



**Université Internationale
de Casablanca**

LAUREATE INTERNATIONAL UNIVERSITIES

UNIVERSITÉ RECONNUE PAR L'ÉTAT

Exploitation des systèmes d'information

Pr. IGUER Hajar



INTRODUCTION

Généralités sur la gouvernance des SI

INTRODUCTION

- Les organisations se veulent plus compétitives dans un monde plus exigeant



Réalisation des objectifs



Prévention des risques



Génération des rapports

GOVERNANCE D'ENTREPRISE (GE)

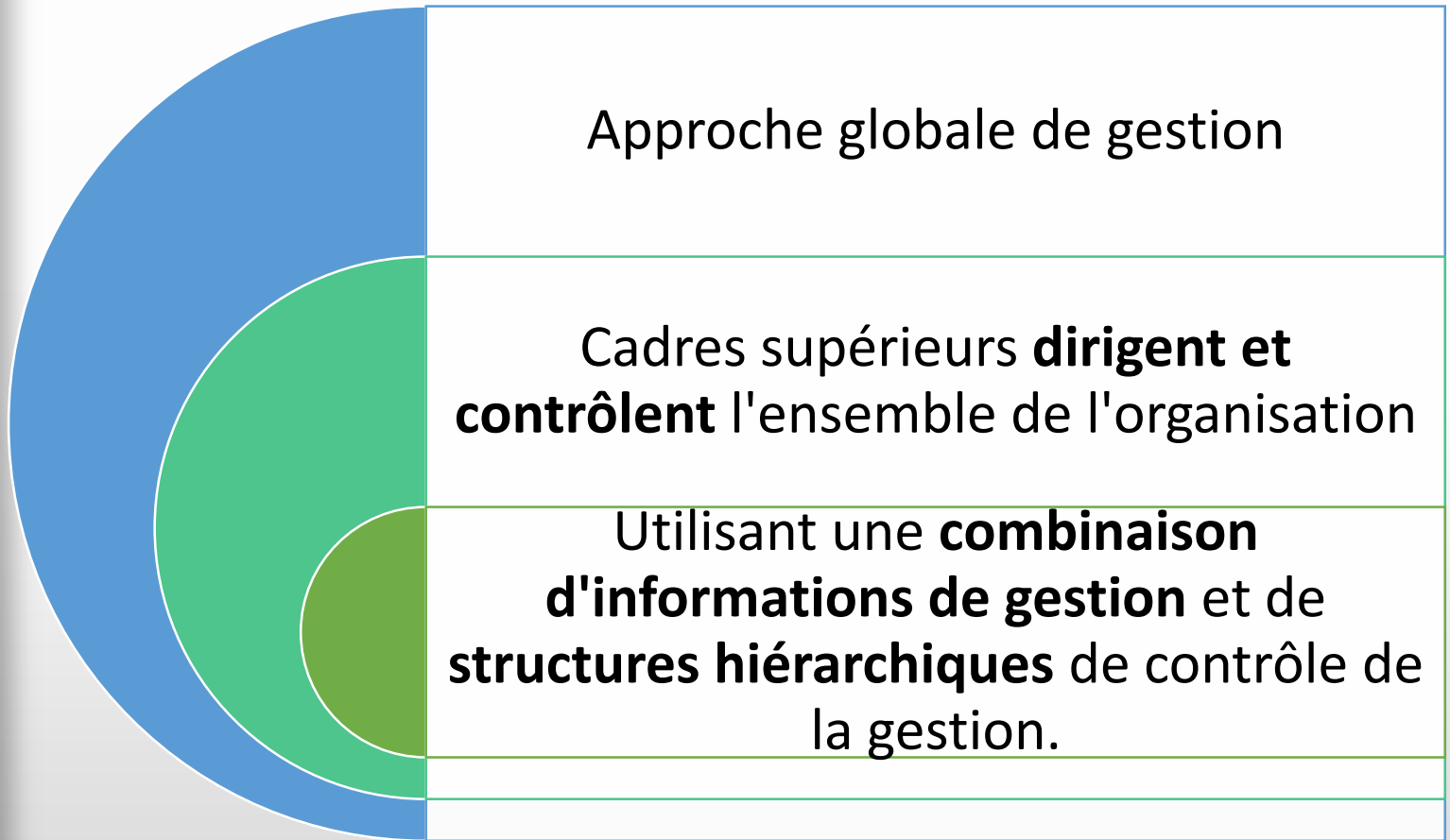
GE se réfère au système par lequel les entreprises sont dirigées et contrôlées

