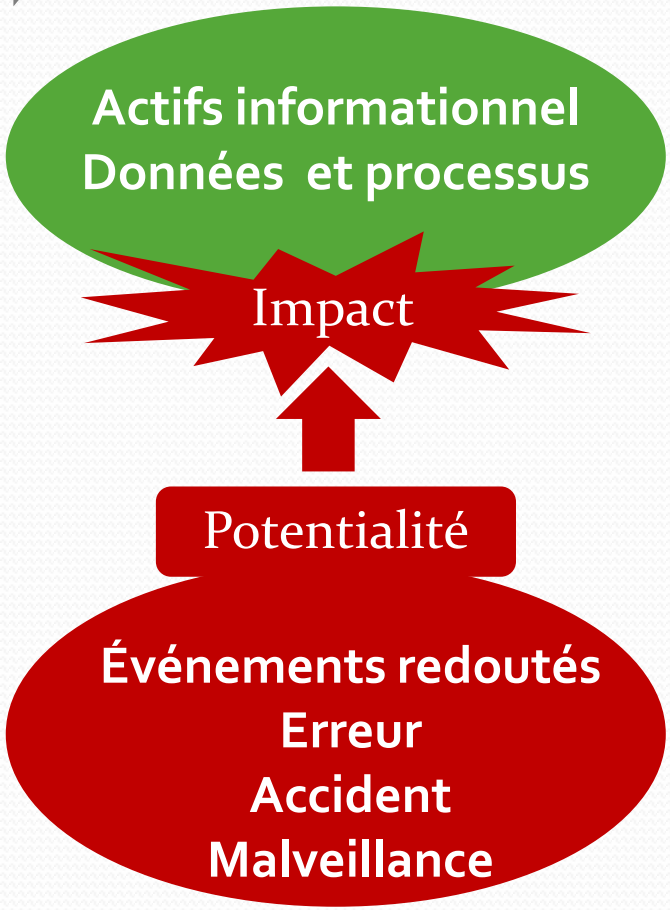
Pourquoi se protéger ?

- 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



Étude de risque de l'application

Appréciation du risque

(Risque = Impact * Potentialité)

