Sécurité des Systèmes d'information
(Analyse des risques)
Partie 2: la méthode EBIOS

université d'Alger 1 -
Benyoucef Benkhedda

Sécurité des SI

Cycle de vie de développement d'un SI:

- **Spécification des besoins** (définir ce quefait le système)
- **Conception** (définir comment on fait lesystème)
- **Réalisation** (faire le système)
- **Utilisation** (installer et exploiter le système)

Une organisation est composée d'un ensemble de **systèmes d'information** chacun un **rôle**, une **position** et un **impact stratégique** sur l'organisation

Sécurité des SI

Intégration de la sécurité:

- **Au niveau de spécification des besoins**

  - ✓ Analyser les **enjeux** stratégiques du système en terme de sécurité (poids stratégiques du système, impact de la sécurité du système sur la sécurité de l'organisme et pertes maximale autorisée)

  - ✓ Analyser le **contexte** du système dans l'organisation (environnement, menaces et contraintes de sécurité)

  - ✓ Définir les **besoins intrinsèques** et les **objectifs** des securité

  - ✓ Se décliner en **mesures non techniques** et **mesures techniques** de sécurité

Sécurité des SI

Intégration de la sécurité:

- **Au niveau de conception**

  - ✓ Choisir les **fonctions** et les **mécanismes** nécessaires répondant aux besoins définis dans la phase précédente

  - ✓ Consoliderle document de la **politique de sécurité du SI (PSSI)**

  - ✓ Définir les différents **plans** de sécurité nécessaires (PCA, PRA, PRS…etc.)

Sécurité des SI

Intégration de la sécurité:

- **Au niveau de réalisation**

  - ✓ **Développer** et/ou **intégrer** les mécanismes de sécurité choisis dans la conception

