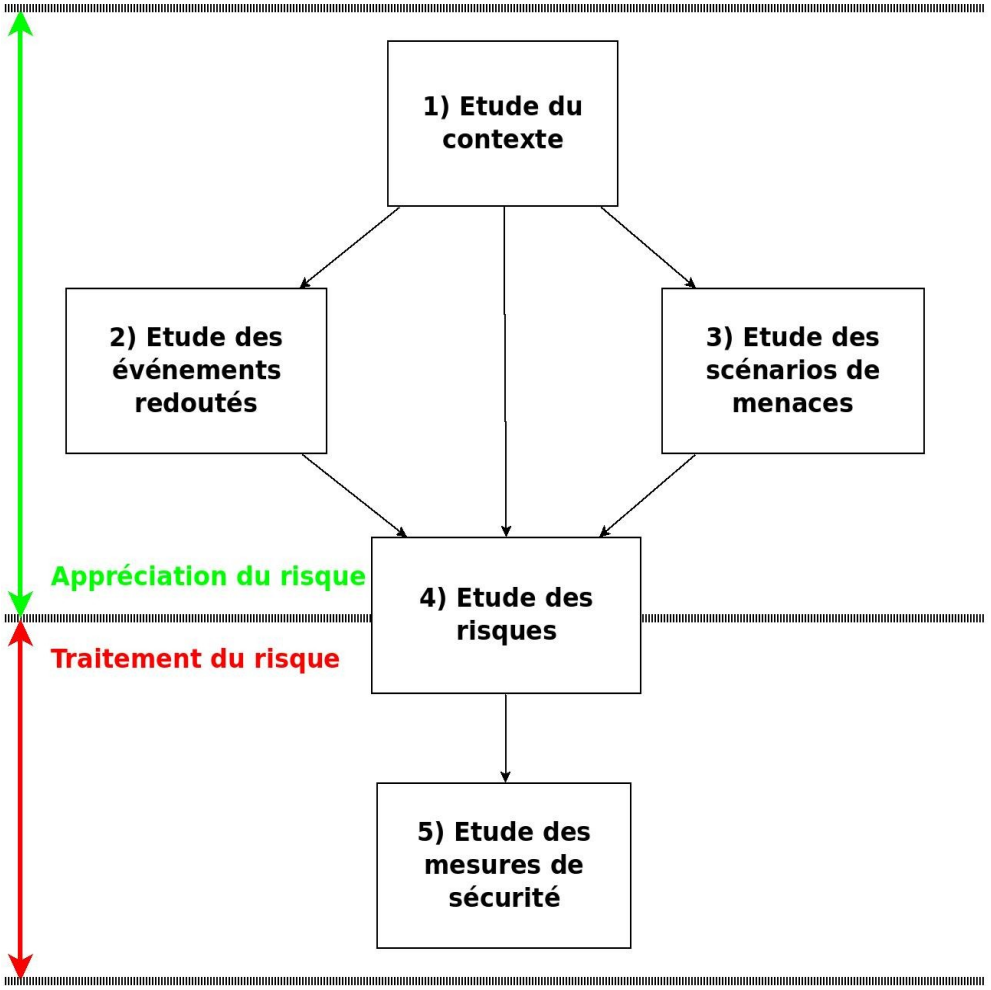
GR – Appréciation du risque

UNIV-PAU / LP

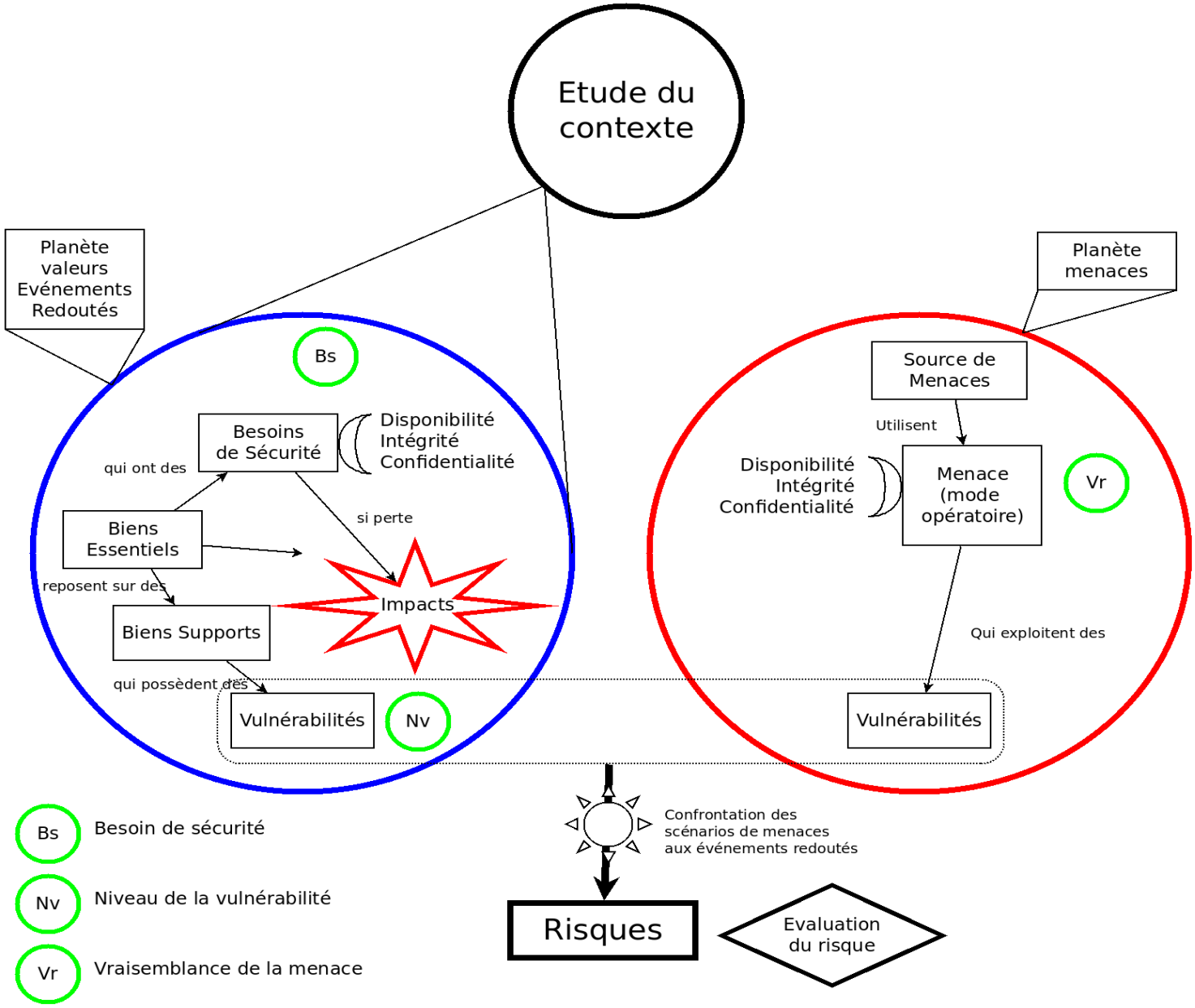
Appréciation des risques

Étapes de l'appréciation du risque



- Étapes concernées par l'appréciation du risque :
  - Étude du contexte
  - Étude des événements redoutés
  - Étude des menaces
  - Identification, estimation et évaluation des risques

Appréciation du risque
Synthèse



Appréciation du risque : Trois activités principales

- Les trois activités suivantes concourent à l'appréciation du risque :
  - L'étude du contexte
  - L'analyse de risque (identification et estimation du risque)
  - L'évaluation du risque
    - Premier point de décision (premier filtre)
    - On élimine tous les risques qui ont un poids trop faible.