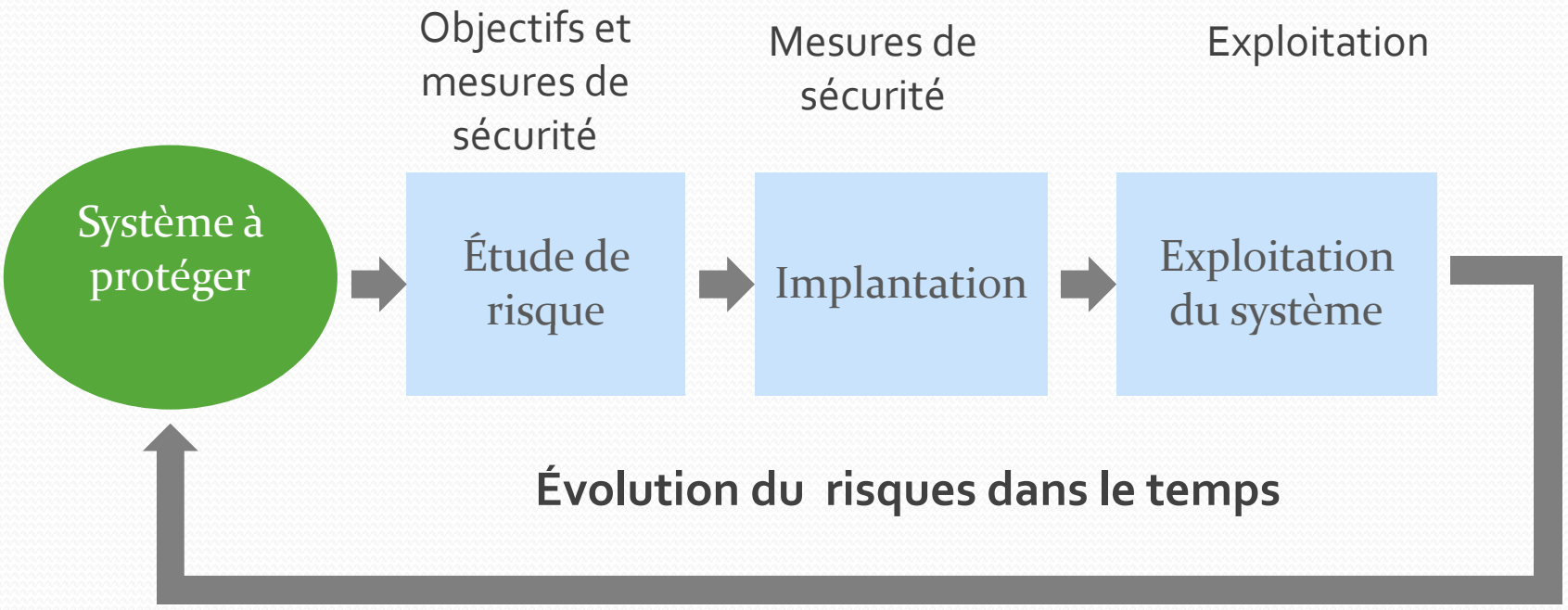
Objectifs de sécurité

Mesures de sécurité adaptées à l'application et son contexte

Compréhension des composantes du risque

Repartir des fondamentaux (3)

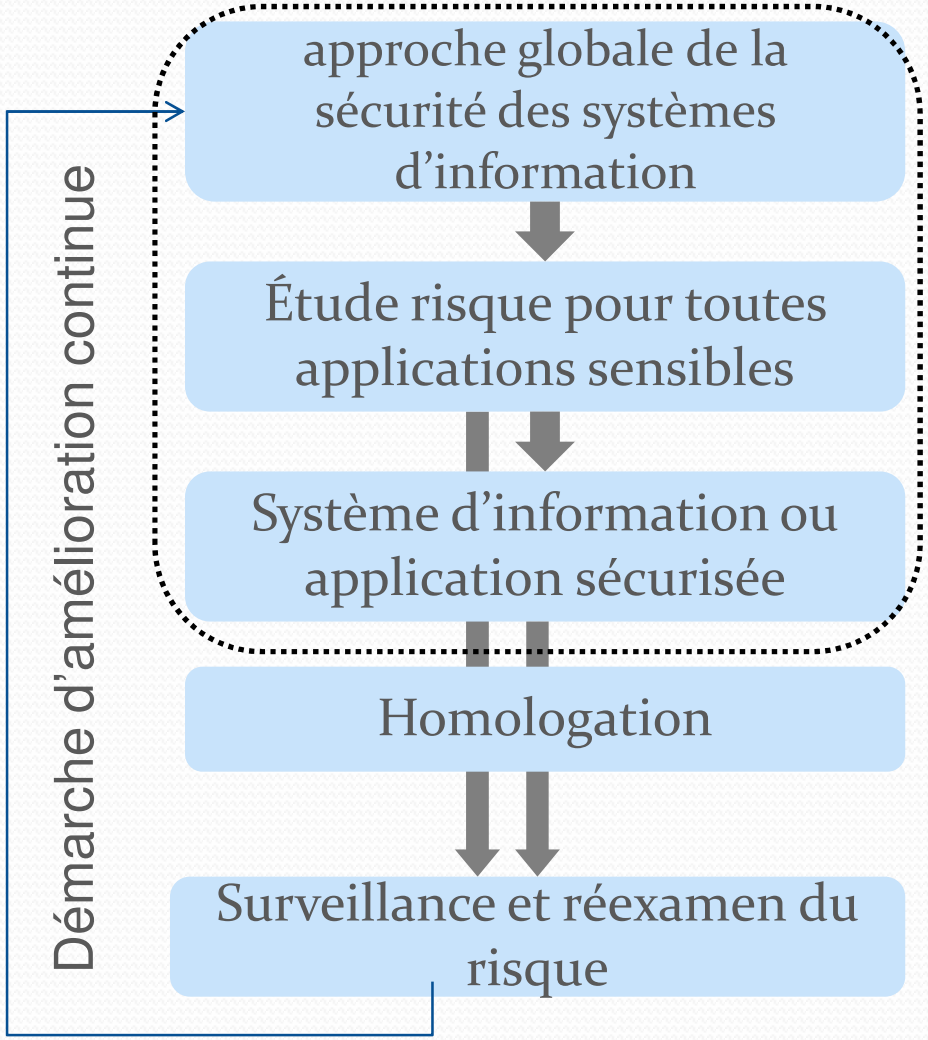
Approche dynamique



Compréhension de la nature évolutive du risque

Repartir des fondamentaux (3)

