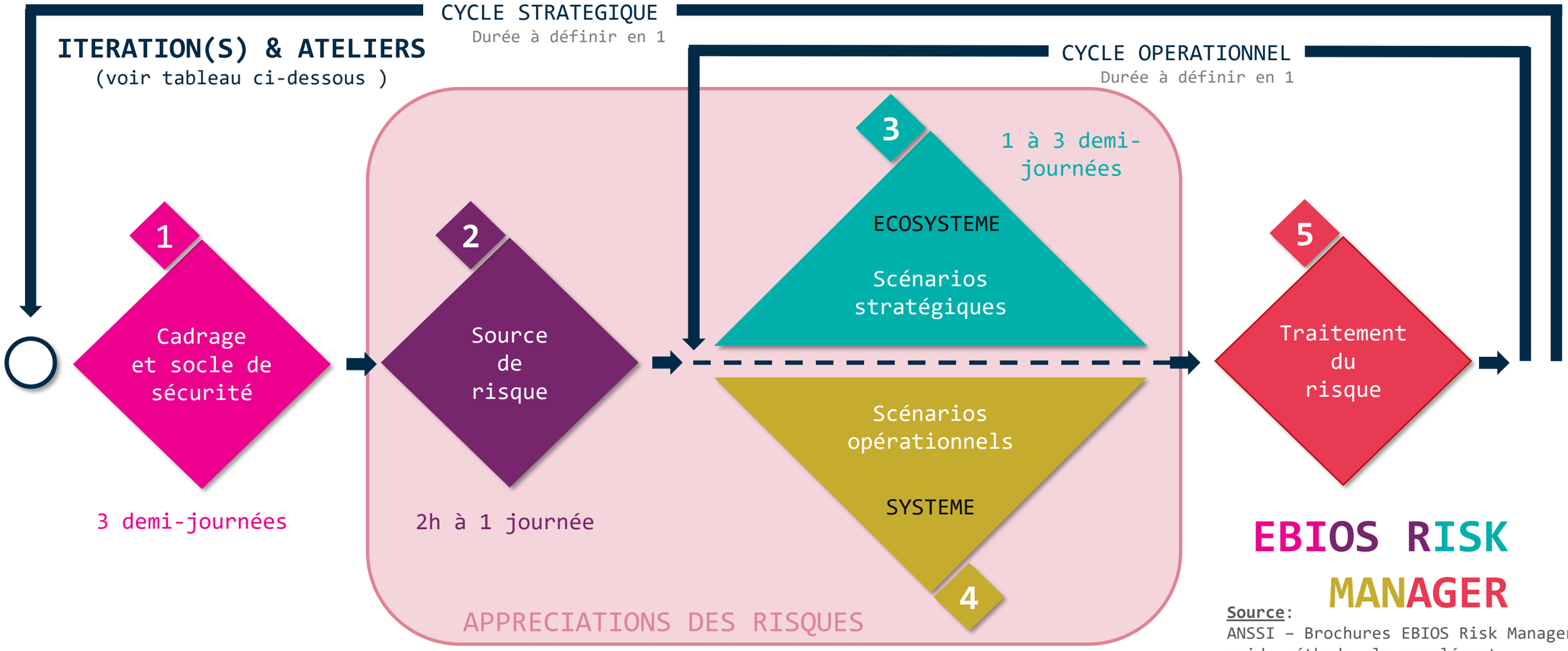
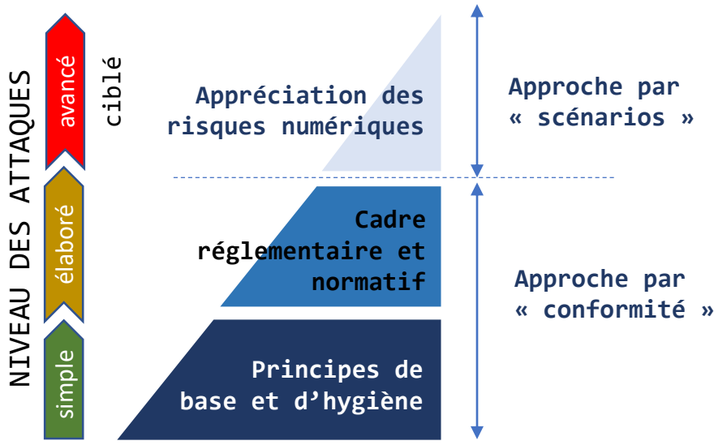


EBIOS RISK MANAGER

Source:
ANSSI – Brochures EBIOS Risk Manager: guide méthode, le supplément

Atelier 1 - Définition du cadre de l'étude, son périmètre métier et technique, les événements redoutés associés (ER) et le socle de sécurité.

Atelier 2 - Identification des sources de risque (SR) et leurs objectifs visés (OV), en lien avec le contexte particulier de l'étude.



Pyramide du management des risques

Atelier 3 - Avoir une vision claire de l'écosystème, afin d'en identifier les parties prenantes les plus vulnérables. Bâtir des scénarios de haut niveau (scénarios stratégiques).

