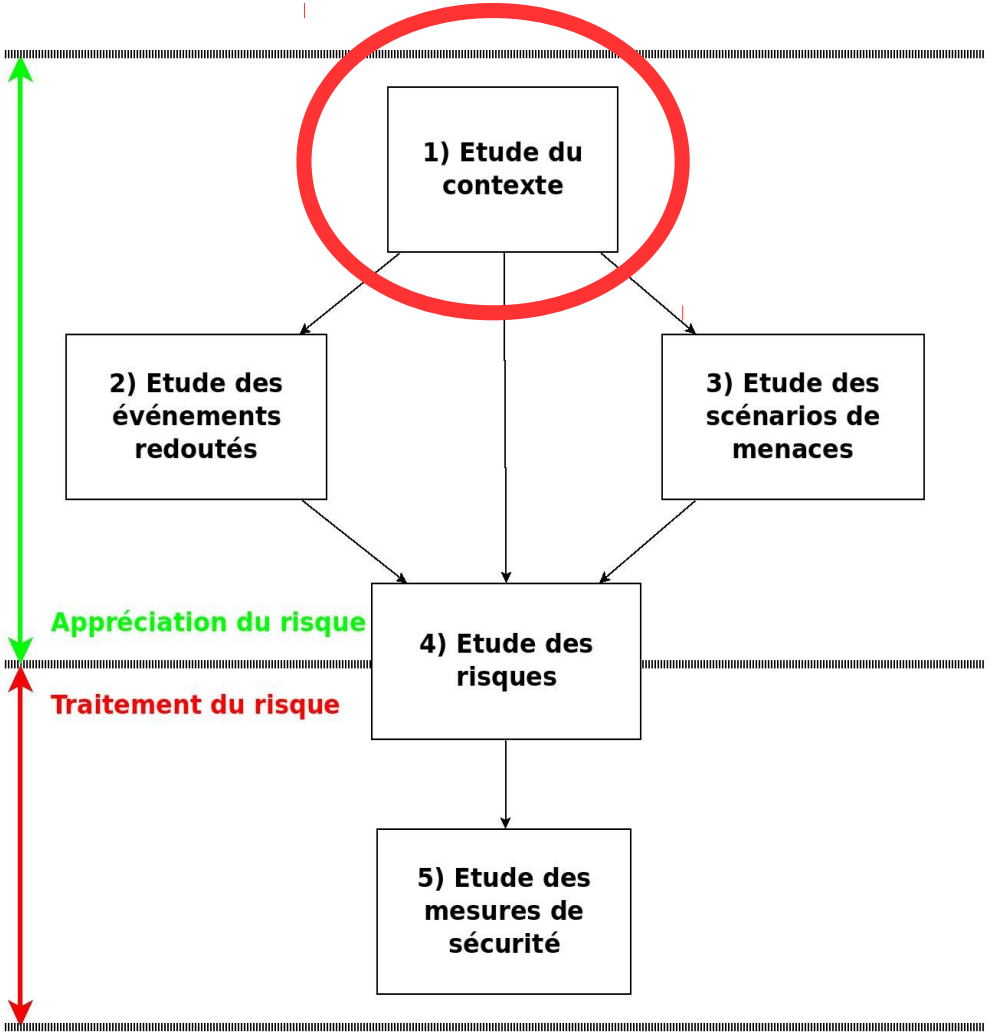
GR - Étude du contexte

UNIV-PAU / LP

Étude du contexte

L'étape la plus importante du processus

Rappel de la démarche



- L'étude de contexte est le premier des 5 modules de la méthode EBIOS.
- Elle est composée de trois activités :
  - 1.1 Définir le cadre de la gestion des risques
  - 1.2 Préparer les métriques
  - 1.3 Identifier les biens
- **C'est l'étape la plus importante**

Définir le cadre de la gestion des risques / périmètre

- Circonscrire **le périmètre de l'étude**
  - Présenter l'organisme (vocation, métier, missions, valeurs, axes stratégiques, structure de l'organisme, organigramme) et le contexte externe.
  - Décrire le sujet de l'étude
  - Identifier les processus métiers ou / et les sites qui vont être concernés par l'étude
  - Identifier les paramètres à prendre en compte dans le traitement des risques (contraintes, hypothèses, références applicables...)
  - Faire une description fonctionnelle du Système d'Information Globale (récupérer si possible les modèles existants : MERISE, UML)

Définir le cadre de la gestion des risques

- Définir un cadre pour la gestion des risques
  - Décrire le but de la gestion des risques qui va être mise en œuvre (homologation, élaboration d'une politique, gestion continue des risques, certification...)
  - Décrire l'organisation mise en place pour gérer les risques (personnes interrogées, autorité de validation, constitution du comité de pilotage...)
  - Décrire la structure de travail (tâches à réaliser, ressources à prévoir, personnes participant à l'étude, chemin de décision, livrables, enregistrements...)

Préparer les métriques

- Cette activité a pour but de fixer l'ensemble des paramètres et des échelles qui serviront à gérer les risques
- Ces éléments peuvent être communs à plusieurs études

Préparer les métriques / actions

- Déterminer et définir les critères de sécurité (disponibilité, intégrité, confidentialité, ...)
  - Élaborer une échelle de besoins de sécurité pour chaque critère de sécurité (être le plus précis possible dans les définitions)
- Déterminer les types d'impacts (sur les missions, sur la sécurité des personnes, financiers, juridiques, sur l'image, sur l'environnement, ...)
  - Élaborer une échelle de niveau de gravité des impacts
- Déterminer les types de sources de menaces (cause : accidentelle ou délibérée, type : humain, naturel, environnemental, interne ou externe)
  - Élaborer une échelle de niveau de vraisemblance des scénarios de menaces
- Définir les critères de gestion des risques (règles de sélection des menaces, règle d'évaluation des risques, …)
- Exemples d'échelles (voir les tableaux EBIOS p36, 37, 38)

Identifier les biens / généralité

- Cette activité a pour but, d'identifier les biens au sein du sujet de l'étude
  - Biens essentiels
  - Biens supports
  - Tableau croisé Biens essentiels / Biens supports
- et d'identifier les mesures de sécurité existantes.

Identifier les biens

- Granularité
  - La granularité dépend du but de l'étude
- Découpage possible en sous-systèmes dans le cas d'un système complexe
  - Plusieurs études en parallèle
- En cas de spécification incomplète du système
  - Étude rapide
  - Et on affine ensuite

Identifier les biens essentiels

- Lister les biens essentiels
  - Informations
  - Processus, activités, fonctions et sous fonctions
    - Informations en entrée
    - Informations en sortie
- Rattacher chaque bien essentiel à un dépositaire (le responsable du bien essentiel)
- Un bien essentiel dont les besoins de sécurité varient dans le temps pourra être scindé en plusieurs biens essentiels.

Identifier les biens supports

- Lister les biens support
  - Les classer selon leur catégorie
    - Système (Matériel, Logiciel, Réseau)
    - Organisation (Personnel, Papier, Canaux interpersonnels)
    - Locaux
  - Les rattacher à un propriétaire
- Décrire les liens qui existent entre eux.