Approche globale



- Politique de sécurité
- choix de produits de confiance
- choix de prestataires de confiance

Compréhension du risque dans sa complexité

Utilisation des normes

Comment utiliser les normes ?
Approche boite à outils

Utilisation des normes

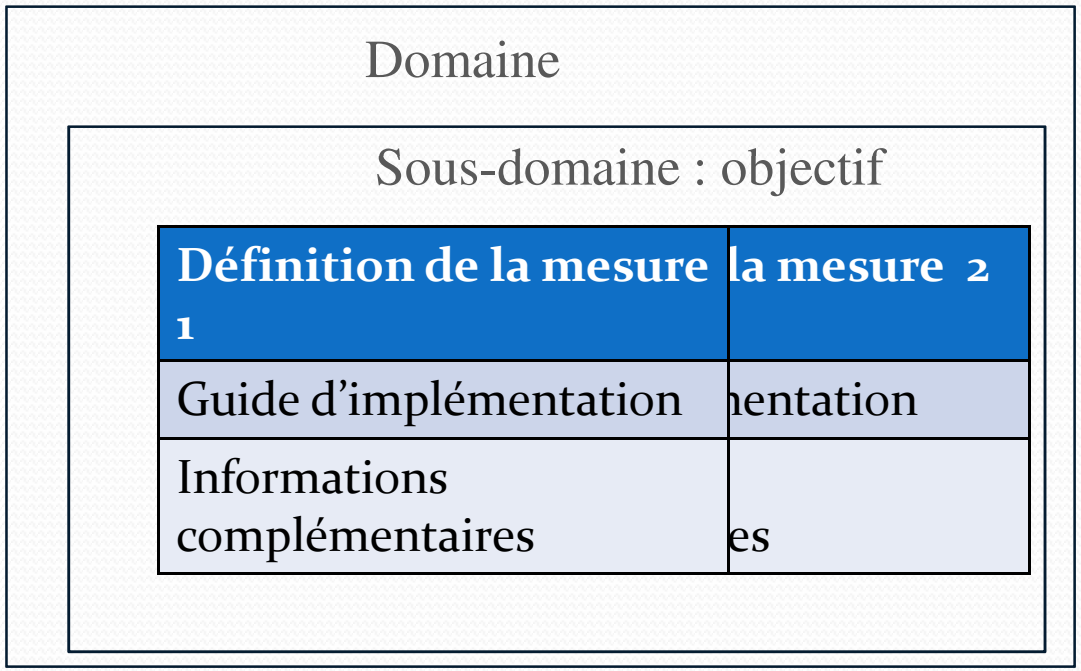
Connaître les normes pour les utiliser

Guide Recommandations	Normes certifiables	Guides pour l'accréditation ou la certification
27000 Vocabulaire		17021 Accréditation
27002 Les bonnes pratiques	15408 Critères communs	
27003 Implémentation	27001 SMSI	27006 Audit SMSI
27004 Métriques		19011 Audit SMSI
27005 Gestion de risques		
27007 Audit		17024 Certification individuelle

Utilisation des normes

Norme ISO/IEC 27002

- Catalogue de 113 mesures réparties en 11 domaines de sécurité
- Vue d'ensemble d'une mesure



