Sécurité des Systèmes d’information
(Analyse des risques)
Partie 1: le risque informatique

université d’Alger 1 -
Benyoucef Benkhedda

Gestion des risques

Risque :

Le risque est la prise en compte par une personne de la **possibilité** de réalisation d'un évènement **contraire** à ses attentes ou à son intérêt. Lorsque la personne concernée agit malgré cette possibilité et s'expose ainsi à cette réalisation, on dit qu'elle prend un risque.

Risque informatique:

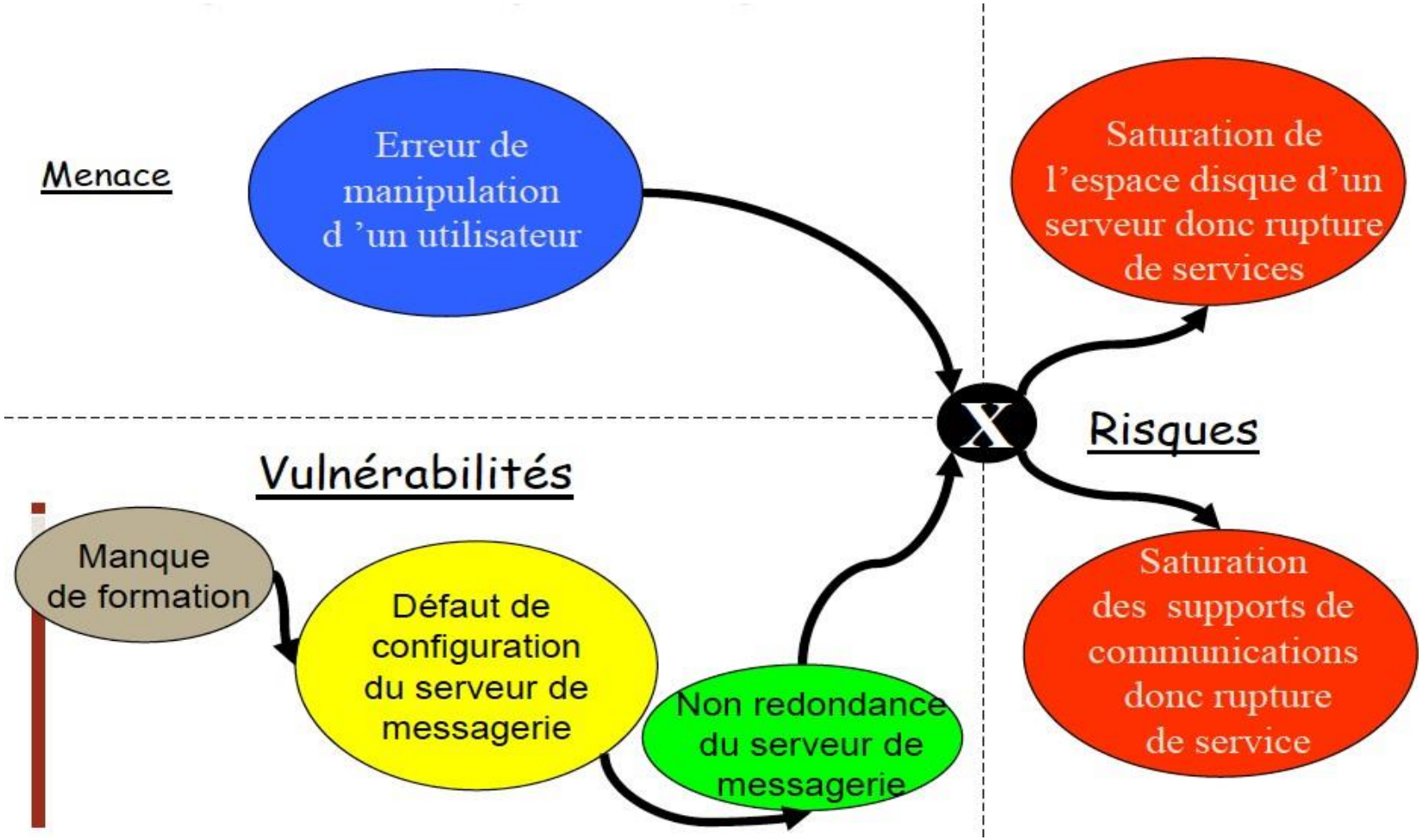
Le **risque** en informatique représente la **possibilité d'exploitation** des **menaces** et **vulnérabilités** existantes d'un SI afin de produire un **impact** bien défini.

