RISK MANAGEMENT: MAÎTRISER LES RISQUES EN MATIÈRE DE SÉCURITÉ DE L'INFORMATION

Par Mehdi Nacer KERKAR
& Abdelkarim YAHIAOUI

LE BUT DE LA GESTION DES RISQUES

S'assurer que les affaires et les actifs de l'entreprise sont en sécurité

Protéger contre les désavantages concurrentiels

Conformité aux lois et aux meilleures pratiques commerciales

Maintenir une bonne réputation publique

CONCEPTS DE LA GESTION DES RISQUES

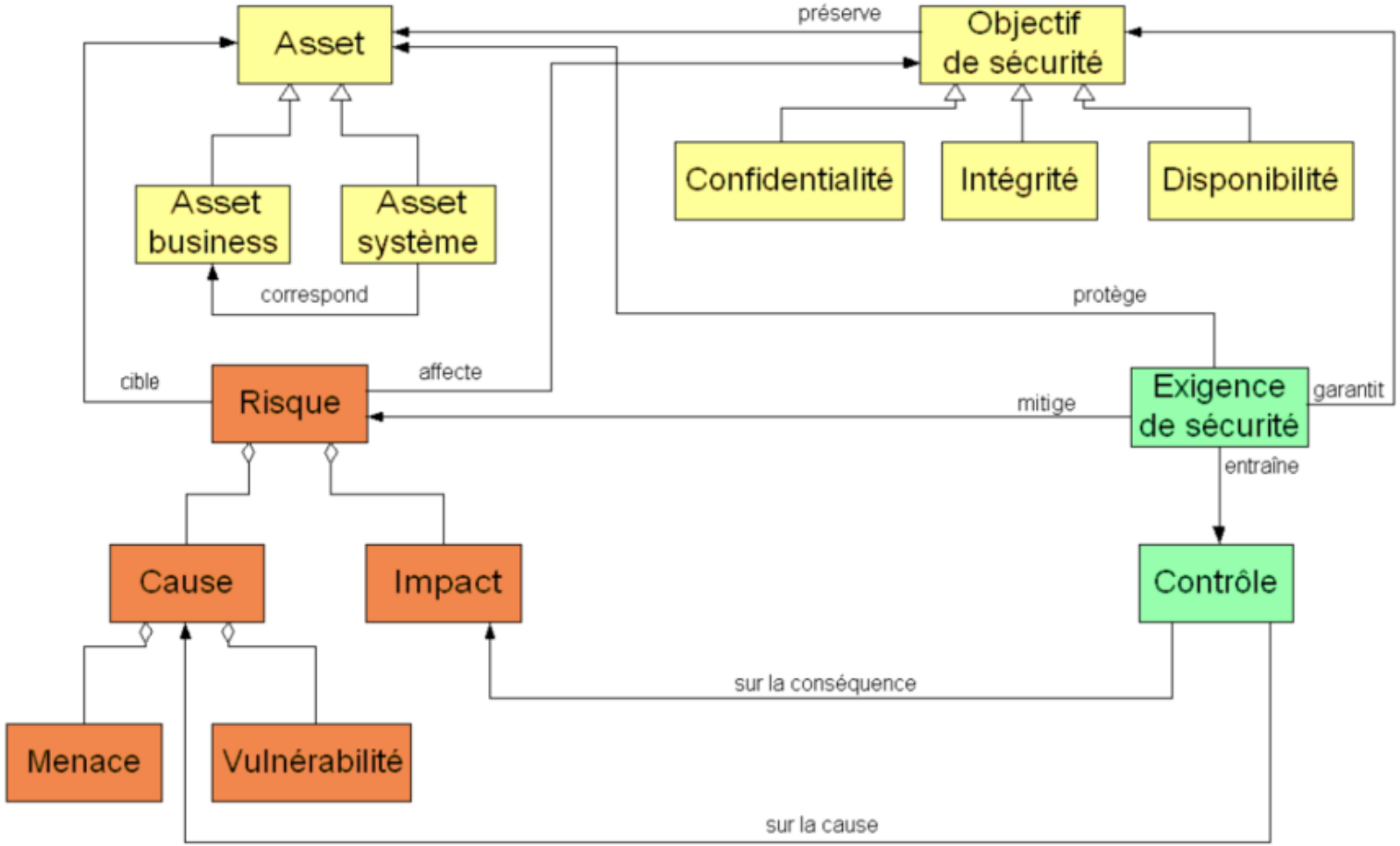


Figure 1: Les concepts de la gestion des risques

PROCESSUS DE GESTION DES RISQUES

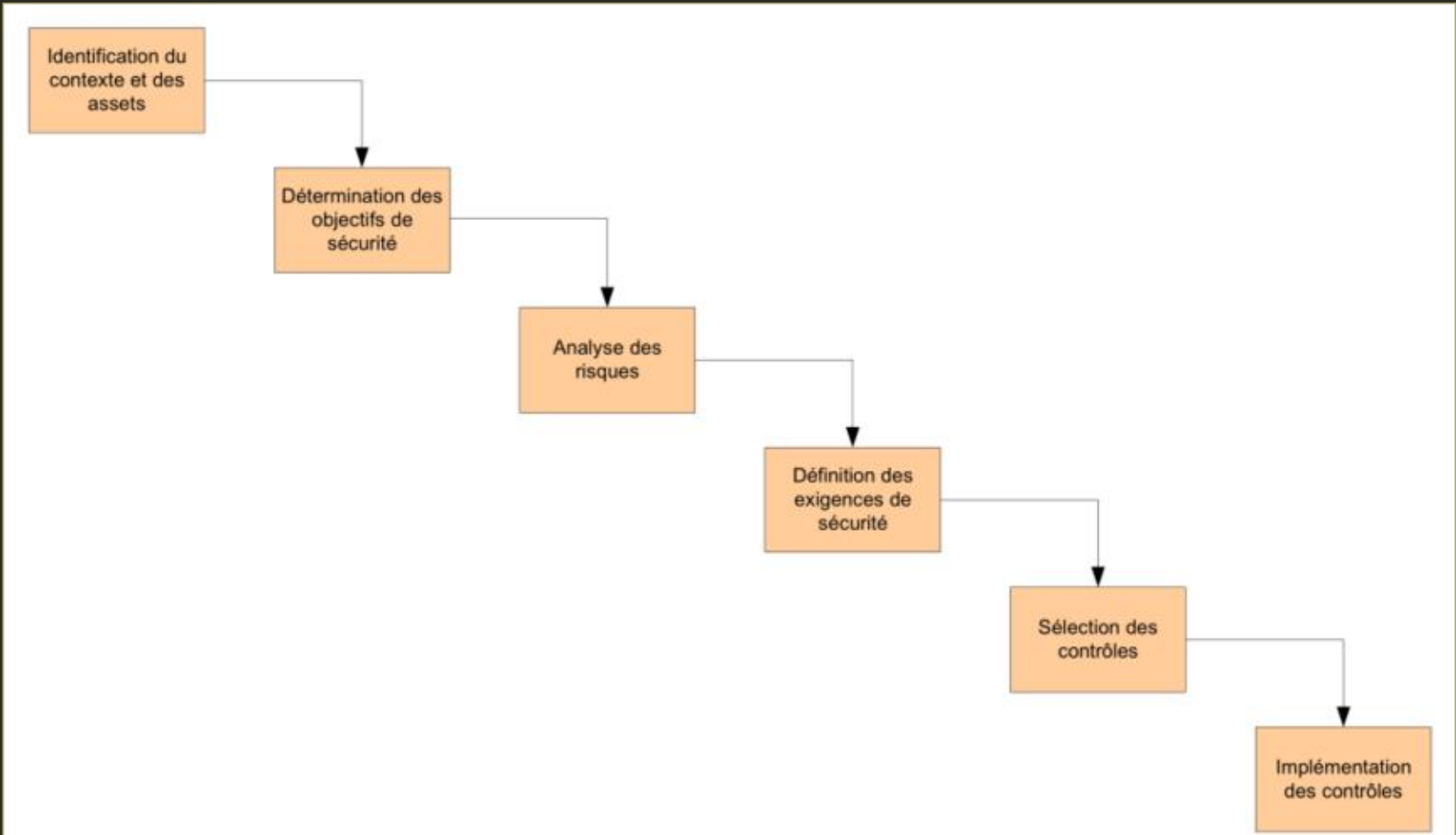


Figure 2: Le processus de gestion des risques

