

# **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 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:

Phases

- |  |  |  |   |  |
|--|--|--|---|--|
| <ul style="list-style-type: none"> <li>• Perception d'un besoin</li> <li>• Expression des besoins</li> <li>• Création d'un projet</li> </ul> | <ul style="list-style-type: none"> <li>• Formalisation de besoins fonctionnels</li> <li>• Étude de marché</li> <li>• Étude de faisabilité</li> <li>• Analyse de coût</li> <li>• Planification</li> <li>• Identification des entrée/sortie</li> </ul> | <ul style="list-style-type: none"> <li>• Développement logiciel ou matériel</li> <li>• Construction de prototype</li> <li>• Tests utilisateurs</li> <li>• Documentation</li> </ul> | <ul style="list-style-type: none"> <li>• Déploiement dans l'environnement de production</li> <li>• Test de performance</li> <li>• Maintien en Condition Opérationnelle</li> <li>• Exploitation</li> </ul> | <ul style="list-style-type: none"> <li>• Libération des ressources</li> <li>• Fin du projet</li> </ul> |
|--|--|--|---|--|

Étude /  
Initialisation

Conception

Implémentation /  
Prototype / Test

Exploitation /  
Maintenance

Fin de vie

Sécurité

- |   |   |  |   |  |
|---|---|--|---|--|
| <ul style="list-style-type: none"> <li>• Analyse de risques amont</li> <li>• Consultation des équipes sécurité</li> </ul> | <ul style="list-style-type: none"> <li>• Analyse de risques</li> <li>• Proposition de mesures de sécurité</li> <li>• Identification des risques résiduels</li> <li>• Expressions de besoins de sécurité</li> <li>• Estimation de coûts</li> </ul> | <ul style="list-style-type: none"> <li>• Développement</li> <li>• Prise en compte des bonnes pratiques</li> <li>• Top 10 OWASP<sup>1</sup></li> <li>• Validation sécurité</li> <li>• Contrôle des mesures de sécurité</li> </ul> | <ul style="list-style-type: none"> <li>• Maintien en condition de sécurité</li> <li>• Gestion des incidents</li> <li>• Analyse Forensique</li> <li>• Sauvegarde</li> <li>• Supervision de sécurité</li> <li>• Veille de sécurité</li> <li>• Audit (technique, opérationnel)</li> <li>• Tests d'intrusion</li> <li>• Résilience</li> </ul> | <ul style="list-style-type: none"> <li>• Archivage des informations</li> <li>• Effacement sécurisé</li> <li>• Réversibilité</li> <li>• Mise au rebut</li> <li>• Obsolescence des configurations</li> </ul> |
|---|---|--|---|--|

# Sécurité des SI

## Méthode EBIOS:

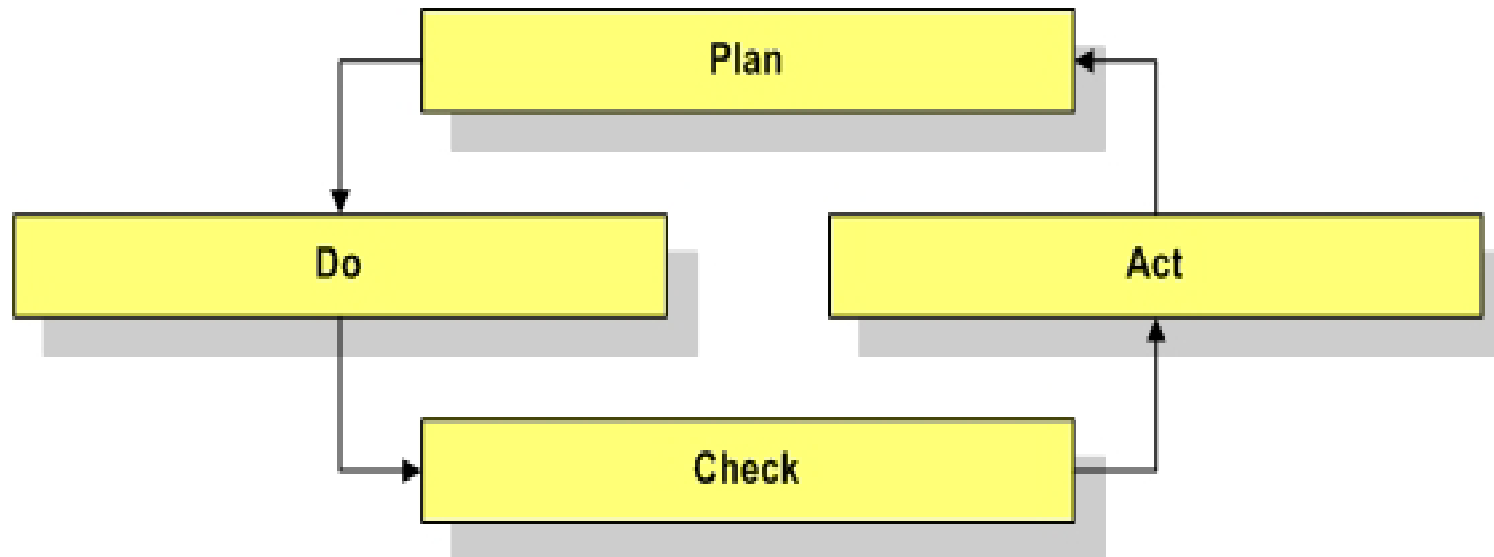
Une méthode d'analyse des risques qui peut être appliquée sur un système **à concevoir** ou **existant**