  - ✓ Effectuer une **analyse des vulnérabilités** résiduelles

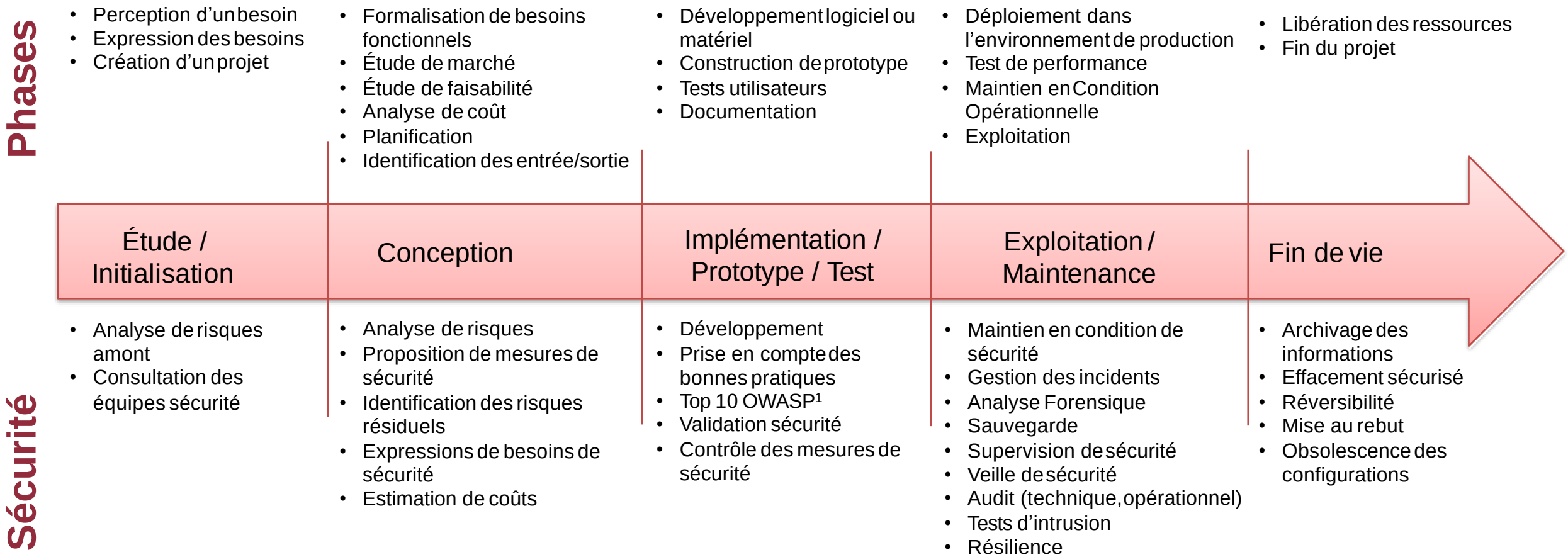
- **Au niveau de l'utilisation**

  - ✓ **Analyser** et **valider** la sécurité du système pour des éventuelles mises-à-jours

  - ✓ **Sauvegarde** des états d'échéance de la sécurité et formation des futurs ingénieurs et responsables sur les actualités de la sécurité

Sécurité des SI

Intégration de la sécurité:



Sécurité des SI

Méthode EBIOS:

Une méthode d'analyse des risques qui peut être appliquée sur un système **à concevoir** ou **existant**

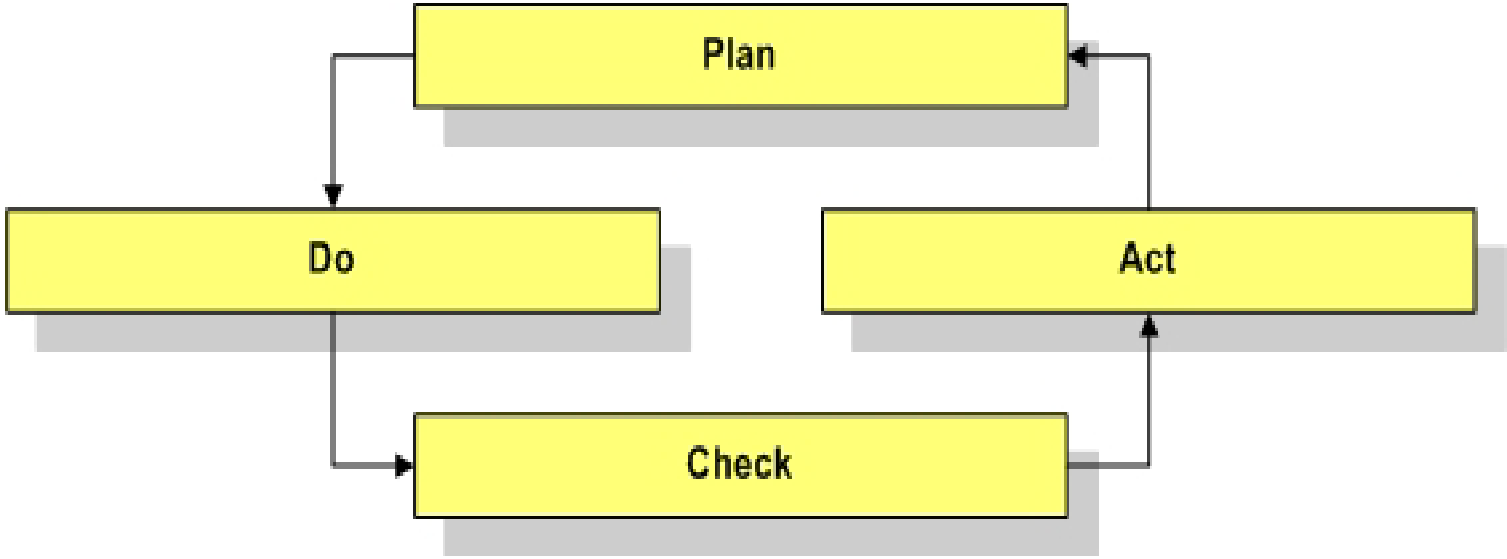
Elle sert à déterminer les actions de sécurité à prendre en considération vis-à-vis le **système** et ses **ressources**