ÉTAPES D'UN PLAN DE GESTION DES RISQUES

Étape 1: Identifiez le risque

Étape 2: Évaluer le risque

Étape 3: Contrôle du risque

Les étapes sont similaires quel que soit le contexte (InfoSec, Sécurité physique, Financier, etc.)

Cette présentation portera sur la maîtrise des risques dans un contexte InfoSec.

IDENTIFICATION DES RISQUES

Les étapes de l'identification des risques sont les suivantes:

- Identifiez les ressources d'information de votre organisation
- Classer et catégoriser ces actifs en groupes utiles
- Classez la nécessité d'actifs à l'organisation

À droite, un exemple simplifié de la manière dont une entreprise peut identifier les risques

Actifs	Type d'actif et sous-catégorie	Fonction d'actif	Niveau de priorité (faible, moyen, élevé, critique)
Bob Employé	Personnel: SecInfo	• Réseaux sécurisés • Tests de d'intrusion • Faire du café	Faible
Blade Serveur Cisco UCS B460 M4	Matériel: mise en réseau	• Serveur de base de données	Elevé
Informations personnellement identifiables du client (PII)	Données: informations confidentielles	• Fournir des informations pour toutes les transactions commercials	Critique
Windows 7	Logiciel: Système d'exploitation	• Accès des employés aux logiciels d'entreprise	Moyen

