Méthodologie de sécurité informatique

(SMSI – Analyse des risques)
la méthode EBIOS risk manager
EBIOS-RM-

université d'Alger 1 -
Benyoucef Benkhedda

Sécurité des SI

Cycle de vie de développement d'un SI:

- **Spécification des besoins** (définir ce que fait le système)
- **Conception** (définir comment on fait le système)
- **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 sécurité

  - ✓ 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

  - ✓ Consolider le 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

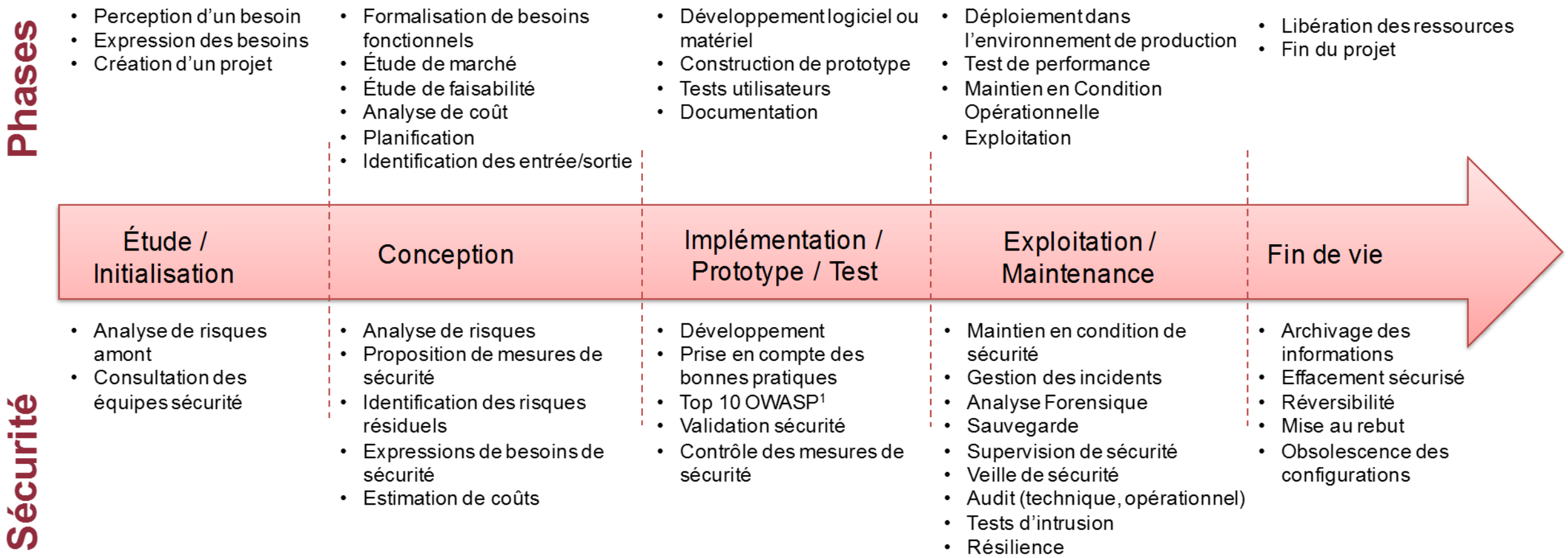
- **Au niveau de l'utilisation**

  - ✓ **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

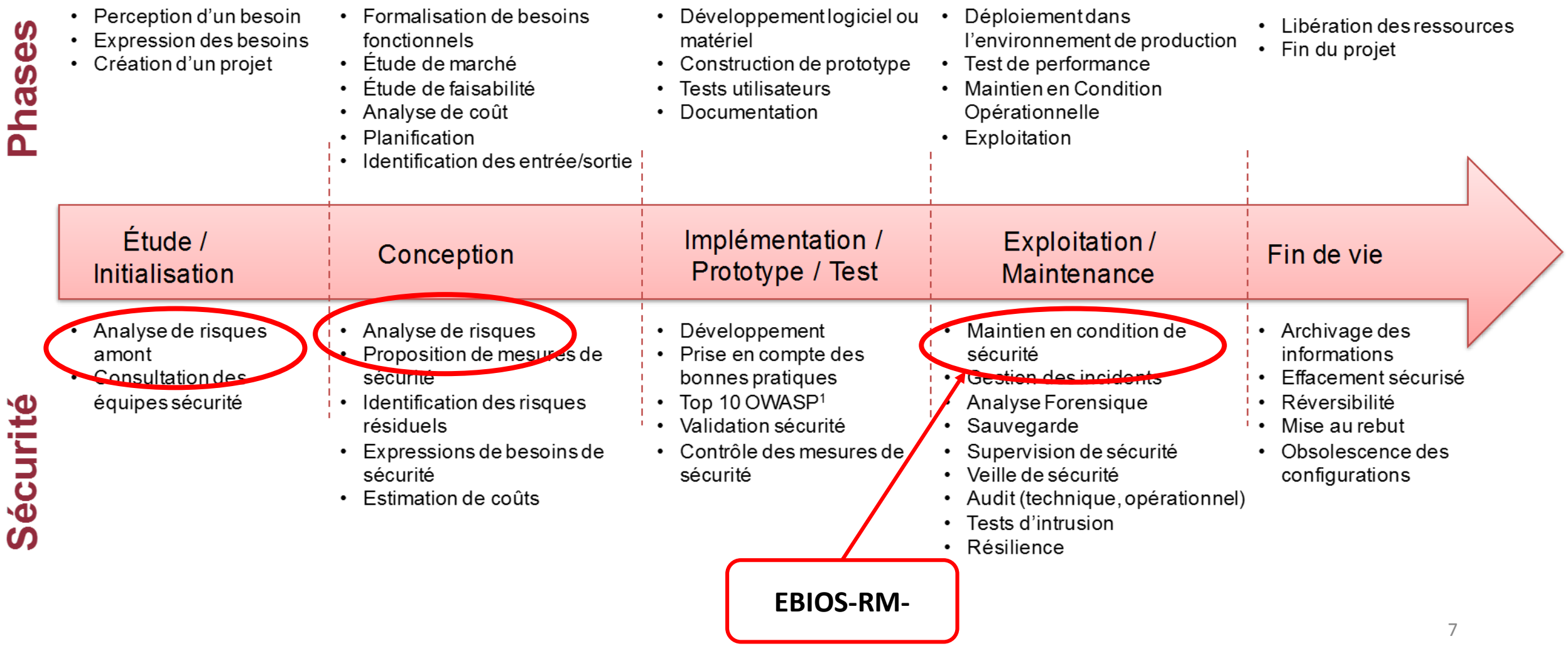
Sécurité des SI

Intégration de la sécurité:



Sécurité des SI

Intégration de la sécurité:



Sécurité des SI

Méthode EBIOS-RM-:

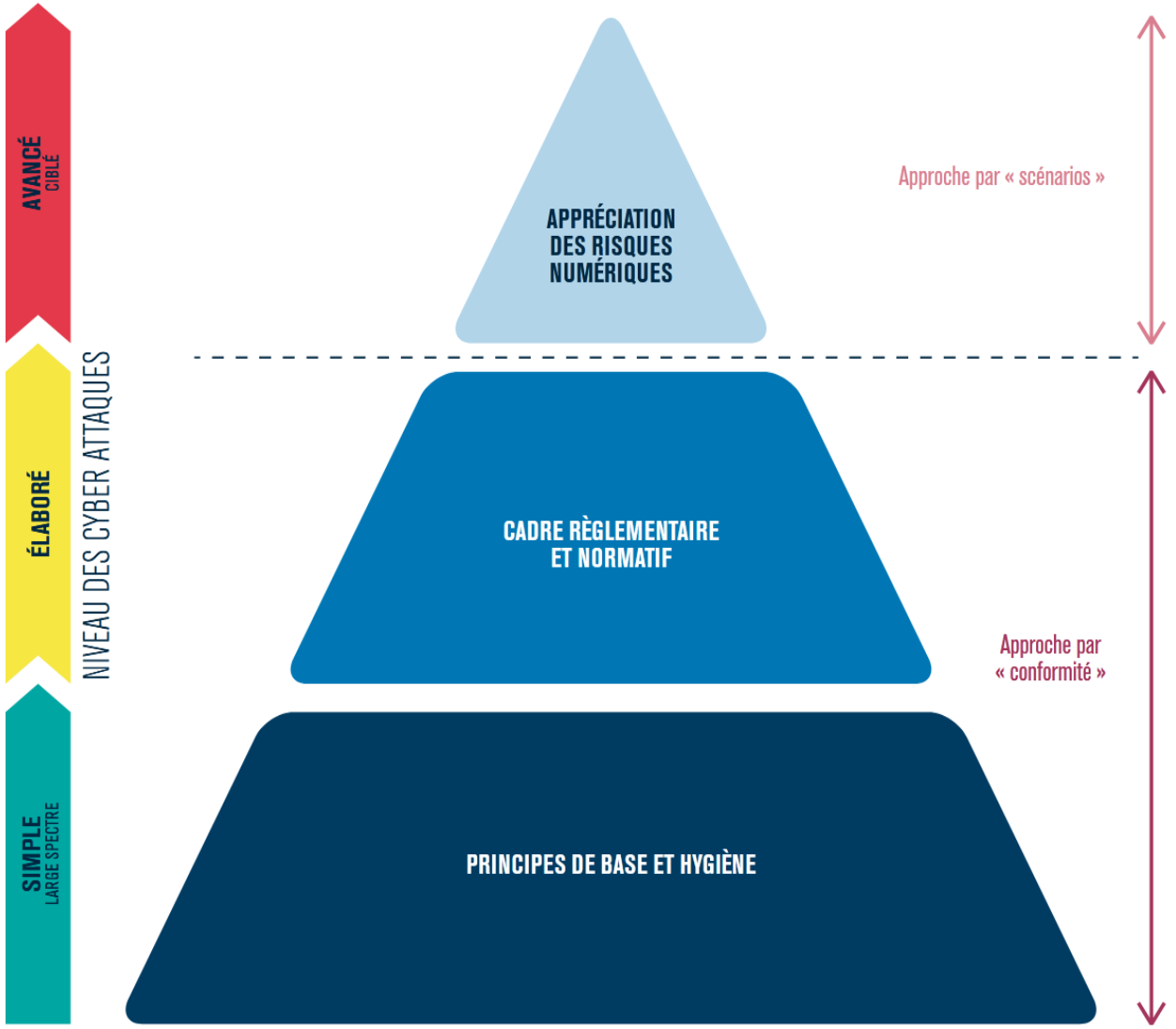
Une méthode d'analyse des risques qui peut être appliquée sur une système **à concevoir** ou **existant**