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



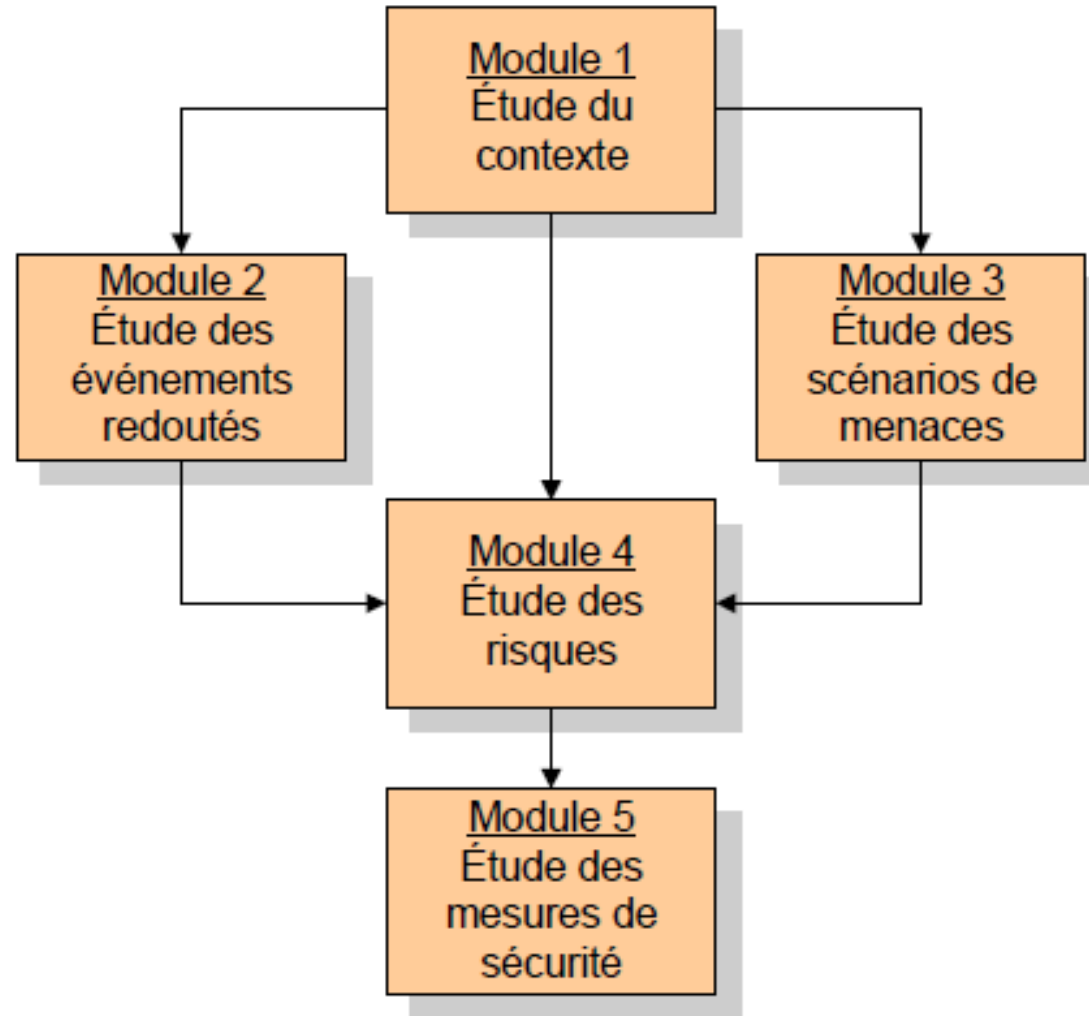
## Méthode d'étude et non pas de sécurisation:

- 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:

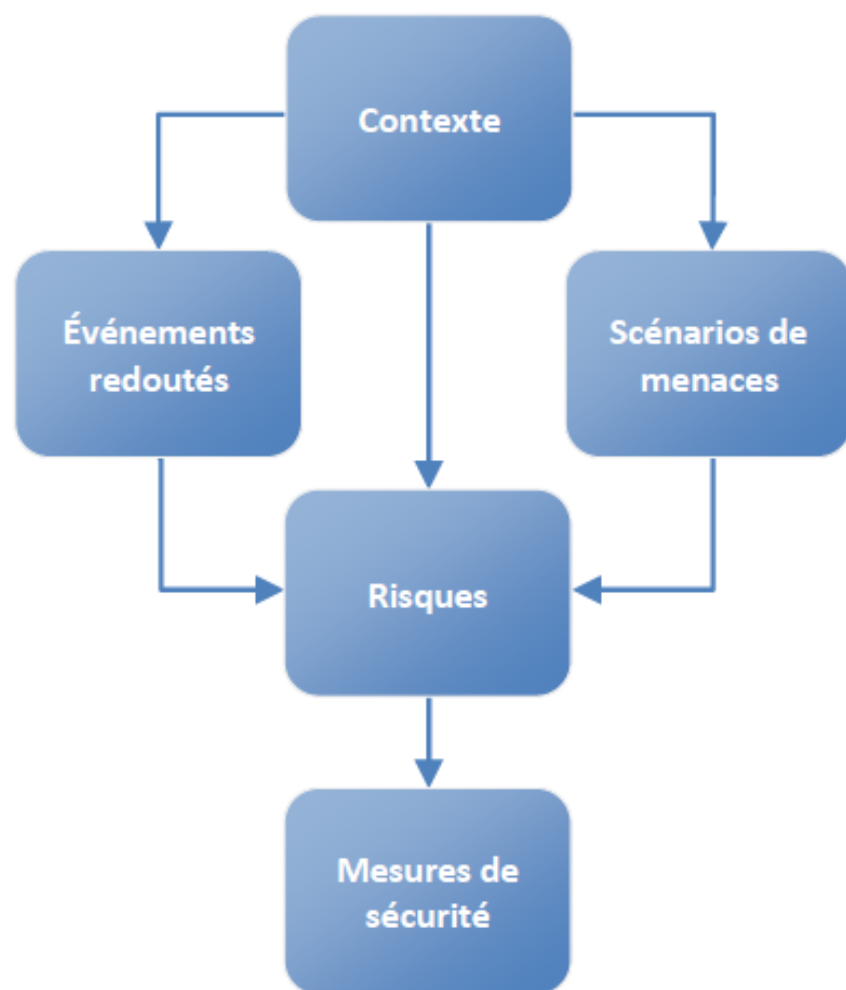




# Démarche générale d'EBIOS

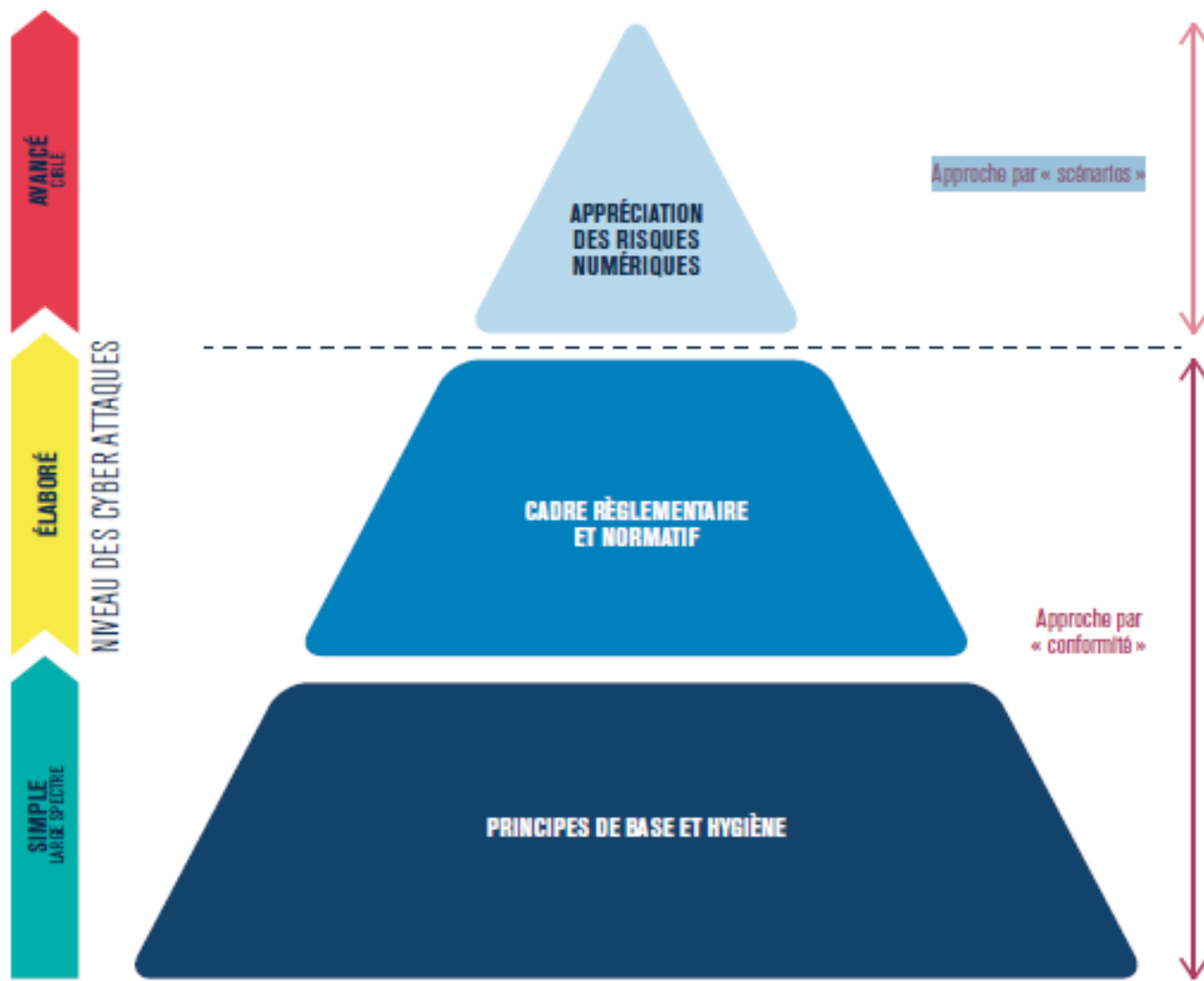


# Les 10 questions essentielles pour gérer les risques

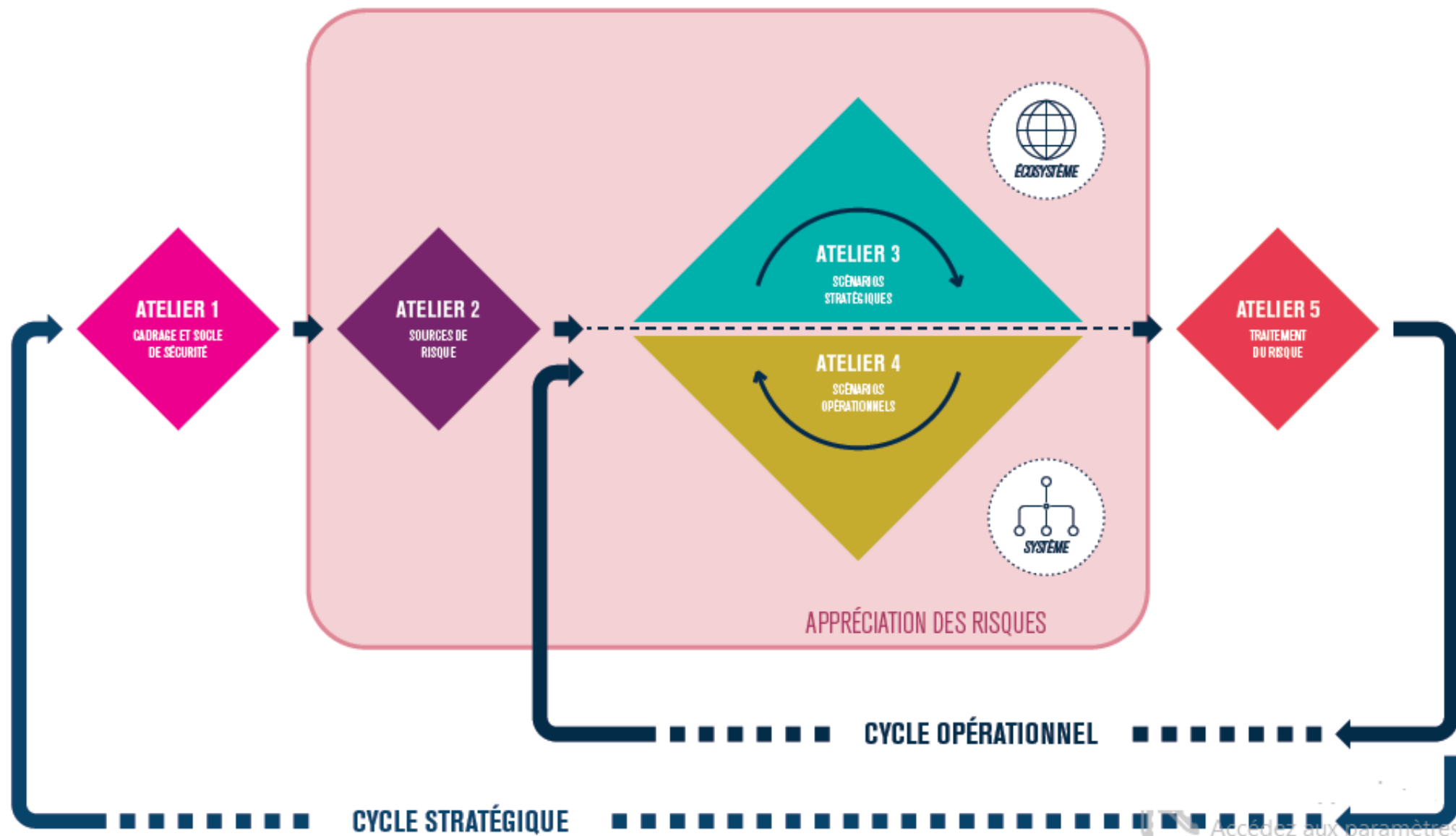


<b>Contexte</b>	<ul style="list-style-type: none"><li>• Pourquoi et comment va-t-on gérer les risques ?</li><li>• Quel est le sujet de l'étude ?</li></ul>
<b>Événements redoutés</b>	<ul style="list-style-type: none"><li>• Quels sont tous les événements craints ?</li><li>• Quels seraient les plus graves ?</li></ul>
<b>Scénarios de menaces</b>	<ul style="list-style-type: none"><li>• Quels sont tous les scénarios possibles ?</li><li>• Quels sont les plus vraisemblables ?</li></ul>
<b>Risques</b>	<ul style="list-style-type: none"><li>• Quelle est la cartographie des risques ?</li><li>• Comment choisit-on de les traiter ?</li></ul>
<b>Mesures de sécurité</b>	<ul style="list-style-type: none"><li>• Quelles mesures devrait-on appliquer ?</li><li>• Les risques résiduels sont-ils acceptables ?</li></ul>

# La pyramide d'EBIOS



# EBIOS Processus itératif à 5 ateliers



## Exemple:

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