ANALYSE DES RISQUES

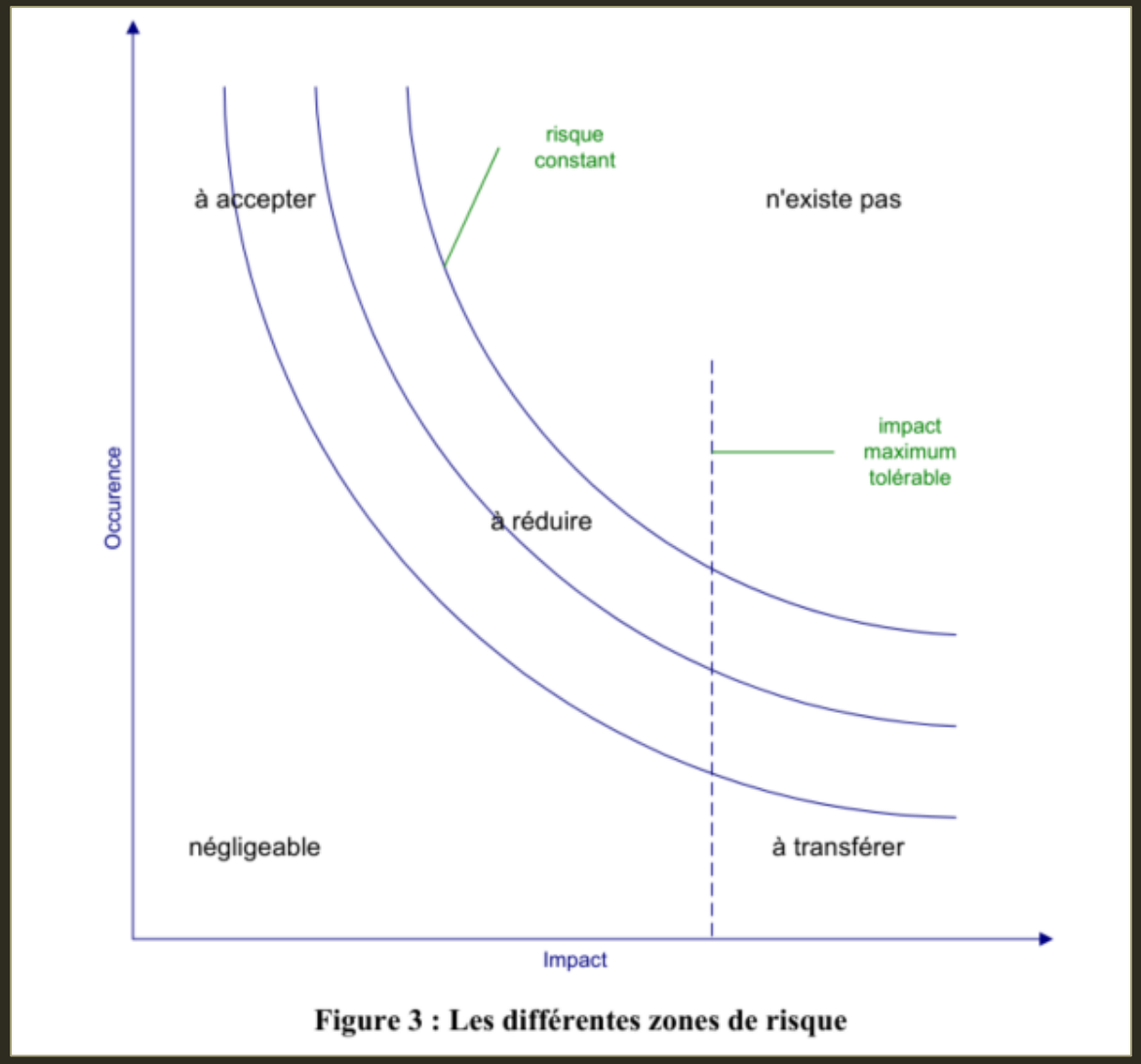


Figure 3 : Les différentes zones de risque

L'ÉVALUATION DES RISQUES

Les étapes de l'évaluation des risques sont les suivantes:

- Identifier les menaces et les agents de menace
- Prioriser les menaces et les agents de menace
- Évaluer les vulnérabilités dans le plan InfoSec actuel
- Déterminer le risque de chaque menace

$R = P * V - M + U$

R = Risque

P = probabilité d'attaque par la menace

V = Valeur de l'actif informationnel

M = atténuation par les contrôles actuels

U = Incertitude de vulnérabilité

Le tableau à droite combine des éléments de tous ces éléments dans un format très simplifié

Agent de menace et menace	Actif ciblé	Niveau de menace	Exploits possibles	Risque (échelle de 1-5)
Employé mécontent: vole d'informations sur l'entreprise À revendre	Données de l'entreprise (ex. informations personnelles du client)	Elevé	Informations d'identification du contrôle d'accès, connaissance des stratégies InfoSec, etc.	4.16
Incendie: brûler l'installation ou causer des dommages importants	Installation de l'entreprise, personnel, équipement	Critique	Mauvais équipement	2.78
Hacktivists: écart de qualité de service	Matériel / logiciel de l'entreprise	Faible	Manque de filtrage efficace	1.39

CONTRÔLE DES RISQUES

Les étapes du contrôle des risques sont les suivantes:

- Analyse coûts-avantages
  - Espérance de perte simple
  - Taux d'occurrence annualisé
  - Espérance de perte annuelle
  - Coût annuel de la sauvegarde
- Analyse de faisabilité
  - Faisabilité organisationnelle
  - Faisabilité opérationnelle
  - Faisabilité technique
  - Faisabilité politique
- Mise en œuvre de la stratégie de contrôle des risques