11 domaines ou chapitres

Objectif précisé par sous domaine

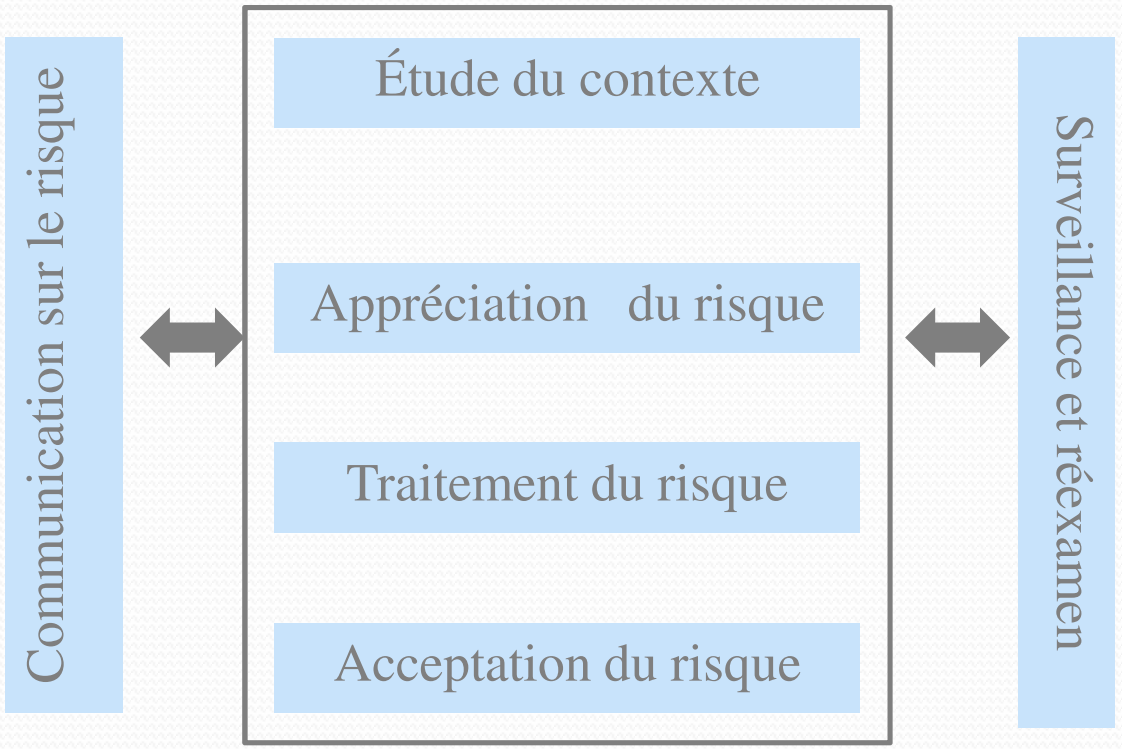
Mesure(s) pour répondre aux objectifs précités