Atelier 4 - Construction des scénarios opérationnels, scénarios techniques reprenant les modes opératoires susceptibles d'être utilisés par les SR pour réaliser les scénarios stratégiques.

Atelier 5 - Réalisation d'une synthèse de l'ensemble des risques étudiés en vue de définir une stratégie de traitement du risque.

Objectifs de l'étude & ateliers à jouer	1	2	3	4	5
Identifier le socle de sécurité adapté à l'objet de l'étude	X				
Être en conformité avec les référentiels de sécurité numérique	X				X
Évaluer le niveau de menace de l'écosystème vis-à-vis de l'objet de l'étude			X		
Identifier et analyser les scénarios de haut niveau, intégrant l'écosystème		X	X		
Réaliser une étude préliminaire de risque pour identifier les axes prioritaires d'amélioration de la sécurité	X	X	X		X
Conduire une étude de risque complète et fine, par exemple sur un produit de sécurité ou en vue de l'homologation d'un système	X	X	X	X	X

Atelier 1 - Cadrage et socle de sécurité

[approche « conformité »]

Participants

Direction | Métiers | RSSI | DSI

Etapes

a Définir le cadre de l'étude: objectifs, participants (RACI), cadre temporel (cycle)

b Définir le périmètre métier et technique de l'objet étudié (missions, VM, BS) → tableau (mission, VM, BS)

c Identifier les événements redoutés et évaluer leur niveau de gravité → tableau (VM, ER, impacts, gravité)

d Déterminer le socle de sécurité.

Livrables

- éléments de cadrage : objectifs visés, rôles et responsabilités, cadre temporel ;
- périmètre métier & technique : missions, VM, BS
- ER & niveau de gravité
- socle de sécurité : liste référentiels applicables, état d'application, identification et justification des écarts

Echelle	Conséquences
G4 Critique Survie menacée	Incapacité pour la société d'assurer tout ou partie de son activité, avec d'éventuels impacts graves sur la sécurité des personnes et des biens.
G3 Grave Mode très dégradé	Forte dégradation des performances de l'activité, avec d'éventuels impacts significatifs sur la sécurité des personnes et des biens.
G3 Significative Mode dégradé	Dégradation des performances de l'activité sans impact sur la sécurité des personnes et des biens.
G1 Mineure	Aucun impact opérationnel ni sur les performances de l'activité ni sur la sécurité des personnes et des biens.

Cotation de la gravité

Atelier 2 - Sources de risque

Participants

Direction | Métiers | RSSI
Eventuellement un spécialiste en analyse de la menace numérique

Etapes

a Identifier SR et OV

b Evaluer les couples SR/OV → tableau (SR, OV, motivation, ressources, activité, **pertinence**)

c Sélectionner les couples SR/OV jugés prioritaires pour poursuivre l'analyse.

Livrables

- liste couples (SR,OV) prioritaires retenus pour la suite de l'étude ;
- liste couples (SR,OV) secondaires susceptibles d'être étudié dans un second temps et qui feront l'objet d'une surveillance attentive
- cartographie des SR.

Atelier 4 – Scénarios opérationnels

Participants

RSSI | DSI
Éventuellement un spécialiste en cybersécurité

Etapes

a Elaborer les scénarios opérationnels

b Evaluer leur vraisemblance → tableau (chemins attaque S+0, vraisemblance globale)

Livrables

- liste scénarios opérationnels et vraisemblance

Abréviations

- BS : Biens Supports
- ER : Elément Redouté
- OV : Objectif Visé
- PACS : Plan Amélioration Continue Sécurité
- PP : Partie Prenante
- PPC : Partie Prenante Critique
- VM : Valeur Métier

Atelier 3 – Scénarios stratégiques

[étude préliminaire du risque]

Participants

Métiers | Architectes fonctionnels | RSSI
Éventuellement un spécialiste en cybersécurité

Etapes

a Construire la cartographie de menace numérique de l'écosystème et sélectionner les PPC → carte menace (PP, exposition, fiabilité)

b Elaborer des scénarios stratégiques → graphes d'attaque, tableau scénarios (SR, OV, chemins attaque, gravité)

c Définir des mesures de sécurité sur l'écosystème → tableau scénarios (PP, chemins attaque, mesures sécurité, menace initiale, menace résiduelle)

Livrables

- cartographie menace numérique de l'écosystème et PPC
- scénarios stratégiques et ER
- mesures de sécurité retenues pour l'écosystème.

Atelier 5 – Traitement du risque

[stratégie de traitement du risque]

Participants

Direction | Métiers | RSSI | DSI

Etapes

a Réaliser la synthèse des scénarios de risque → matrice risque initial (scénario, gravité, vraisemblance)

b Définir la stratégie de traitement du risque et les mesures de sécurité → matrice stratégie traitement risque (scénario, gravité, vraisemblance) , PACS (tableau)

c Evaluer et documenter les risques résiduels

d Mettre en place le cadre de suivi des risques → indicateurs de pilotage

Livrables

- stratégie de traitement du risque ;
- synthèse des risques résiduels ;
- plan d'amélioration continue de la sécurité ;
- cadre du suivi des risques.