

# GR-Vocabulaire

UNIV-PAU / LP

Importance de la précision du vocabulaire

# Importance de la communication

- Dans la mise en œuvre d'un processus de gestion du risque, **la communication joue un rôle primordial.**
- Le vocabulaire employé dans le cadre de ce processus doit être clairement défini.
- C'est un langage commun pour l'ensemble des participants aux études.

# Quelques définitions

- **Bien**
  - Bien essentiel
    - Critères de sécurité
    - Besoins de sécurité
  - Bien support
    - Vulnérabilité
- **Scénario de menace**
  - Source de menace
  - Menace
- **Événement redouté**
  - Impact
- **Risque**

# Bien

- Toute ressource qui a de la valeur pour l'organisme et qui est nécessaire à la réalisation de ses objectifs.
- Il en existe de deux types :
  - Biens Essentiels (actifs primordiaux, Primary assets)
  - Biens Supports (actifs supports, Supporting assets)

# Bien Essentiel

- Il s'agit d'un bien qui peut être de deux types :
  - Informations
  - Processus, fonctions, activité
- Les biens essentiels constituent la valeur ajoutée du système d'information pour l'organisme
- **Un bien essentiel n'est pas porteur de vulnérabilité.**
- Exemple :
  - Gestion des factures, liste des clients, liste des élèves

# Critères de sécurité

- Caractéristique d'un bien essentiel permettant d'apprécier ses différents besoins de sécurité.
  - Disponibilité
  - Intégrité
  - Confidentialité

# Besoin de sécurité

- Définition précise et non ambiguë du niveau d'exigences opérationnelles relatives à un bien essentiel pour un critère de sécurité donné (disponibilité, confidentialité, intégrité...).
  - doit être disponible dans la journée
  - ne doit être connu que du groupe projet

# Bien Support

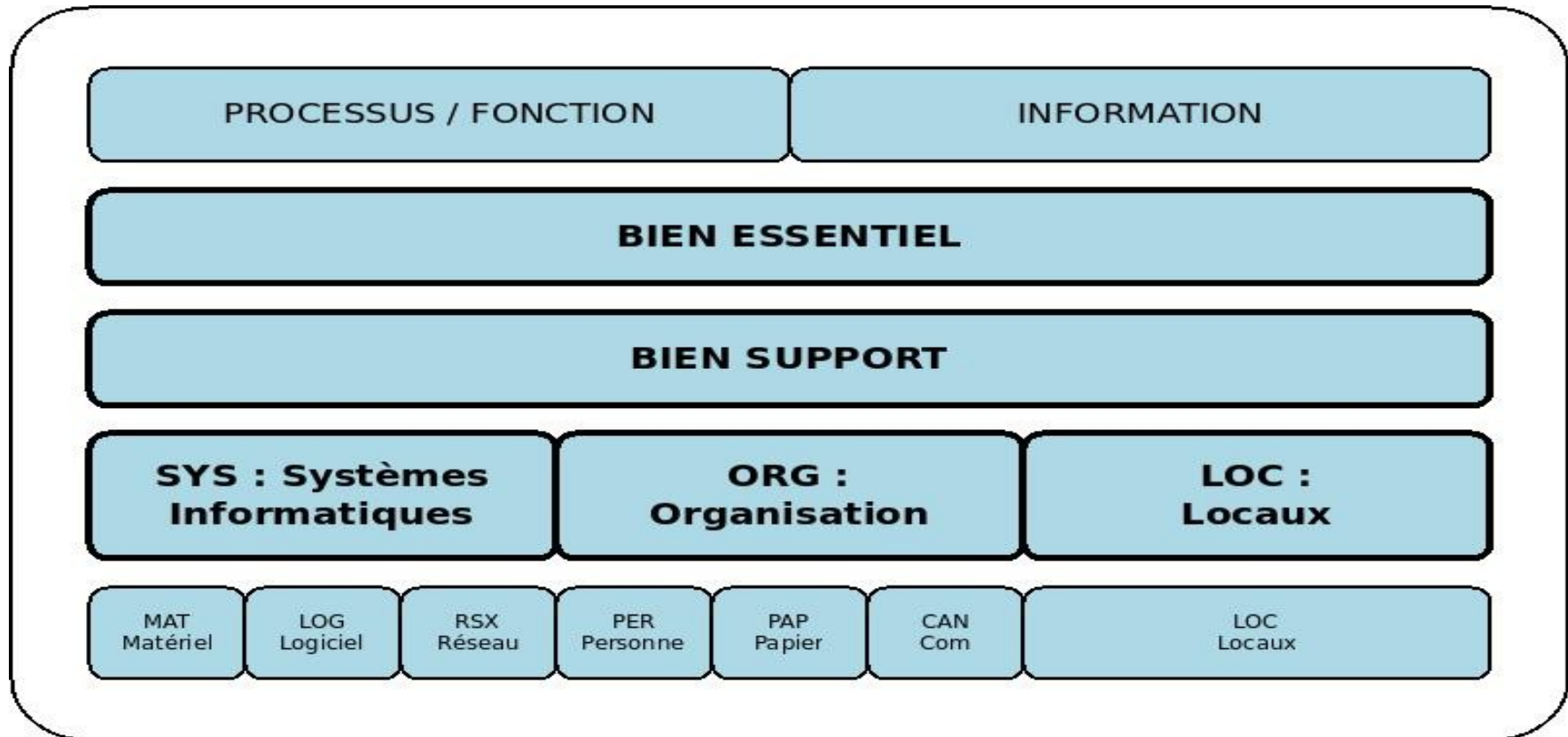
- C'est un bien sur lequel reposent des biens essentiels
- **Les biens supports sont porteurs de vulnérabilités**
- Exemples
  - Service du personnel
  - La salle machine
  - Utilisateur, Administrateur
  - Réseau d'hébergement
  - Un portable