L'étude de contexte

- Prendre de la hauteur avant de commencer l'étude (étape essentielle du processus de gestion des risques)
  - stratégie, enjeux, contrainte, règles, étendue du système d'information
  - Détermination du périmètre de l'étude
  - Organisation du processus de gestion du risque
  - Définition des critères de base et des échelles correspondantes pour réaliser les estimations et les évaluations
  - Choix de la bonne granularité des actifs
    - Découpage en sous-systèmes si nécessaire
  - Identification des sources de menace
  - Faire l'inventaire des biens et de leurs propriétaires (biens supports et essentiels + tableau de croisement)

L'analyse de risque

- L'analyse de risque est composée de deux activités :
  - L'identification des risques
  - L'estimation des risques

Analyse de risque / Identification des risques

- Le début de l'identification des risques a déjà été réalisé dans l'étude de contexte : identification des biens (supports et essentiels)
- **Étude des événements redoutés :**
  - Identification et estimation des besoins de sécurité : Valorisation des biens essentiels en utilisant, par exemple les critères (D, I, C)
  - Identification et estimation des impacts en cas de non respect de ces besoins
  - Identification des sources de menaces susceptibles d 'être à l'origine des impacts
- **Étude des scénarios de menaces :**
  - Identification et estimation des scénarios qui peuvent engendrer les événements redoutés.
    - Utilisation des listes de menaces génériques (voir tableau EBIOS)
  - et la vraisemblance des scénarios menaces en utilisant les échelles définies dans l'étude de contexte.

Analyse de risque / Identification des risques

- Identification des risques : Elle se fait en confrontant les événements redoutés aux scénarios de menaces :
  - Les **sources de menace** vont utiliser des **menaces** qui exploiteront des **vulnérabilités** attachées à des **biens supports** sur lesquels reposent des **biens essentiels** qui ont une valeur (exprimée sous forme de **besoins de sécurité**). La perte de ces valeurs a des **conséquences (impacts)** sur l'organisme.
- Comment obtenir ces informations : Interview, brainstorming collectif, expertise.
  - On peut noter ici l'importance de la **communication et de la pédagogie** car on s'adresse généralement à des personnes qui ne connaissent pas les notions que l'on manipule.
  - Les réponses peuvent différer selon les personnes interrogées.
  - Une synthèse doit être effectuée. Un consensus doit être trouvé en comité de pilotage
  - Plusieurs itérations peuvent être nécessaires

Analyse de risque / Estimation du risque

- Estimation des conséquences (impacts)
- Estimation de la vraisemblance des menaces
- Estimation du niveau de risque

Méthode d'estimation

- La méthode peut être
  - Quantitative
    - On dispose d'une échelle avec des valeurs numériques (coût)
  - Qualitative
    - Exemple : faible, moyen, élevé
  - Un mélange des deux

Estimer le niveau de risque

- Il n'existe pas de formule magique pour estimer le risque.
- Il n'existe pas de calcul normalisé
- Il vaut mieux commencer par une formule simple que l'on affinera à chaque itération.

Exemple de méthode

	Vraisemblance de la menace	Non envisageable	Très improbable	Possible mais improbable	Probable	Très probable
Impact sur l'organisme	Insignifiant	0	1	2	3	4
	Significatif	1	2	3	4	5
	Très grave	2	3	4	5	6
	Extrêmement grave	3	4	5	6	7

- Après avoir estimé la vraisemblance de la menace et l'impact sur l'organisme, on en déduit le niveau de risque en appliquant le tableau ci-dessus.
  - Risque faible : 0-2
  - Risque moyen : 3-5
  - Risque fort : 6-7

Synthèse estimation du risque

- On fait une série de petites évaluations
  - Vraisemblance de la menace
  - Niveau des vulnérabilités
  - Estimation des besoins de sécurité sur chaque critère et estimation de la gravité des impacts
- Grâce à la synthèse de toutes ces petites estimations, en confrontant les menaces aux besoins de sécurité, on obtient une liste de risques hiérarchisés.

Évaluation du risque

- C'est **la première décision forte** dans le processus
  - A partir de quel niveau, le traitement du risque doit-il être engagé ?
  - Comment va-t-on prioriser le traitement du risque ?
  - On utilise tout le travail effectué dans l'analyse de risque.
- Seuls les risques ayant passé ce premier filtre seront présentés aux décideurs.

Synthèse appréciation du risque