Le risque informatique peut être désigné comme le **risque métier** associé à l'utilisation, la possession, l'exploitation, l'implication, l'influence et l'adoption de l'informatique dans une organisation

Gestion des risques

Exemples de risque:

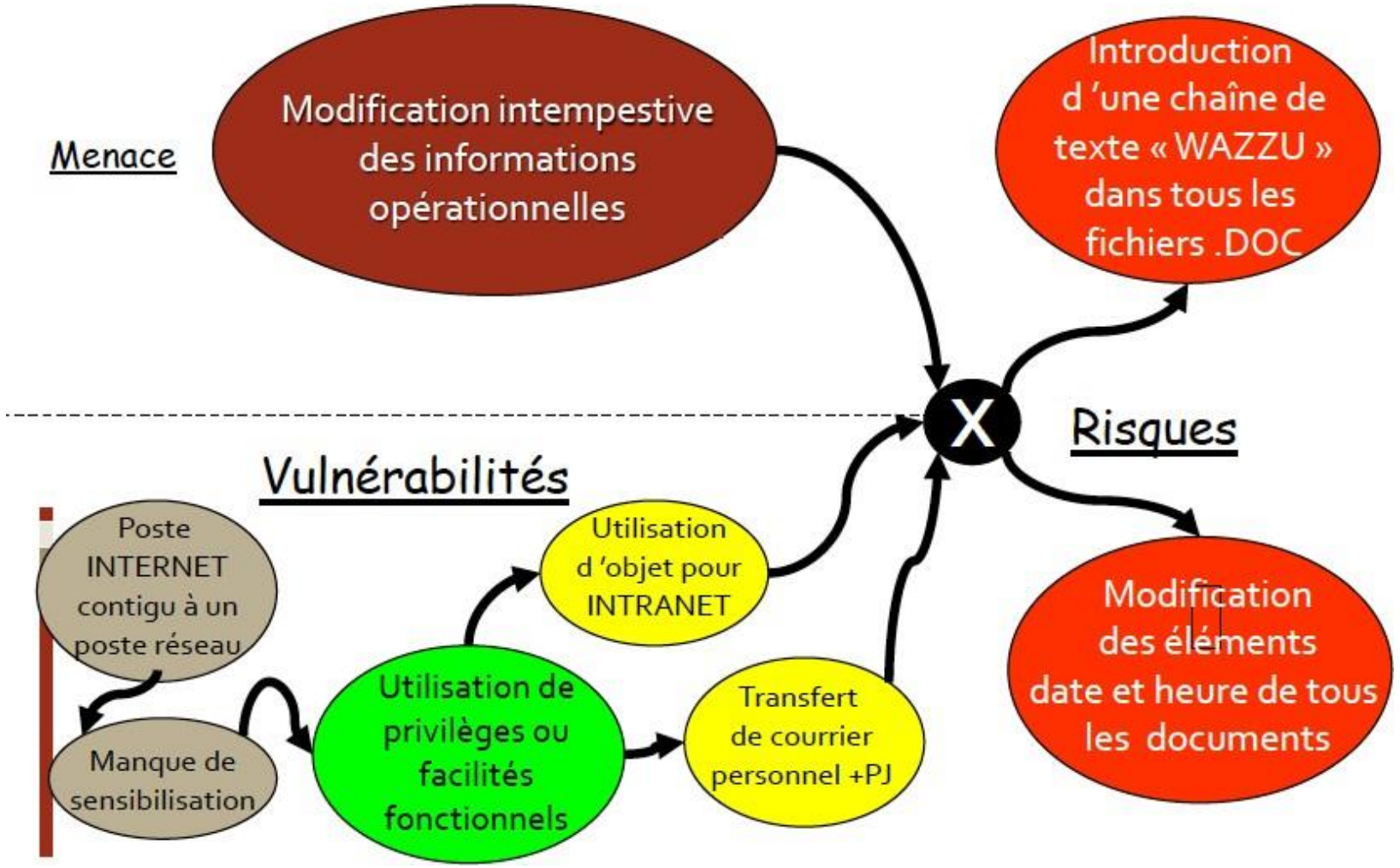
Risque lié à la disponibilité



Gestion des risques

Exemples de risque:

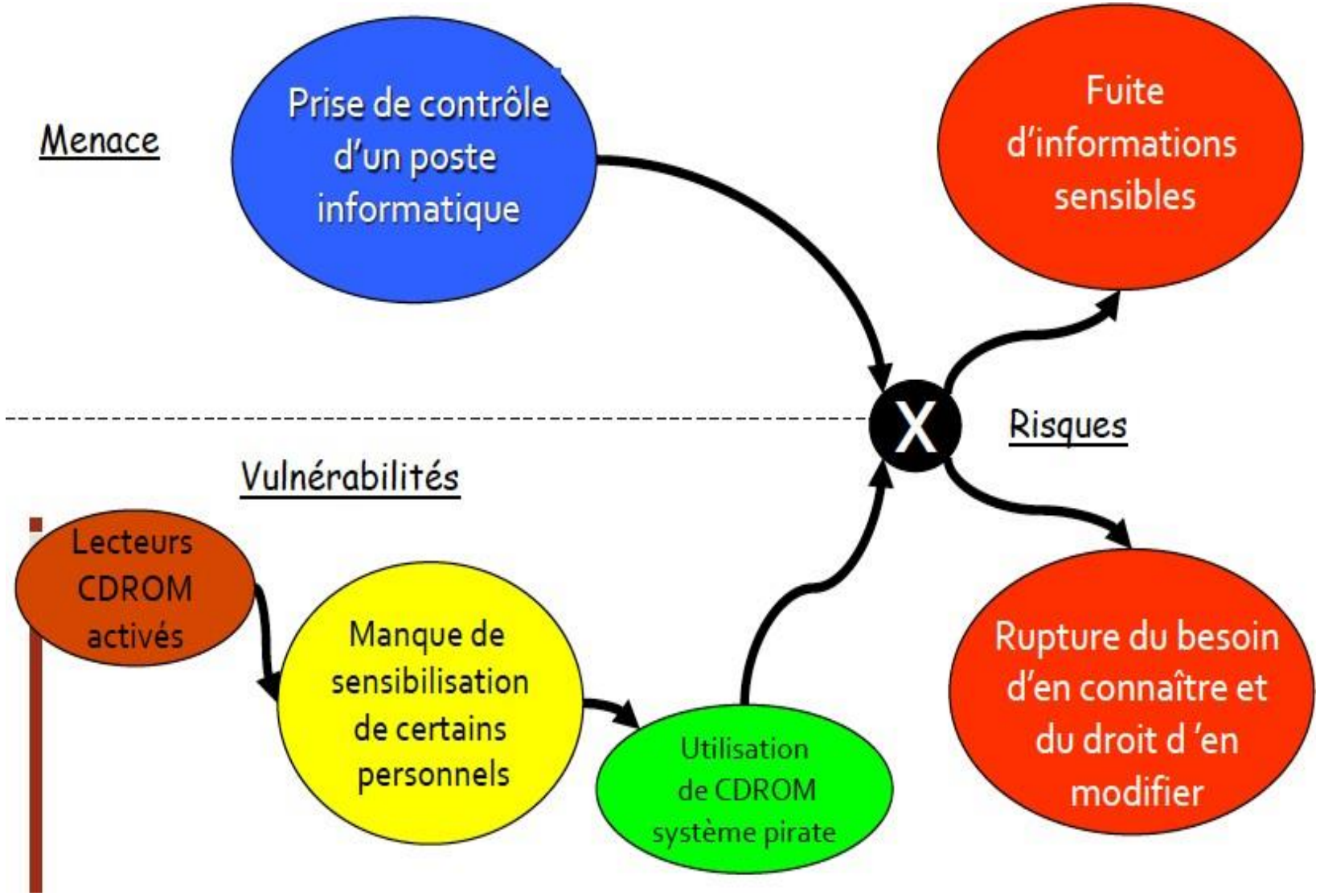
Risque lié à l'intégrité



Gestion des risques

Exemples de risque:

Risque lié à la confidentialité



Gestion des risques

Concepts de gestion de risque:

L'identification et l'évaluation des risques du système et les classifier pour mieux décider sur la sécurisation du système

La gestion des risques se compose de trois blocs interdépendants. Nous distinguons l'organisation cible de l'étude, définie par ses assets et ses besoins de sécurité, puis les risques pesant sur ces assets et enfin les mesures prises ayant pour but de traiter les risques et donc d'assurer un certain niveau de sécurité.

Avant implémentation

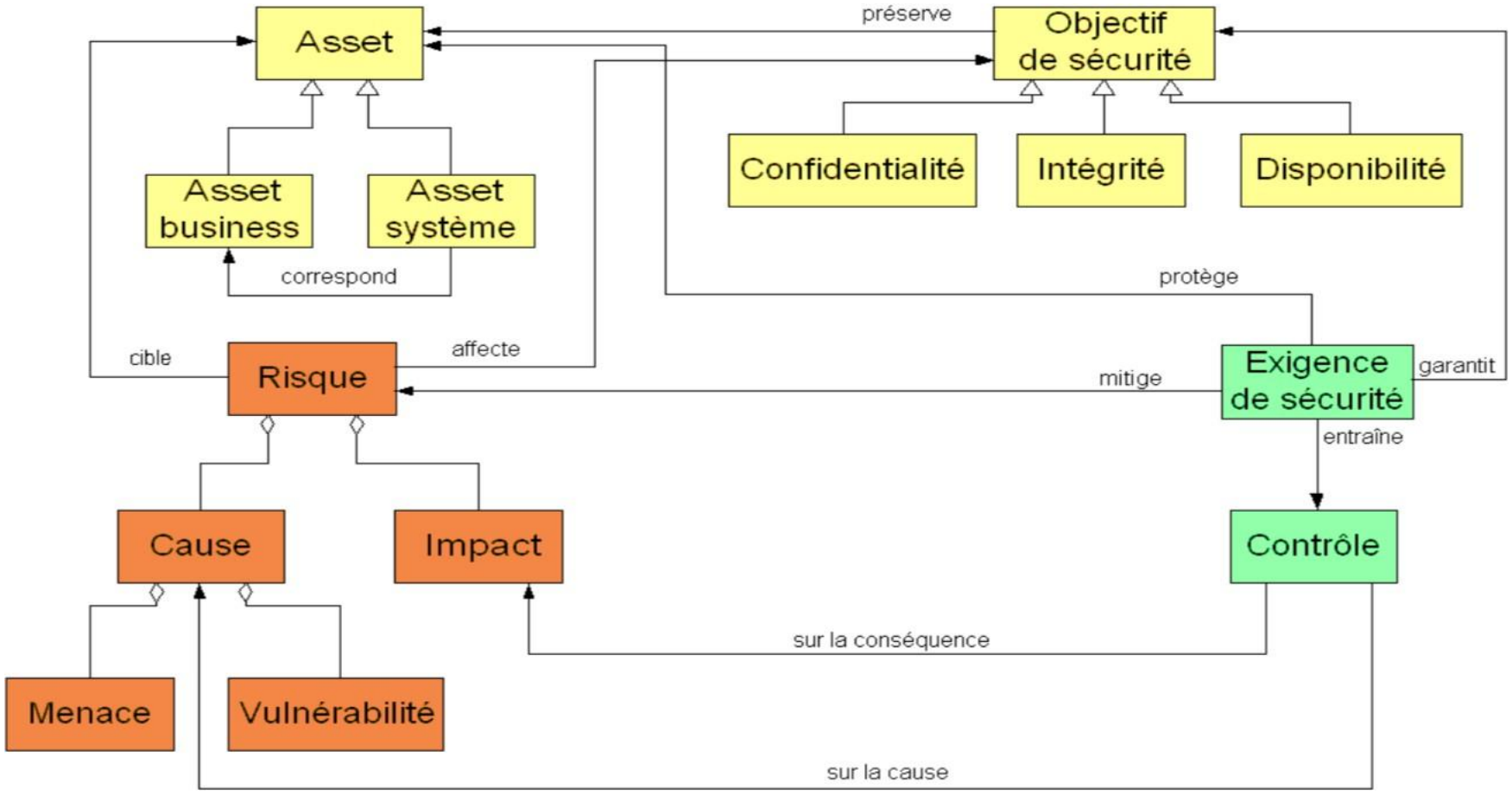
$$\text{Risque} = \text{vulnérabilité} * \text{menace} * \text{impact}$$