Conseil d'administration est responsable d'assurer l'intégrité de leurs systèmes informatiques

CA doit avoir accès aux informations disponibles en temps opportun

D'où l'importance de générer des rapports de synthèse expliquant l'état de leurs systèmes d'information

GOUVERNANCE



CONFORMITE

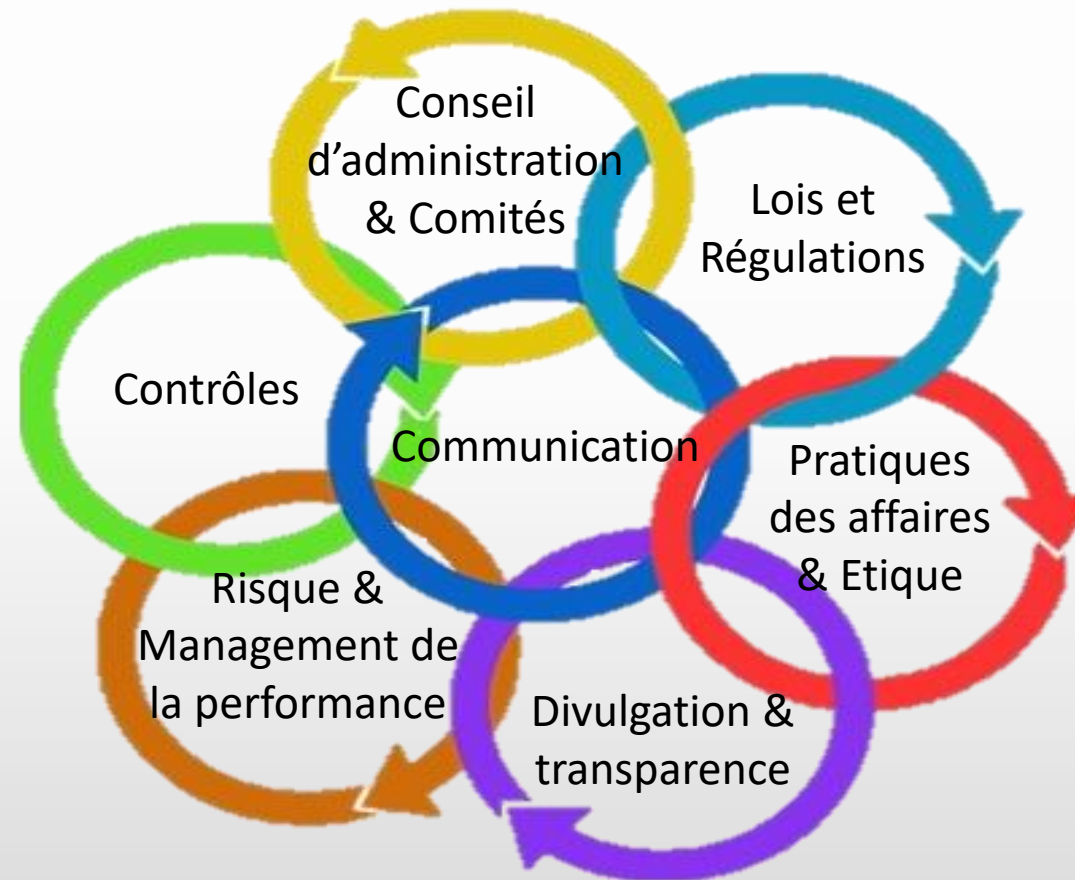


- **Exemple : Loi 09-08**

- Relative à la protection des personnes physiques et morales à l'égard du traitement des données à caractère personnel
- Ce sont des données sensibles qui proviennent à partir de fichier de données ou d'un traitement automatisés ou non automatisés ou mêle des contenus dans des fichiers manuels.

