

Méthodes d'Analyse de Risques

 par Stéphane LARCHER



La feuille de route

Introduction à la Gestion des Risques

Concepts fondamentaux et processus de gestion des risques

Méthodes Françaises d'Analyse des Risques

EBIOS Risk Manager et MEHARI

Méthodes Internationales de Cybersécurité

OCTAVE, NIST RMF, ISO/IEC 27005, FAIR et CRAMM

Méthodes Industrielles et Sectorielles

AMDEC, HAZOP et Méthode Bow-Tie

Méthodes Émergentes et Spécialisées

Cyber Value at Risk, STRIDE, PASTA et Attack Trees

Comparaison et Sélection des Méthodes

Matrice comparative et critères de sélection

Applications Pratiques et Cas d'Usage

Exercices pratiques et workshops



Concepts Fondamentaux

Risque

ISO 31000 : "Effet de l'incertitude sur l'atteinte des objectifs"

Formule classique : $\text{Risque} = \text{Probabilité} \times \text{Impact}$

Vision moderne : $\text{Risque} = \text{Menace} \times \text{Vulnérabilité} \times \text{Impact}$

Gestion des Risques

Processus d'identification, d'évaluation et de traitement des risques

Approche systématique et continue

Intégration dans la gouvernance organisationnelle

Analyse des Risques

Phase du processus de gestion des risques

Compréhension détaillée de la nature du risque

Estimation du niveau de risque

Classification des Risques

Par Nature

- Risques stratégiques : Menacent les objectifs business
- Risques opérationnels : Affectent les processus quotidiens
- Risques techniques : Liés aux systèmes et technologies
- Risques réglementaires : Non-conformité aux exigences légales

Par Origine

- Risques internes : Générés par l'organisation
- Risques externes : Imposés par l'environnement
- Risques mixtes : Combinaison des deux

Cycle de Vie Standard (ISO 31000)

Établissement du contexte

Objectifs et périmètre

Critères d'évaluation

Structure organisationnelle

Surveillance et revue

Monitoring continu

Mise à jour

Amélioration

Traitement des risques

Stratégies de traitement

Plan d'action

Mise en œuvre



Identification des risques

Inventaire exhaustif

Caractérisation des risques

Documentation

Analyse des risques

Évaluation de la probabilité

Estimation de l'impact

Niveau de risque

Évaluation des risques

Comparaison avec critères

Priorisation

Acceptabilité

Communication et Consultation

Parties prenantes

- Direction et gouvernance
- Équipes opérationnelles
- Experts techniques
- Parties externes

Modalités

- Reporting régulier
- Workshops d'analyse
- Formation et sensibilisation
- Documentation partagée

EBIOS Risk Manager



Atelier 1 : Cadrage et socle de sécurité

Définition du périmètre d'étude et identification des biens supports



Atelier 2 : Sources de risque

Identification des sources de risque et analyse de leurs motivations



Atelier 3 : Scénarios stratégiques

Construction des chemins d'attaque et évaluation de la gravité



Atelier 4 : Scénarios opérationnels

Déclinaison technique des scénarios et évaluation de la vraisemblance



Atelier 5 : Traitement du risque

Stratégies de traitement et plan d'action priorisé

EBIOS Risk Manager - Avantages et Limites

Avantages

- Approche moderne par scénarios
- Prise en compte du contexte métier
- Méthode officielle française
- Documentation complète et gratuite
- Adaptable à tous secteurs

Limites

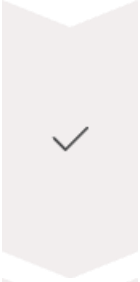
- Complexité de mise en œuvre
- Nécessite une expertise importante
- Peut être chronophage
- Moins connue à l'international



MEHARI



- Phase 1 : Classification et enjeux
- Identification des enjeux de sécurité
- Classification des informations
- Définition des niveaux de sécurité requis



- Phase 2 : Audit des mesures
- Évaluation des mesures de sécurité existantes
- Utilisation de la base de connaissances
- Notation de l'efficacité des mesures



- Phase 3 : Analyse des risques
- Calcul automatique des risques résiduels
- Identification des vulnérabilités critiques
- Priorisation des actions



- Phase 4 : Plan de sécurité
- Sélection des mesures à implémenter
- Planification et budgétisation
- Suivi et mise à jour