# Vulnérabilité

- Caractéristique d'un **bien support** qui peut constituer une faiblesse ou une faille au regard de la sécurité des systèmes d'information
- Exemples :
  - Absence de sensibilisation des utilisateurs à la sécurité.
  - Crédulité du personnel
  - Faille de sécurité dans le logiciel Internet explorer.

# Biens Supports / Biens Essentiels



- Les biens essentiels constituent la valeur ajoutée du système d'information pour l'organisme. Ils reposent sur les biens supports qui, potentiellement, sont porteurs de vulnérabilités. Dans une analyse de risque, pendant la phase d'inventaire, il est nécessaire de réaliser un tableau qui croise les biens supports et les bien essentiels.

# Source de menace

- Chose ou personne à l'origine de menaces. Elle peut être caractérisée par son type (humain ou environnemental), par sa cause (accidentelle ou délibérée) et selon le cas par ses ressources disponibles, son expertise, sa motivation...
- Exemples :
  - Virus
  - Utilisateurs
  - Ancien membre du personnel ayant peu de compétences techniques et de temps mais susceptible d'avoir une forte motivation.
  - Pirate avec de fortes compétences techniques, bien équipé et une forte motivation liée à l'argent qu'il peut gagner.

# Menace

- Moyen type utilisé par une source de menace
  - Exemples :
    - vol de supports ou de documents
    - piégeage du logiciel
    - atteinte à la disponibilité du personnel
    - écoute passive
    - crue

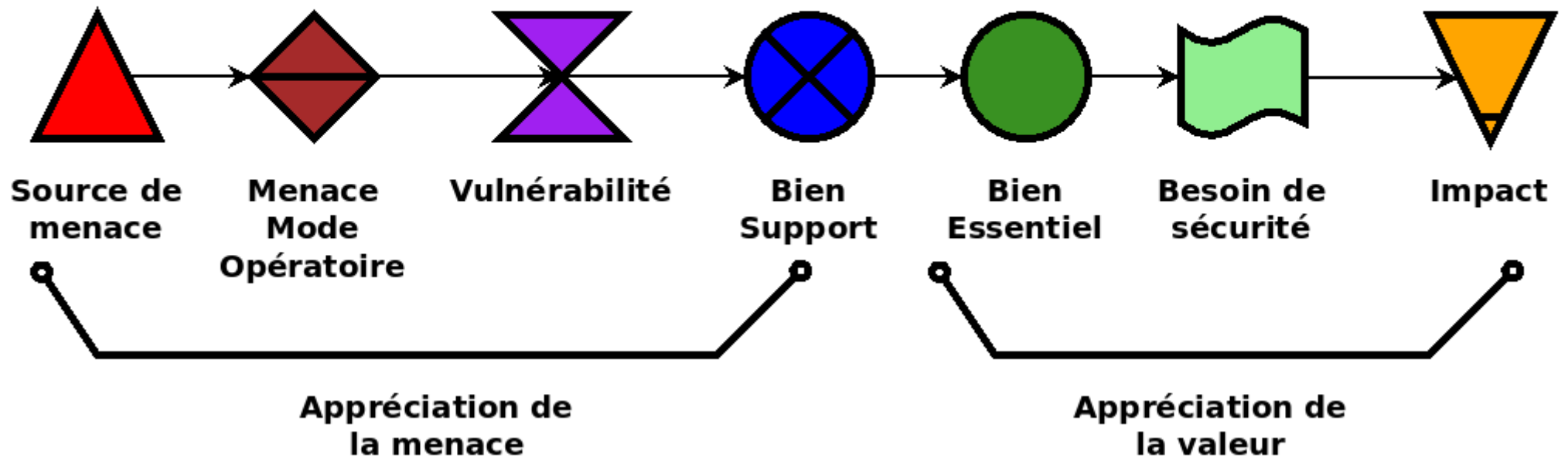
# Impact

- Conséquence sur l'organisme de la réalisation d'une menace.
- Exemples :
  - perte d'image de marque vis-à-vis de la clientèle
  - perte financière à hauteur de 10% du chiffre d'affaires
  - infraction aux lois et aux règlements donnant lieu à des poursuites judiciaires à l'encontre du Directeur