Mise au point au sein d'une organisation qui a été développée en raison d'**interdépendances** entre les trois composantes G,R, et C

GOVERNANCE, RISQUE ET CONFORMITÉ (GRC)



PILIERS DE L'IT GRC

Alignement stratégique

Soutenir l'objectif métier de l'entreprise

Création de la valeur

Optimisation des investissements

Gestion des ressources

Gérer les ressources humaines et technologiques

Gestion des risques

Réduction du risque à un niveau acceptable

Mesure de la performance

Cohérence des systèmes de mesure



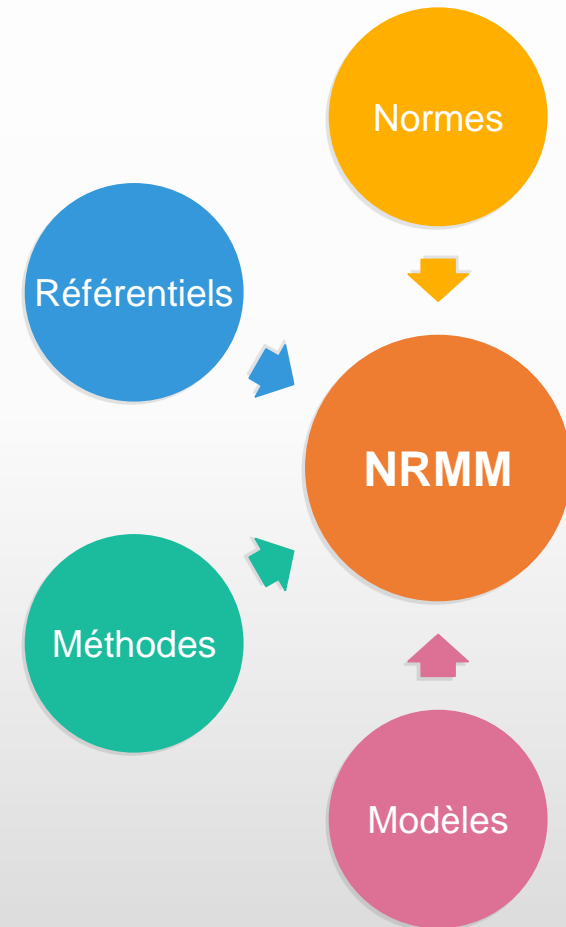
NRMM

Normes : Règlement, ce que dit la loi, voire dans certains cas ce qu'elle impose.

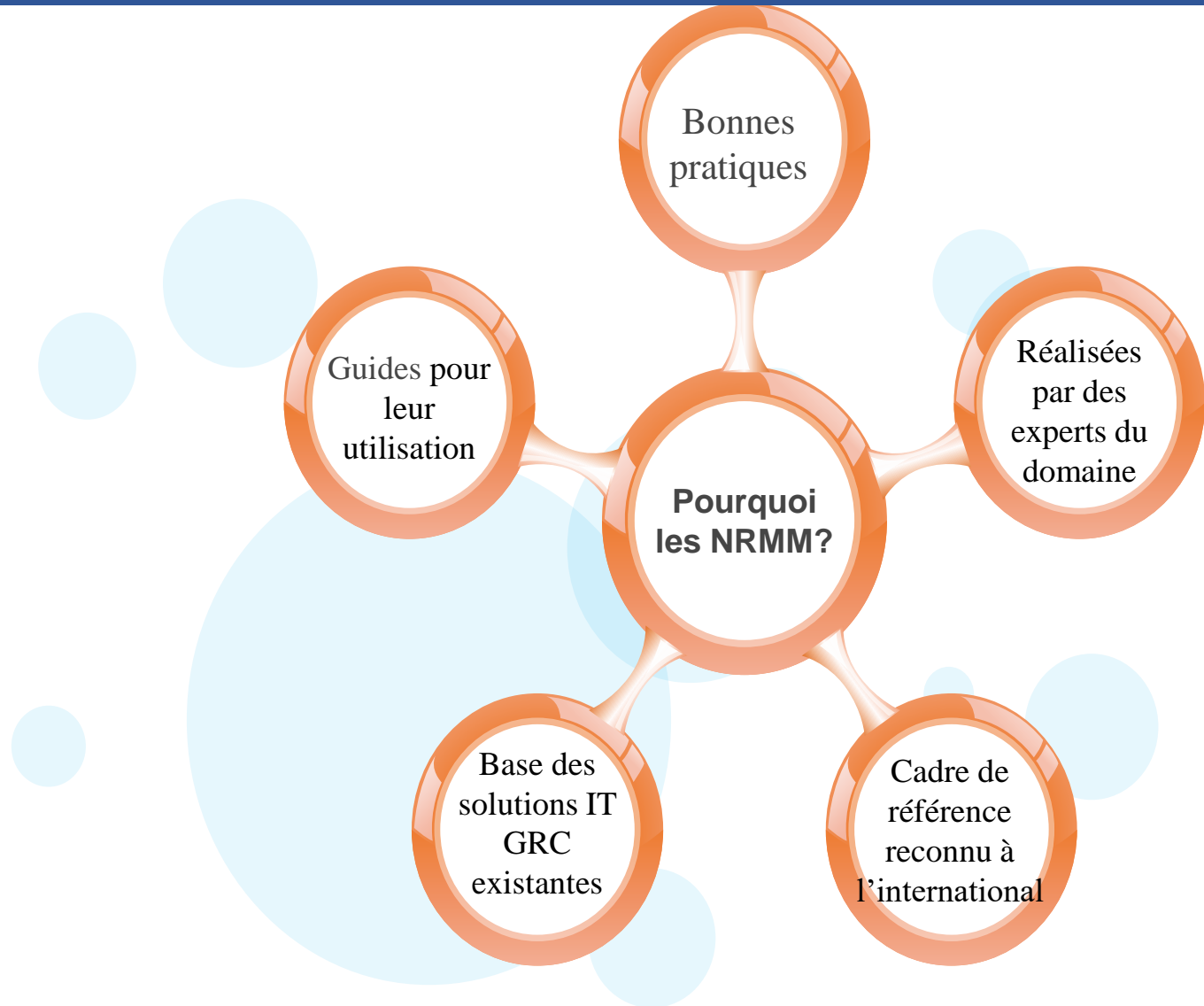
Référentiels : Choix de l'entreprise qui est le plus adapté à son activité et à sa stratégie, avec à la clé une certification soit pour l'entreprise ou un de ses départements.