MEHARI - Base de Connaissances



Structure

Services de sécurité : 39 services identifiés

Mesures de sécurité : Plus de 300 mesures

Métriques : Échelles de mesure standardisées

Règles de calcul : Algorithmes de calcul des risques



Domaines Couverts

Organisation de la sécurité

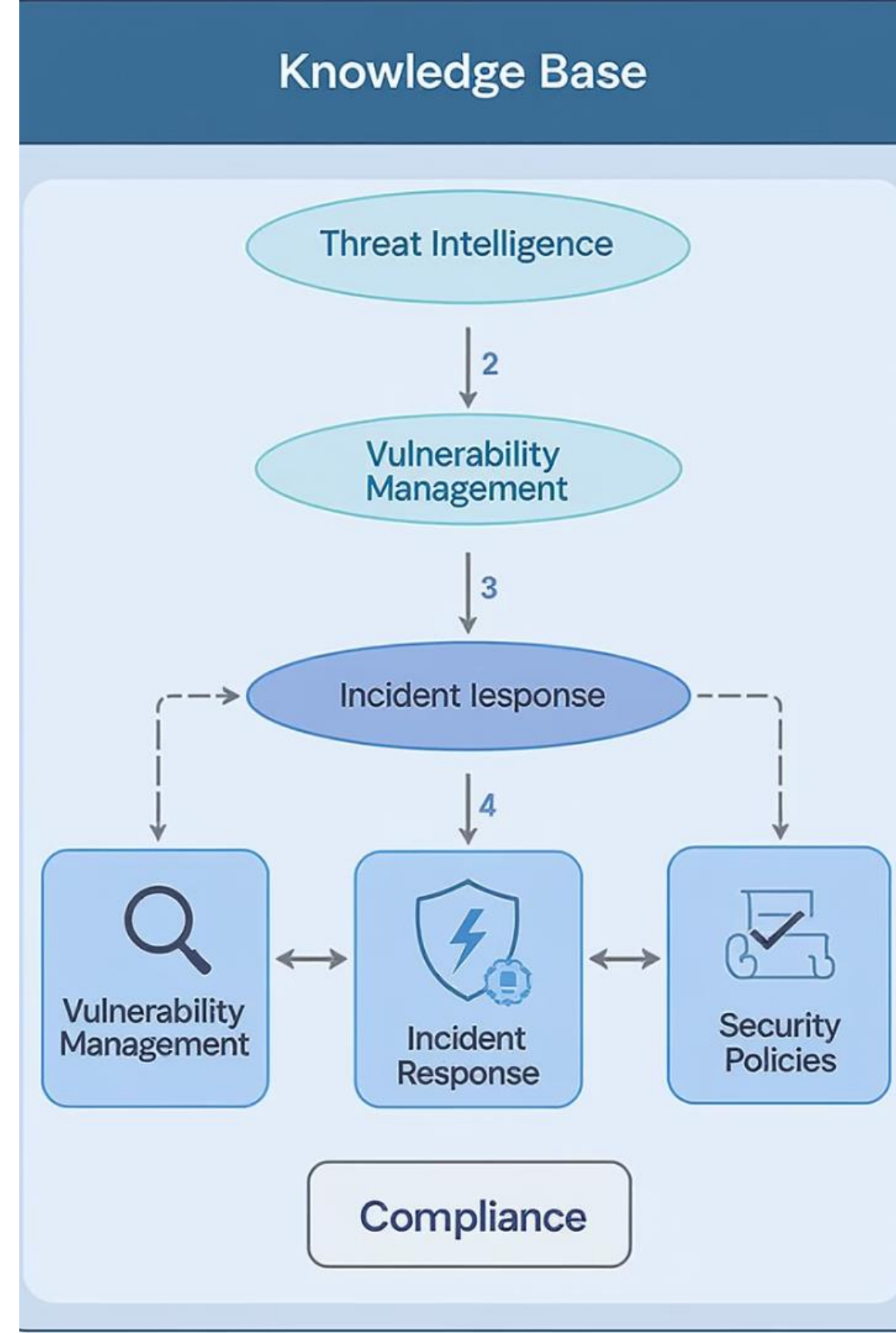
Sécurité physique et environnementale

Gestion des communications et des opérations

Contrôle d'accès

Développement et maintenance des systèmes

Gestion de la continuité d'activité



MEHARI - Avantages et Limites

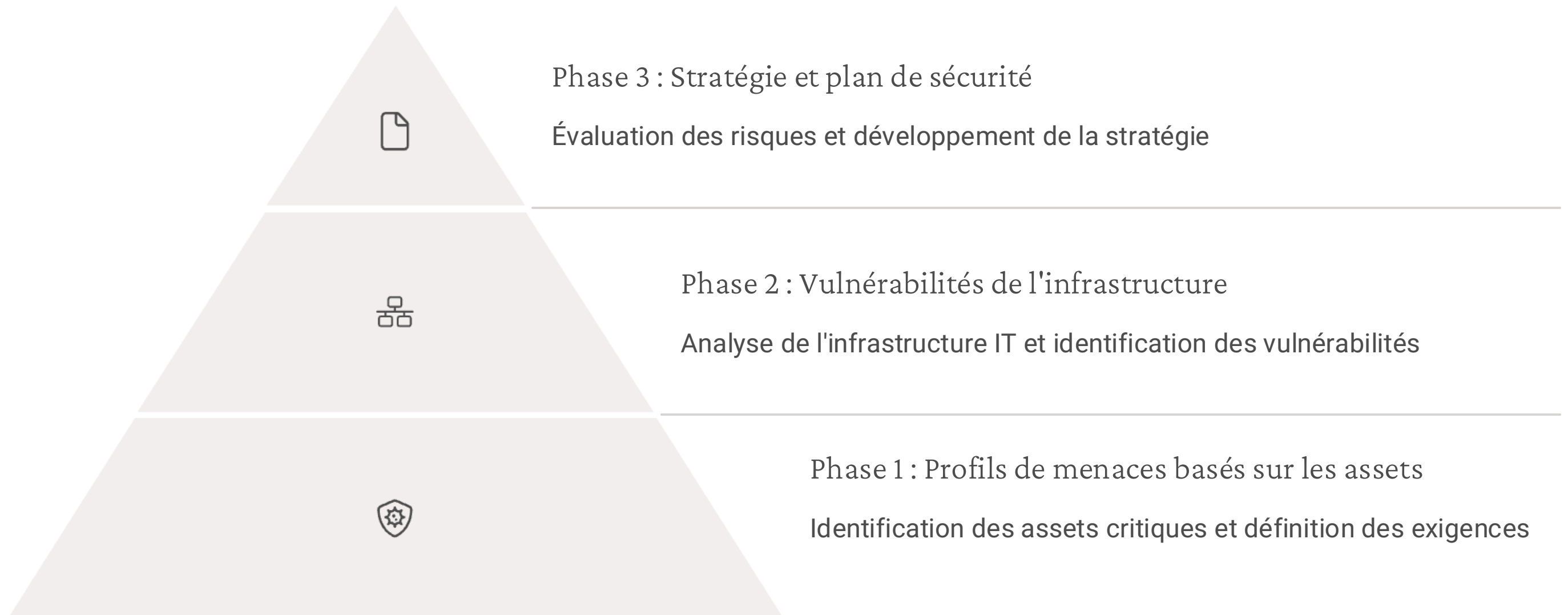
Avantages

- Approche quantitative rigoureuse
- Base de connaissances riche
- Calculs automatisés
- Résultats reproductibles
- Suivi dans le temps facilité

Limites

- Complexité de paramétrage
- Rigidité de la méthode
- Nécessite une expertise MEHARI
- Moins adaptée aux nouvelles menaces

OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation)





OCTAVE Allegro (Version Simplifiée)

Étapes 1-2

Établir les critères de mesure des risques et développer un profil d'information asset

Étapes 3-4

Identifier les conteneurs d'information et les zones de préoccupation

Étapes 5-6

Identifier les scénarios de menace et les risques

Étapes 7-8

Analyser les risques et sélectionner les stratégies de mitigation

OCTAVE - Avantages et Limites

Avantages

- Approche centrée business
- Auto-évaluation (appropriation)
- Méthode collaborative
- Focus sur les assets critiques
- Adaptabilité organisationnelle

Limites

- Nécessite forte implication interne
- Peut manquer d'expertise externe
- Subjectivité dans l'évaluation
- Moins de guidance technique