Après implémentation

$$\text{Risque} = \frac{\text{vulnérabilité} * \text{menace} * \text{impact}}{contre-mesure}$$

Gestion des risques

Concepts de gestion de risque:



Gestion des risques

Processus de gestion de risque:

Deux approches pour la gestion des risques :

- **L'approche réactive :** en concentrant sur le processus des **réponses sur les incidents**
- **L'approche proactive :** en basant sur le concept de **prévenir** et **préparer**. Celle là sert à définir les mesures quantitative et qualitative des assets du système

Gestion des risques

Processus de gestion de risque:

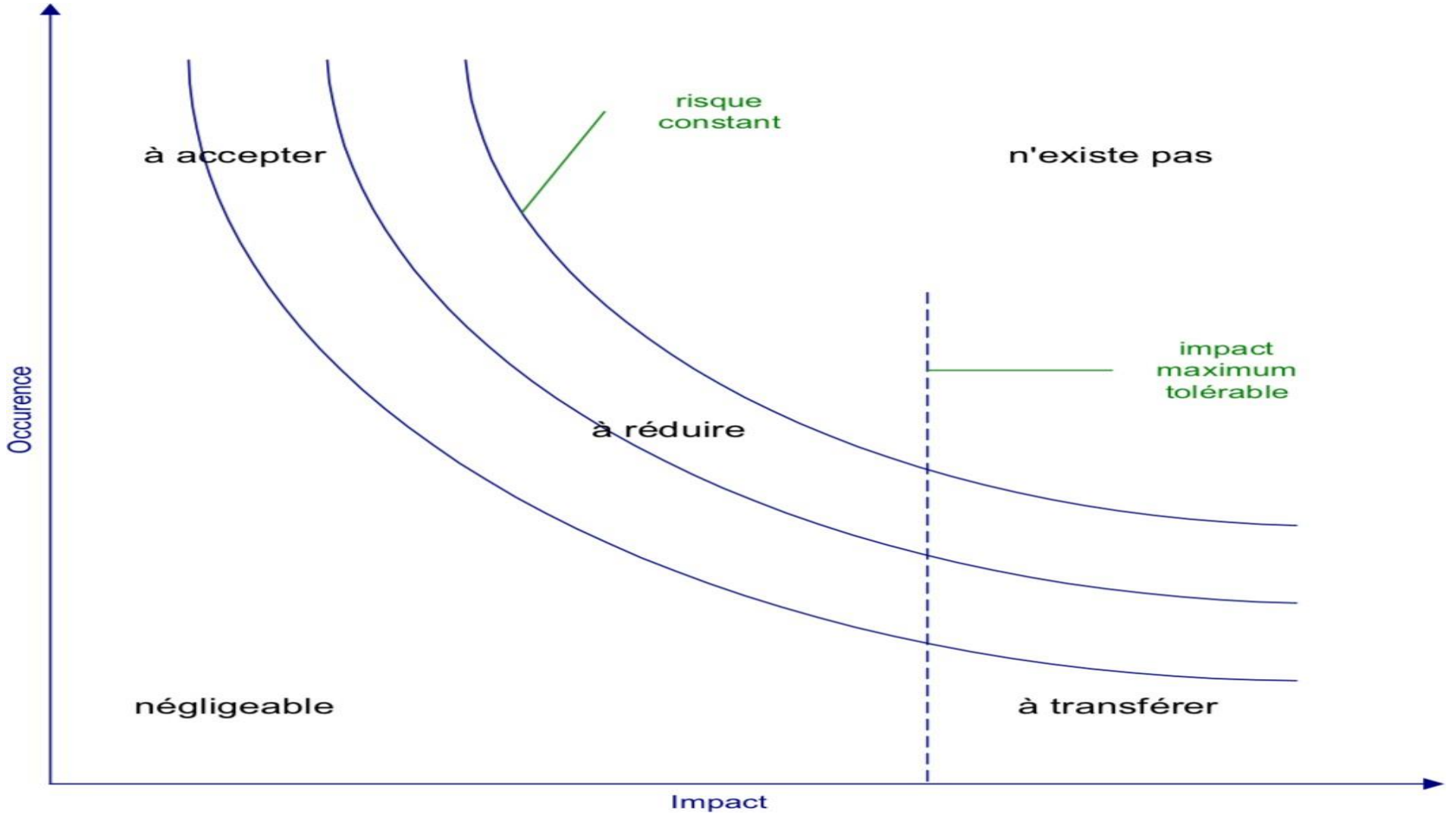
1. Estimation du risque :