Successeur de la méthode EBIOS qui est devenue obsolète depuis 2010

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

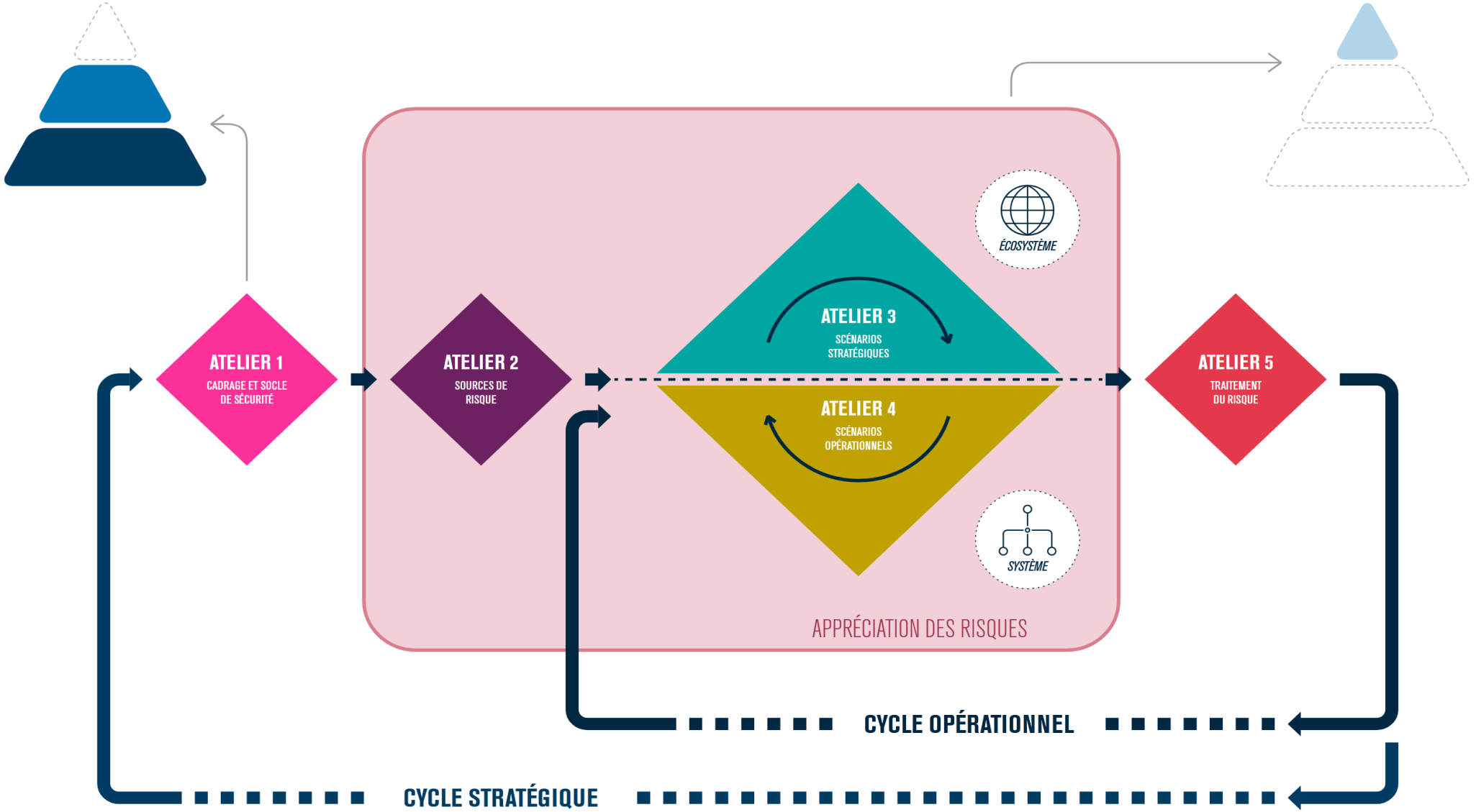
EBIOS-RM-

Approche générale:



EBIOS-RM-

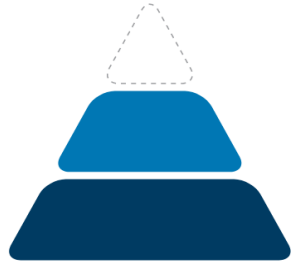
Démarche générale:



EBIOS

Démarche générale:

Atelier 1: Cadrage et socle de sécurité



- Sert à identifier les **objets, participants** et **cadre** de l'étude
- Un recensement des **biens essentiels** (valeurs métiers), **biens supports** et **missions**
- Identifier les **événements redoutés** et leurs gravités
- Définir le **socle** de sécurité
- Cet atelier suivre l'approche « **par conformité** »

EBIOS

Démarche générale:

Atelier 2: **Sources de risque**

- Sert à identifier les **sources de risque (SR)** et **leurs objectifs visés (OV)**
- Juger la pertinence des couples SR/OV par rapports au système d'information
- Formaliser les SR retenus en cartographie