NIST Risk Management Framework (RMF)

1. Prepare
Stratégie organisationnelle de gestion
des risques

7. Monitor
Surveillance continue

6. Authorize
Décision d'acceptation du risque



2. Categorize
Classification selon FIPS 199

3. Select
Choix des contrôles de sécurité

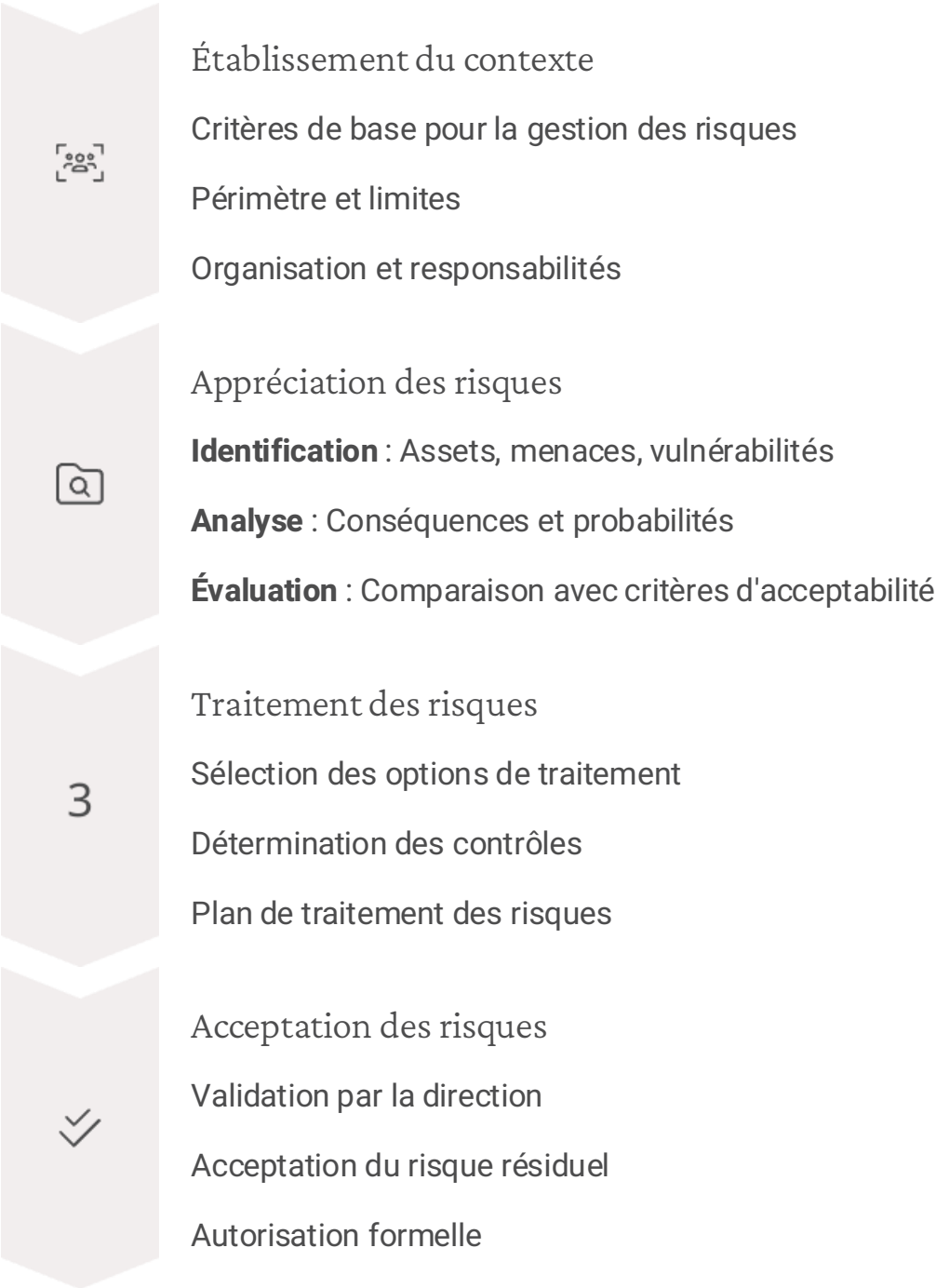
4. Implement
Déploiement des contrôles

5. Assess
Test de l'efficacité des contrôles

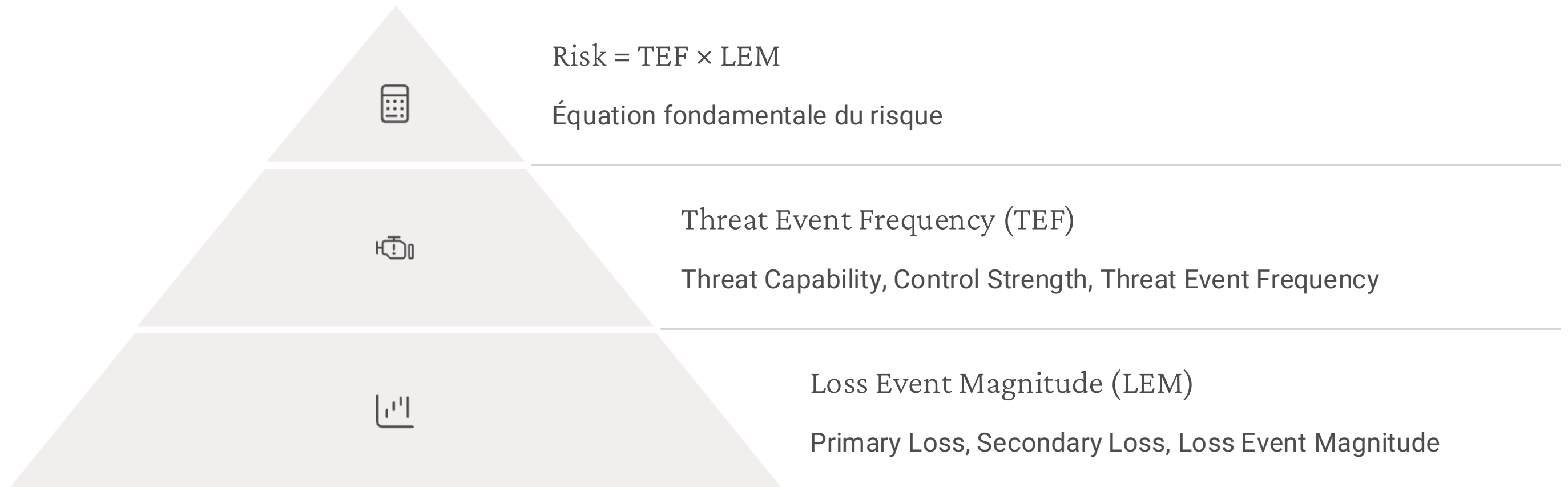
Risk Management Process



ISO/IEC 27005 - Gestion des Risques



FAIR (Factor Analysis of Information Risk)





FAIR - Processus d'Analyse

Étape 1 : Définir le scénario

Asset concerné, Threat community, Effect recherché

Étape 3 : Modéliser

Définition des ranges, Distributions de probabilité, Simulation Monte Carlo

Étape 2 : Rassembler les informations

Données historiques, Expert judgment, Sources externes

Étape 4 : Analyser les résultats

Distribution des pertes, Métriques de risque (VaR, TVaR), Analyse de sensibilité

FMEA



Brainstorm for
Failure Modes presented
list potential effects everactizing,
Potential effect, for wessial Failure,
cafect a quning, as furnsbly.
effects failure rerview, ful monity.



Assigning Prx effects
Raning: a the pate trital disonauges



Assigning Occerence
Ranking: a phankings for clanings



Assigning Detection
Ranking: ges for tast dialetes



Calculating Risk Priority
Number is even, last heo to rankings

AMDEC (Analyse des Modes de Défaillance, de leurs Effets et de leur Criticité)



Étape 1 : Préparation

Constitution de l'équipe

Définition du périmètre

Décomposition fonctionnelle



Étape 2 : Analyse

Identification des modes de défaillance

Analyse des causes

Évaluation des effets



Étape 3 : Évaluation

Gravité (G) : Sévérité des conséquences (1-10)

Occurrence (O) : Fréquence d'apparition (1-10)

Détection (D) : Capacité de détection (1-10)

Criticité = G × O × D



Étape 4 : Actions

Priorisation selon criticité

Plan d'actions correctives

Suivi et mise à jour