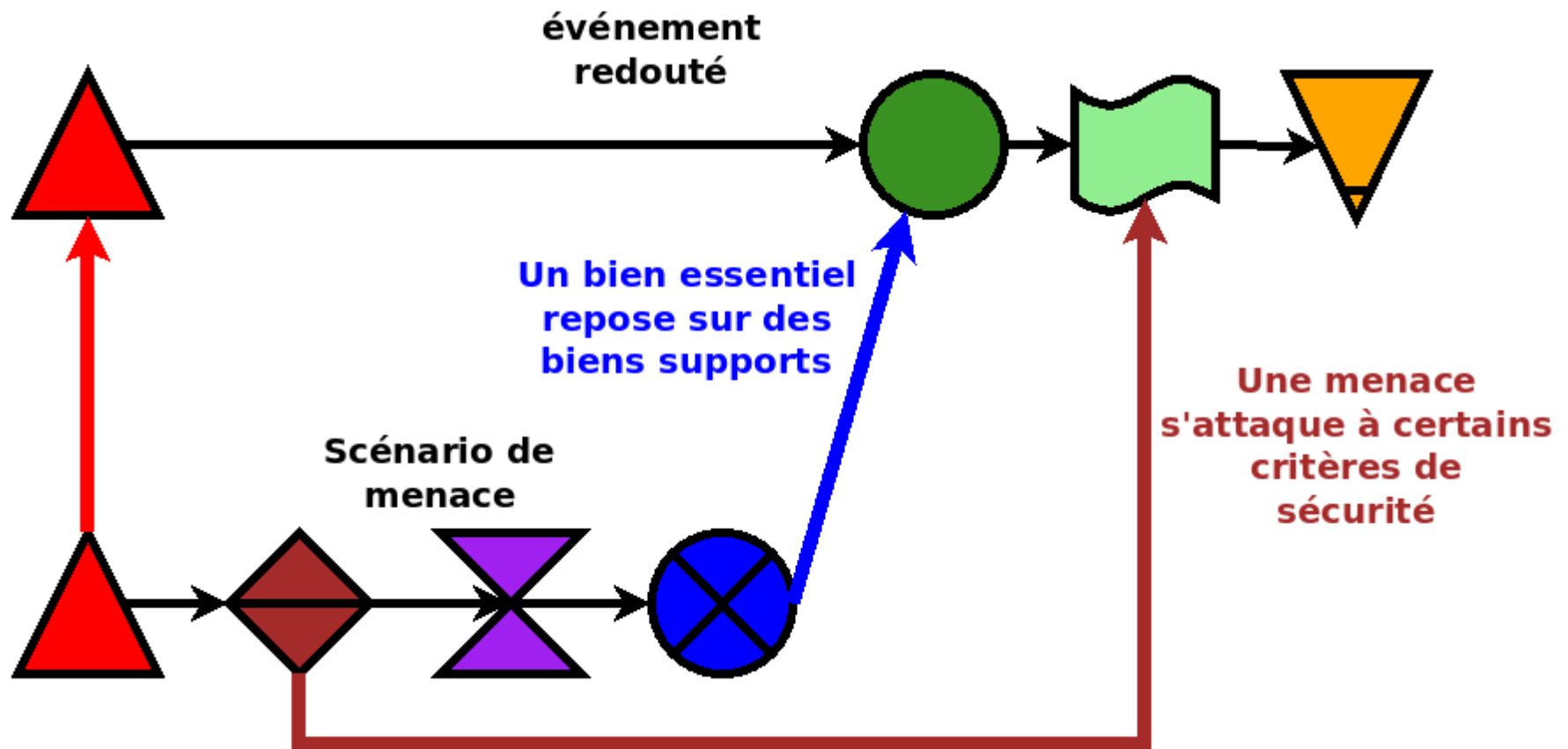
# Le risque

- Utilisez les éléments précédents pour définir le risque

# RISQUE =



# Croisement Événements redoutés et Scénarios de menace





# La méthode EBIOS

- Signification
  - Expression des Besoins et Identification des Objectifs de Sécurité
- Méthode développée et promue par l'ANSSI.
  - Utilisée dans les administrations, dans le secteur privé et à l'étranger.
  - Travail important de pédagogie et de développement de l'outillage autour de la méthode (Logiciel d'assistance sous licence libre)

# Évolution de la méthode

- Avant 2010 : Version 2 de la méthode
- Le club EBIOS et l'ANSSI ont développé une nouvelle version : EBIOS 2010
  - Objectif : devenir conforme à la norme Internationale : ISO 27005
  - ISO 27005 = On a pris ce qu'il y avait de mieux dans les nombreuses méthodes de gestion du risque existantes dans le monde pour aboutir à un consensus.
- La version 3 en cours de développement

# La méthode EBIOS

- Flexible
  - Peut être utilisée pour les systèmes très simples à très complexes en fonction du périmètre choisi.
- Utilisée comme outil de négociation entre la maîtrise d'ouvrage et la direction.