Composé de plusieurs étapes:

- **Portée, atouts et équipes:** identification des actifs matériels et immatériels du processus
- **Identification des menaces** existes dans le système, leurs sources et leurs impacts possibles
- **Identification des vulnérabilités** existes dans le système (CVEdetails, MBSA…etc.)
- **Détermination de la vraisemblance** par rapport à la motivation de la source et ses capacités ainsi que l'existence des mécanismes de contrôle
- **Analyse de l'impact** résultat des scénarios réussit du risque
- **Déterminer la valeur finale du risque** (zone du risque)

Gestion des risques

Zones de risque:



Gestion des risques

Processus de gestion de risque:

2. Réduction du risque :

Consiste à contrôler les risques les plus prioritaires en définissant les mesures de contrôle possibles:

- **Contrôles compensatoires:** proposer d'autres mesures de sécurité
- **Contrôles détectives:** identification des actions des attaques et leurs sources
- **Contrôles de récupérations:** rendre le système dans son comportement normal
- **Contrôles correctifs:** réparation des résultats après incidents
- **Contrôles préventifs:** éviter le risque avant qu'il se produise
- **Contrôles dissuasifs:** décourager l'attaquant avant qu'il commence

À la fin, cette étape permet d'assurer une prévention en terme de budget de sécurisation du système à travers un ensemble de rapports définissant les différents plans d'actions en matière de sécurité (plan de reprise d'activités - PRA -, plan de continuité d'activités – PCA - …etc.)

Gestion des risques

Processus de gestion de risque:

3. Évaluation du risque :

Représente le facteur principal de la réussite de la gestion du risque. Il sert à évaluer la sécurité du système pour assurer la continuité de fonctionnement normal.

Certains critères sont importants pour l'évaluation des risques:

- Garder le processus d'évaluation de risque aussi simple
- Ne jamais prendre le programme de gestion de risque comme propriété personnelle
- Concentrez-vous sur **les besoins de l'entreprise** et non sur **l'excellence technologique**
- Adapter les principes de base de la gestion des risques au contexte de votre organisation

Gestion des risques

La gestion des risques en pratique:

- Plusieurs modèles ont été créés

- Trois modèles de références (populaires):

  - ✓ EBIOS (Expression des Besoins et Identification des Objectifs de Sécurité)
  - ✓ OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation)
  - ✓ MEHARI (Méthode Harmonisée d'Analyse de RIsques)