Méthodes : Bonnes solutions qui permettent à l'entreprise d'aboutir à son objectif.

Modèles : Outils utilisés et reconnus par les professionnels ; ils sont indispensables et complémentaires aux méthodes.



POURQUOI LES NRMM?



NRMM : EXEMPLES



MetricStream

The MetricStream logo, featuring the word "MetricStream" in a white, sans-serif font on a dark blue background.

NORMES ISO 27000

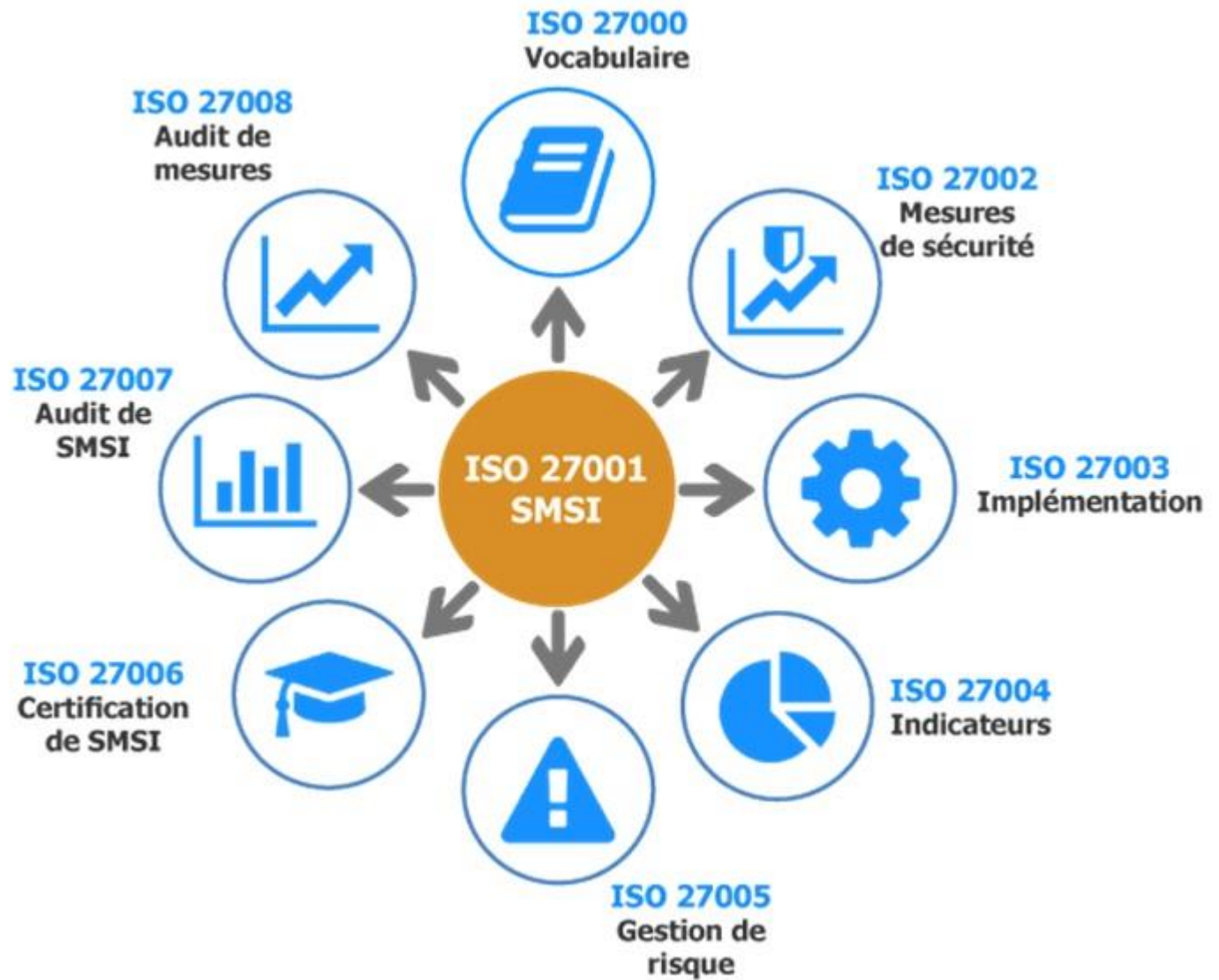


Figure – Normes ISO 27000

- **La norme régit:**

- la conception,
- la mise en œuvre,
- le suivi, l'entretien,
- l'amélioration,
- la certification d'un système de gestion de la sécurité de l'information (SMSI).



**Définition d'une approche
d'évaluation des risques qui
identifie la méthode
appropriée pour définir leurs
critères d'acceptation**