EBIOS

Démarche générale:

Atelier 3: Scénarios stratégiques

- Permet d'avoir une vision claire des **écosystèmes**
- Cartographier les **menaces** par rapport au objets
- Définir des scénarios d'attaque de haut niveau appelés « **scénarios stratégiques** »
- Ces scénarios sont évalués par rapport à leurs gravités

EBIOS

Démarche générale:

Atelier 4: **Scénarios opérationnels**

- Construire des **scénarios techniques** reprenant les modes opératoires susceptibles d'être utilisés par les sources de risque pour réaliser les scénarios stratégiques

- Suivre le même principe de l'atelier 3 mais en focalisant sur les **biens supports** critiques

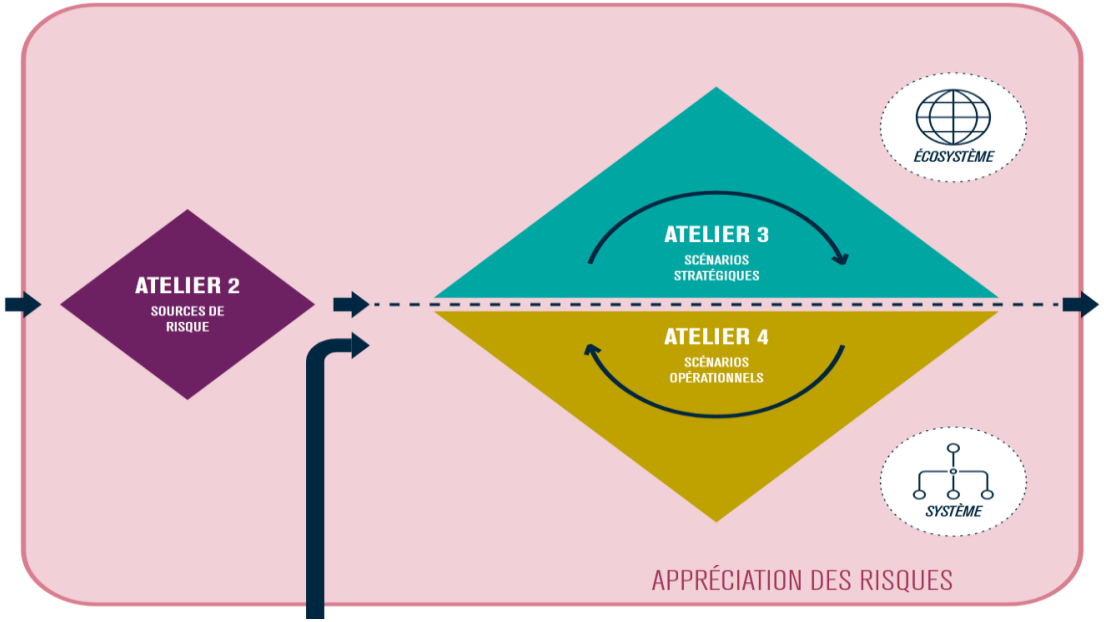
- Ces scénarios sont évalués aussi selon leurs vraisemblances

EBIOS

Démarche générale:
Appréciation de risque

- Les ateliers **3** et **4** se complètent d'une façon itérative

- Les ateliers **2**, **3** et **4** ensemble permettent une appréciation des risques ce qui le dernier étage du **pyramide de management du risque numérique**



EBIOS

Démarche générale:

Atelier 5: **Traitement du risque**

- Faire la synthèse des risques identifiés
- Établir une stratégie de sécurité répondant à ces risques
- Définir un cadre de suivie des risques

EBIOS

Démarche générale:

cycles:

- Deux cycles sont observés:
  - ✓ **Cycle stratégique** permet la révision de l'étude en particulier les scénarios stratégiques
  - ✓ **Cycle opérationnel** permet la révision des scénarios opérationnel vis-à-vis les incidents de sécurité et nouveautés du domaine