EBIOS

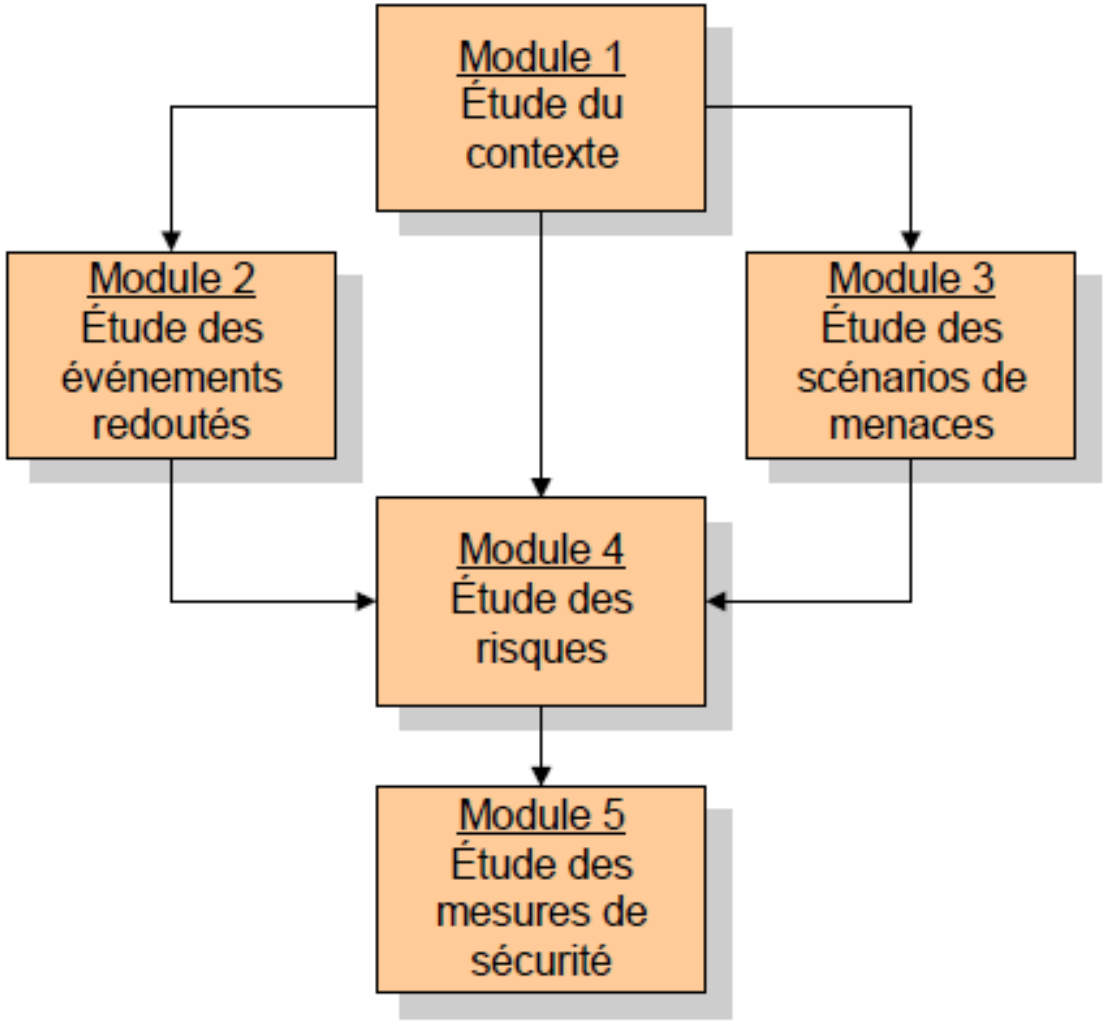
Méthode d'étude et non pas de sécurisation:

- La méthode EBIOS, tout comme les autres méthodes connues, n'est pas une méthode de sécurisation des systèmes mais plutôt une méthode de prise de décision pour le choix des mesures de sécurité à prendre en considération.