ISO 27005

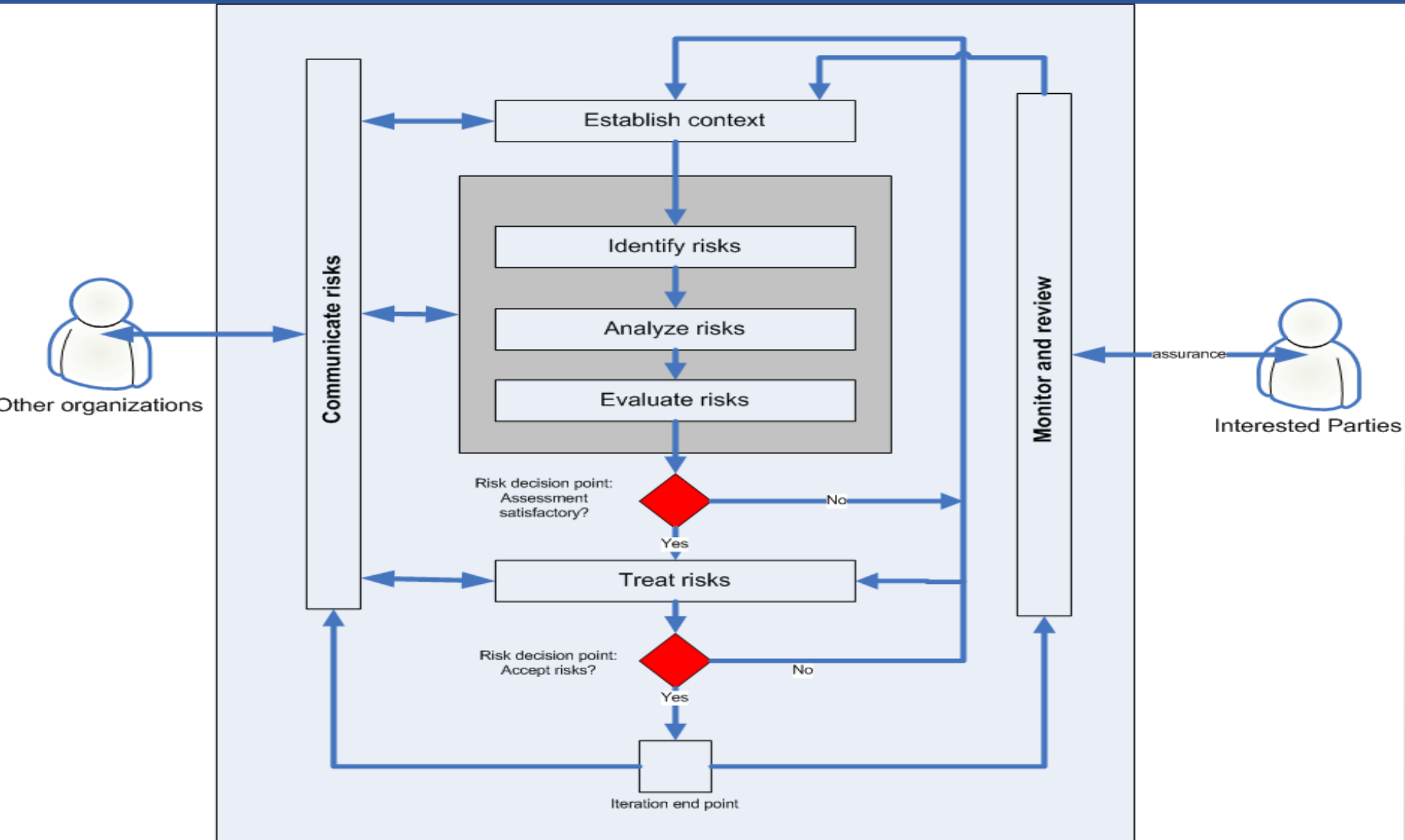


Figure – Processus ISO 2005

APPROCHE PDCA: THE DEMING CYCLE

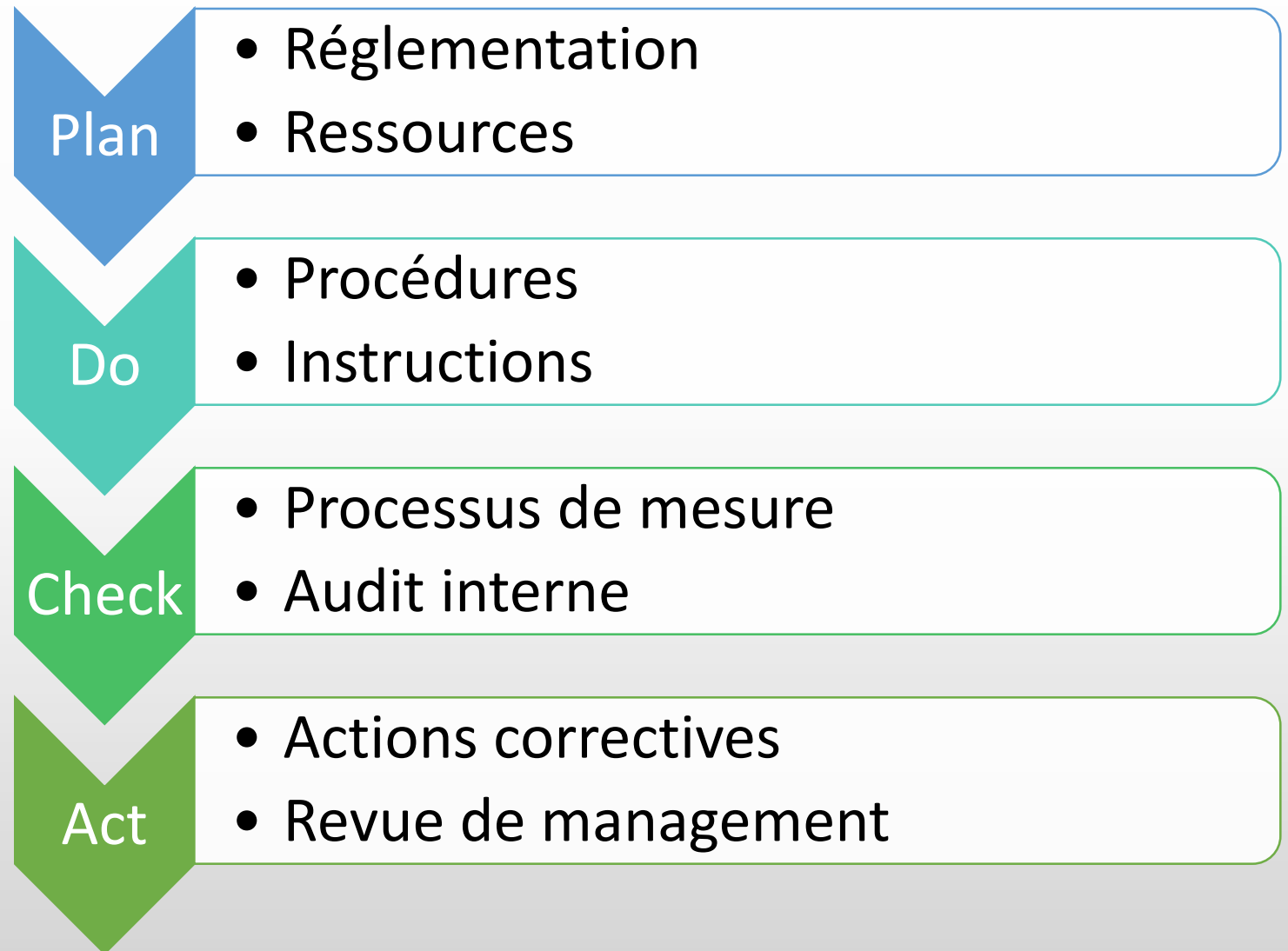