Les mesures portent essentiellement sur les actifs supports

Utilisation des normes

Norme ISO/IEC 27005

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

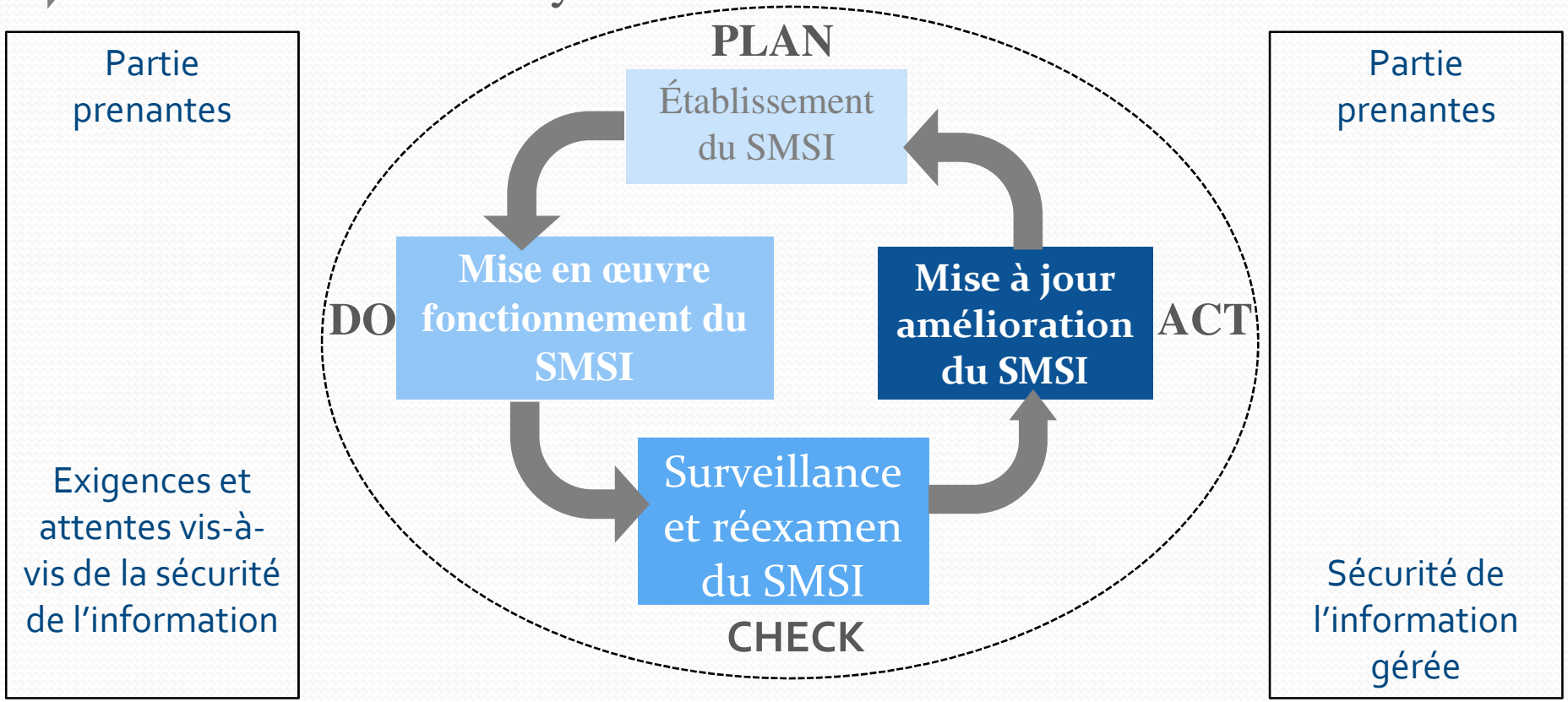


Appréciation du risque sur les actifs informationnels supports

Utilisation des normes

Norme ISO/IEC 27001

- Système de management de la sécurité de l'information
- Vue d'ensemble du cycle PDCA

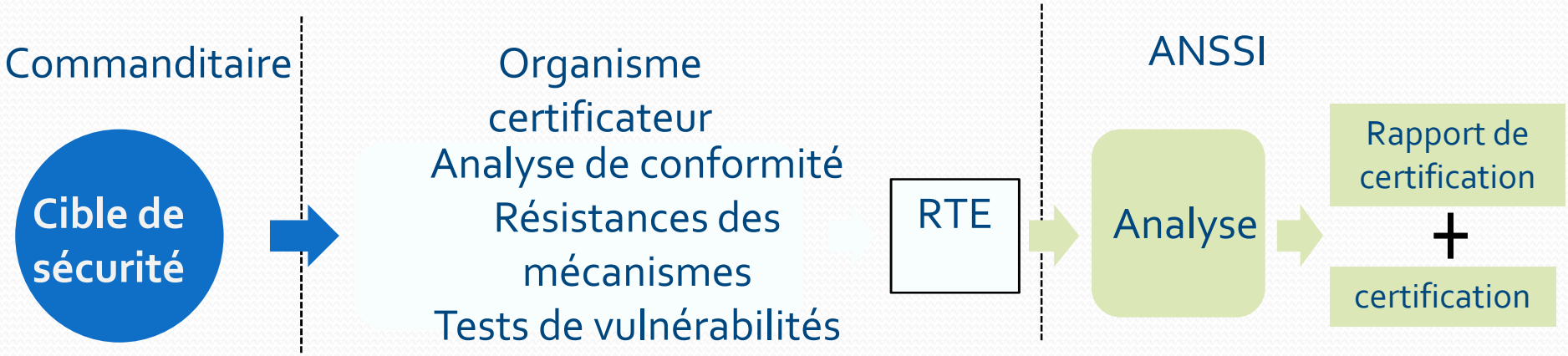


Approche focalisée pour l'essentiel sur les actifs informationnels

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