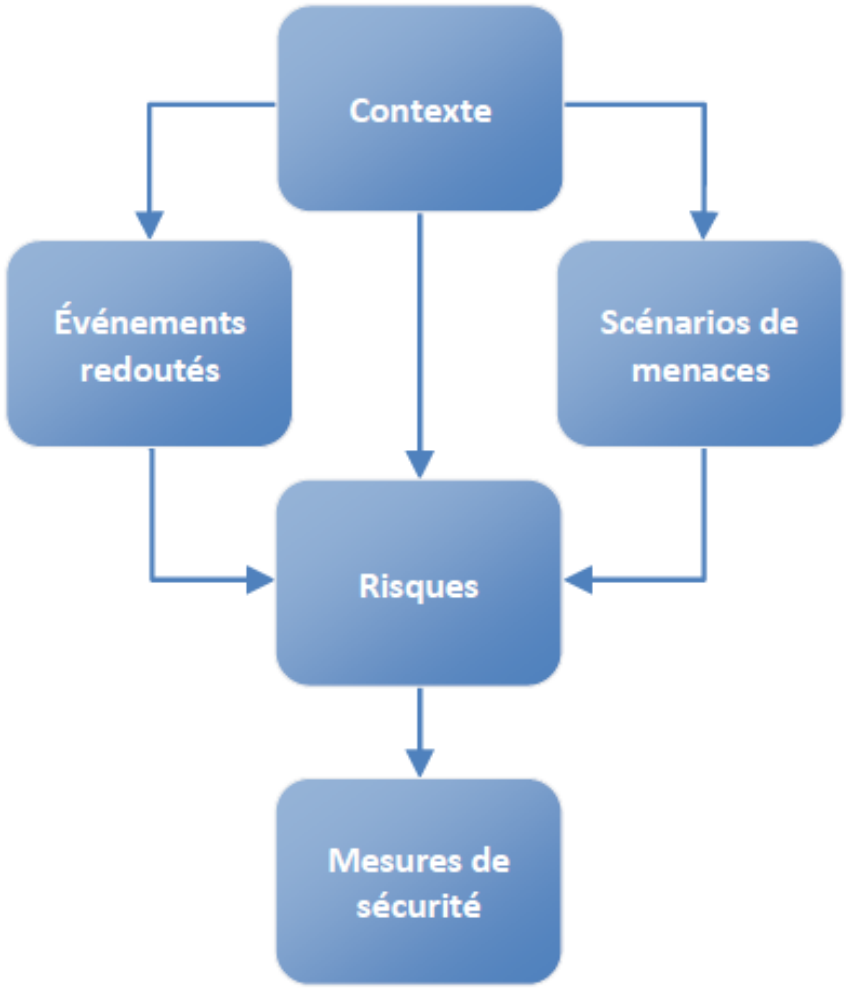
- La sécurité d'un tel système doit être prise en compte dans toute les étape:



Démarche générale d'EBIOS



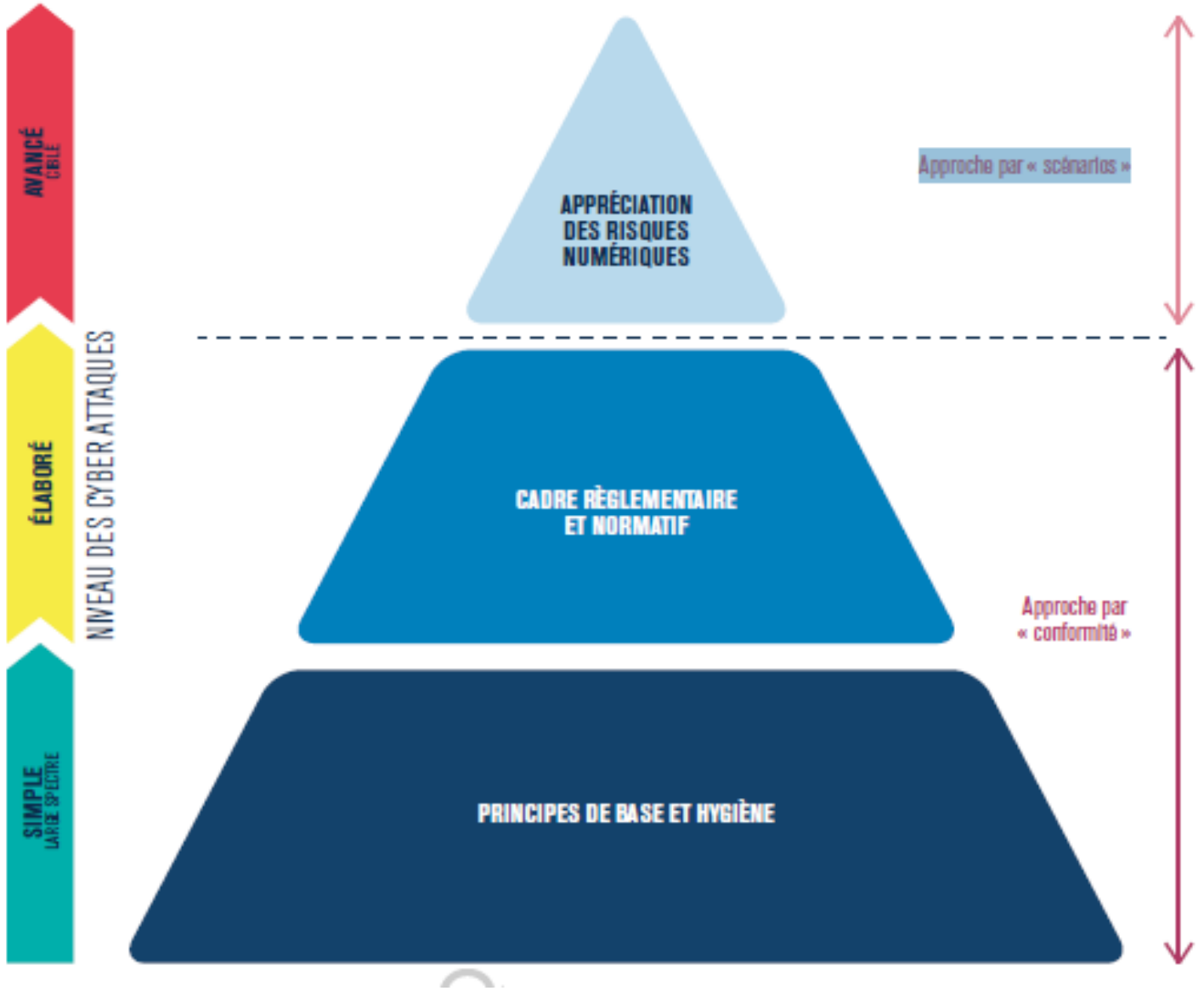
Les 10 questions essentielles pour gérer les risques



Contexte	•Pourquoi et comment va-t-on gérer les risques ? •Quel est le sujet de l'étude ?
Evénements redoutés	•Quels sont tous les événements craints ? •Quels seraient les plus graves ?
Scénarios de menaces	•Quels sont tous les scénarios possibles ? •Quels sont les plus vraisemblables ?
Risques	•Quelle est la cartographie des risques ? •Comment choisit-on de les traiter ?
Mesures de sécurité	•Quelles mesures devrait-on appliquer ? •Les risques résiduels sont-ils acceptables ?