Figure – PDCA – The deming cycle

EXAMPLE : METRICSTREAM

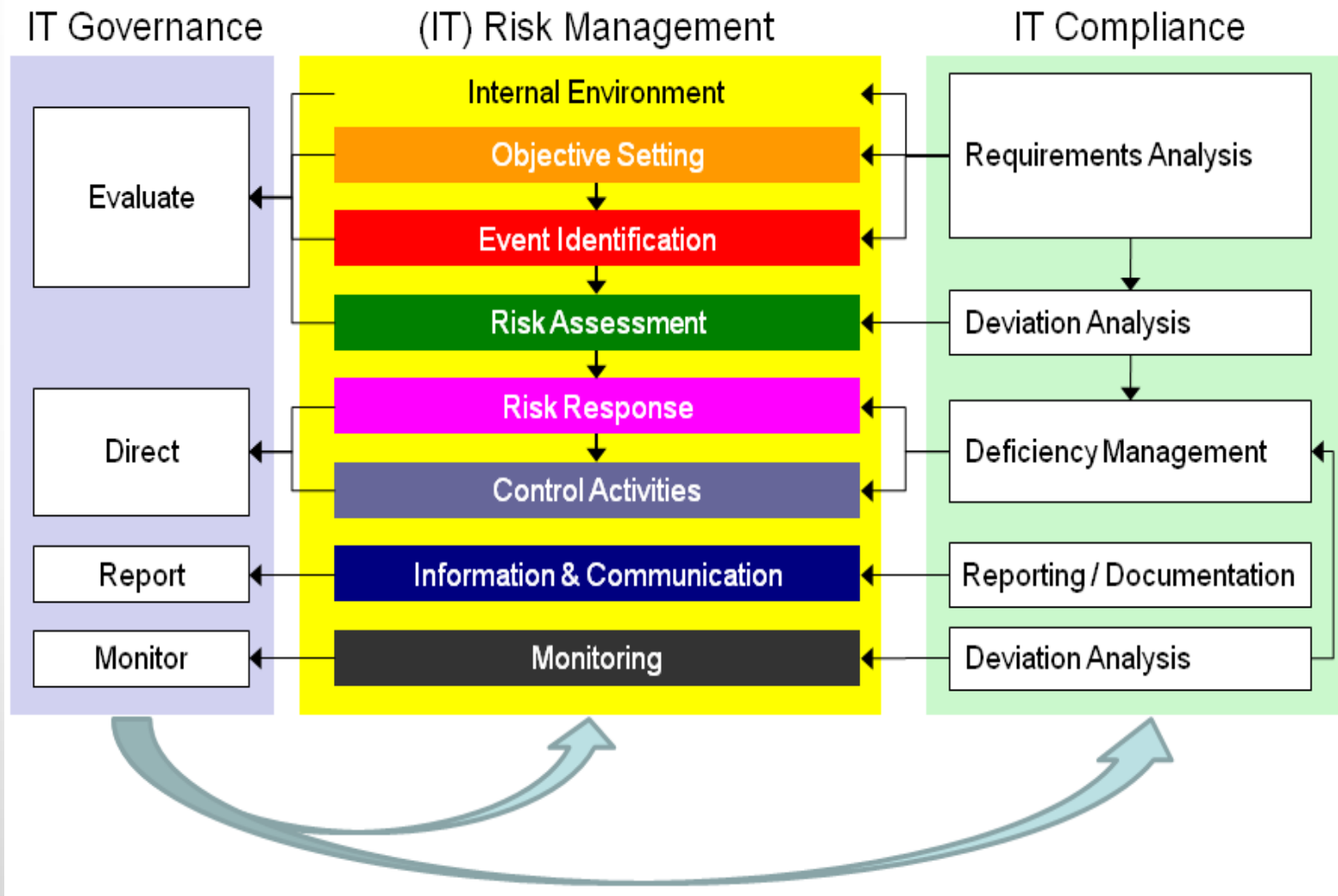
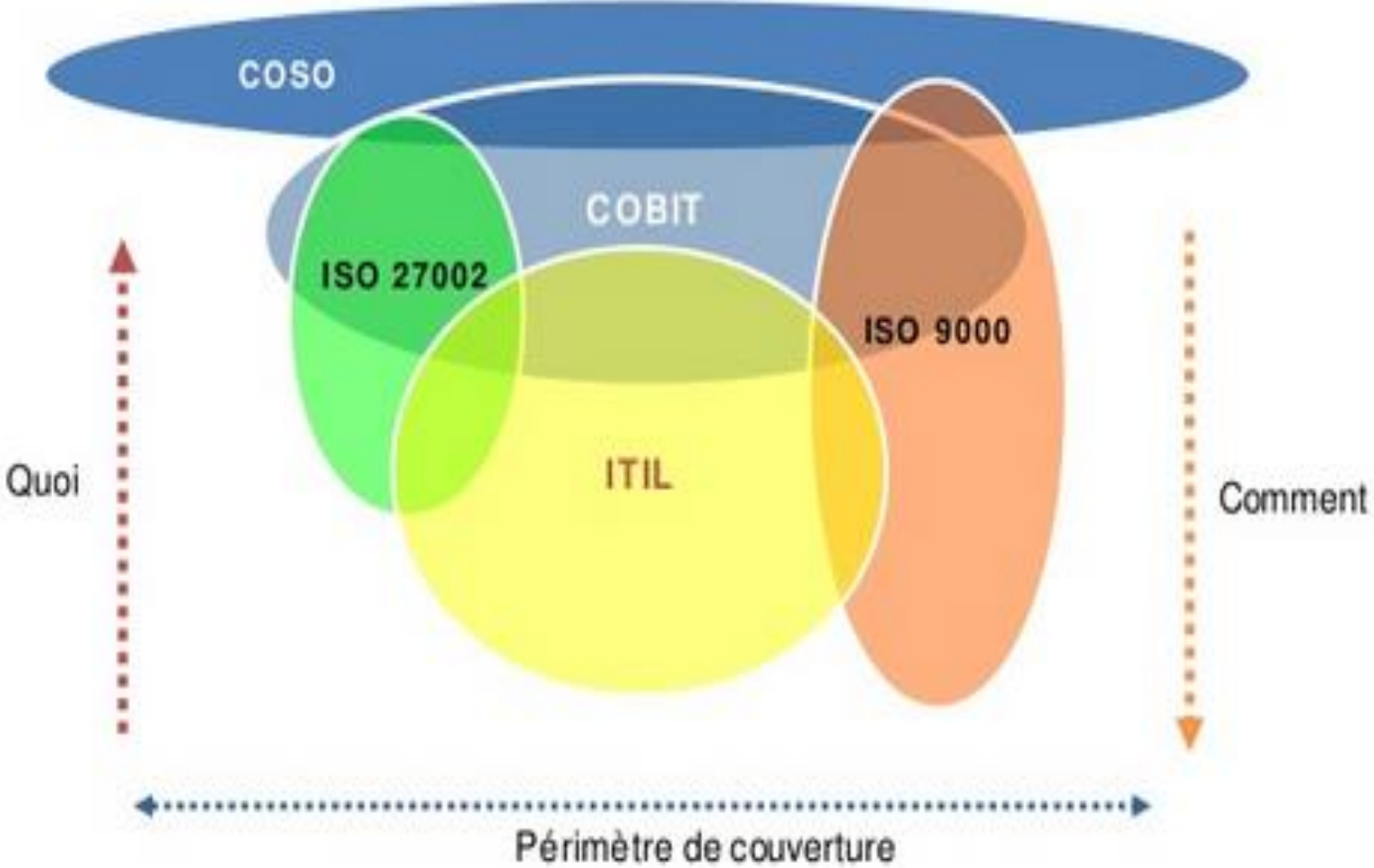


Figure – Exemple MetricStream

COBIT ET LES NRMM



COSO – Committee of Sponsoring Agencies of the Treadway Commission – Internal Control Integrated Framework – focused on business controls
ISO 27001/002 – Information Security Policy
ISO 9000 – Family of standards for Quality Management

Figure – Mapping COBIT