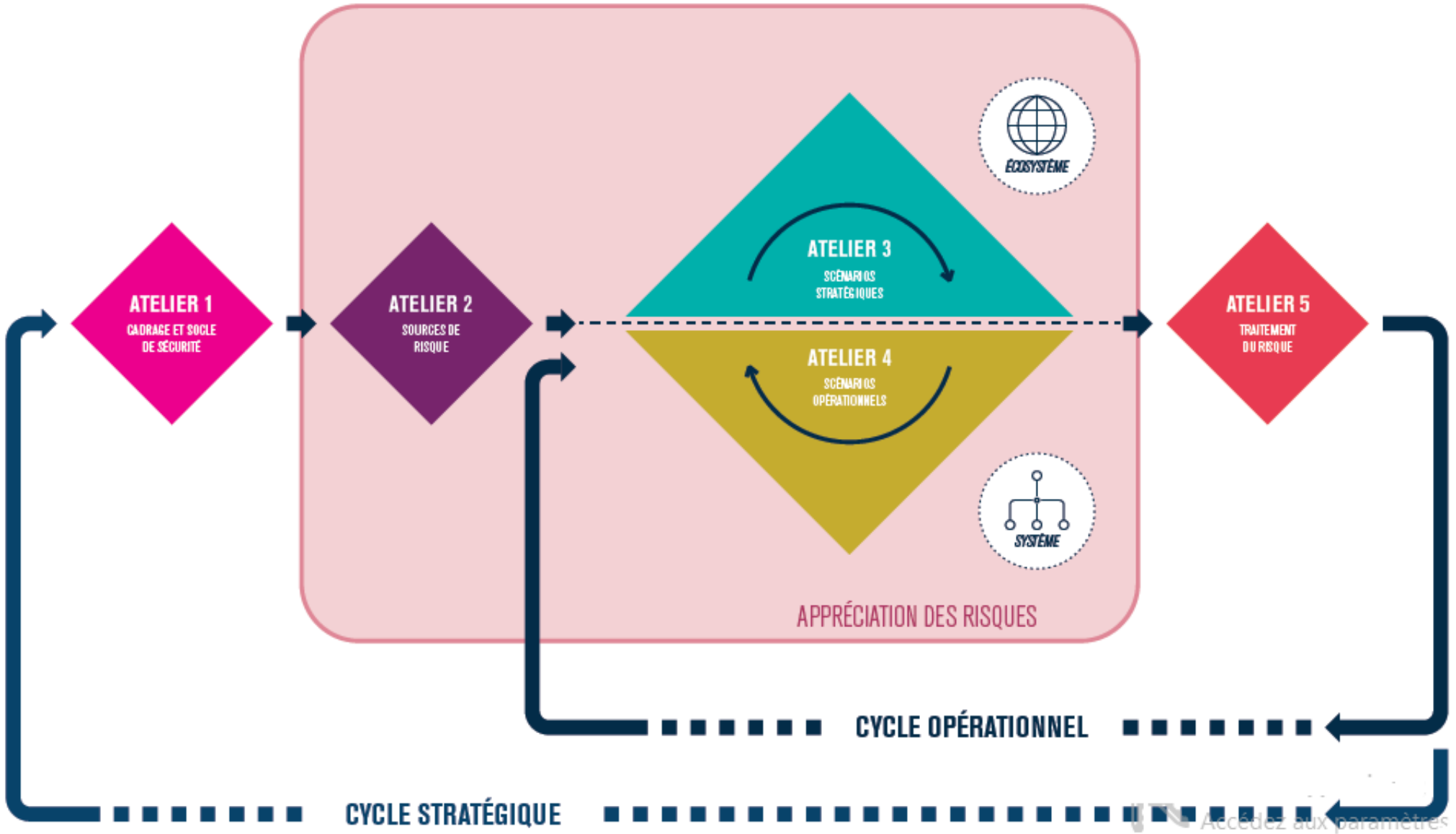
Source : ANSSI

La pyramide d'EBIOS



Source : guide Ebios

EBIOS Processus itératif à 5 ateliers



Source : guide Ebios

EBIOS

Exemple:

- Système d'information d'un bureau d'étude appelé « @RCHIMED »