L'ANALYSE COÛTS-AVANTAGES

Déterminer quelles stratégies de contrôle des risques sont rentables

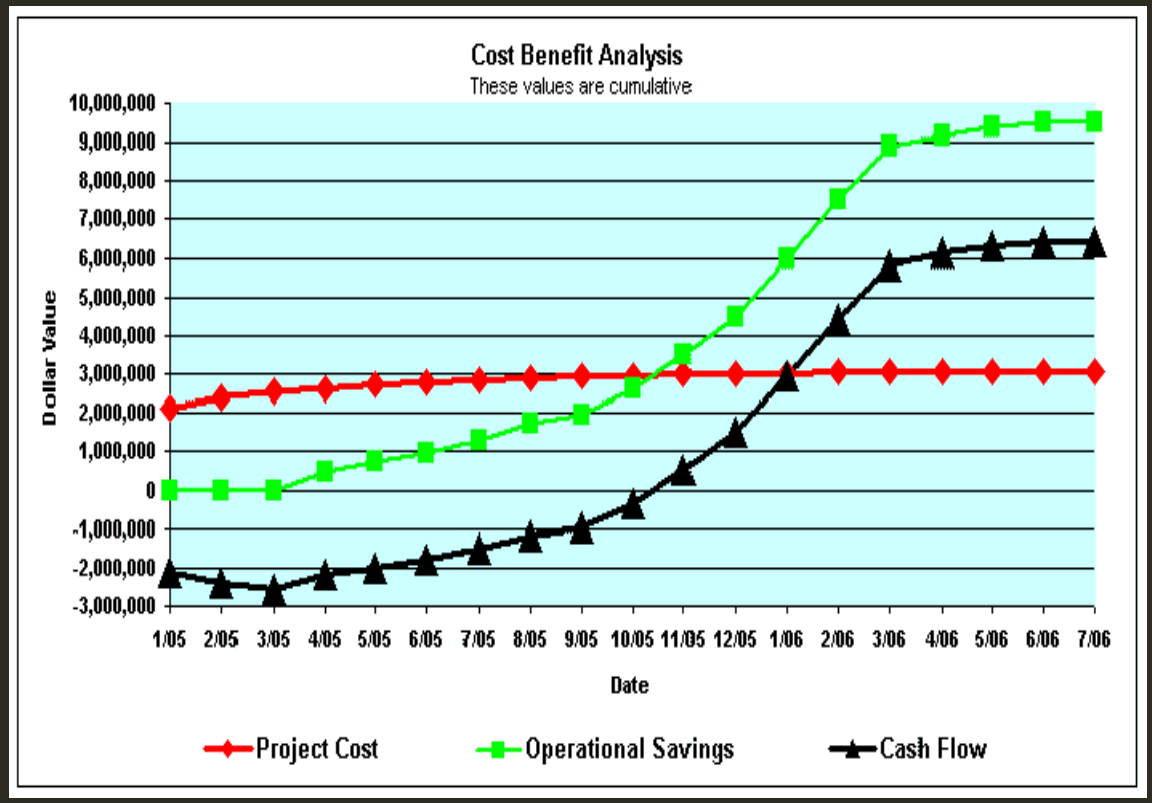
Vous trouverez ci-dessous quelques formules courantes utilisées pour calculer l'analyse coûts-avantages.

SLE = AV * EF

- AV = Valeur de l'actif, EF = Facteur d'exposition (% de l'actif affecté)

ALE = SLE * ARO

CBA = ALE (pré-contrôle) - ALE (post-contrôle) - ACE



ANALYSE DE FAISABILITÉ

Organisation:

- le plan correspond-il aux objectifs de l'organisation?
- Qu'y a-t-il dedans pour l'organisation?
- Limite-t-il les capacités de l'organisation de quelque manière que ce soit?

Opérationnel:

- les actionnaires (utilisateurs, gestionnaires, etc.) seront-ils capables / disposés à accepter le plan?
- Le système est-il compatible avec les nouvelles modifications?
- Les changements possibles ont-ils été communiqués aux employés?

ANALYSE DE FAISABILITÉ

Technique:

- la technologie nécessaire est-elle possédée ou obtenue?
- Nos employés sont-ils formés et sinon pouvons-nous nous permettre de les former?
- Devrions-nous embaucher de nouveaux employés?

Politique:

- SecInfo peut-il obtenir le budget et l'approbation nécessaires pour mettre en œuvre le plan?
- Le budget requis est-il justifiable?
- SecInfo doit-il concurrencer les autres départements pour obtenir le budget souhaité?

STRATÉGIES DE CONTRÔLE DES RISQUES

La défense

Transfert

Atténuation (Mitigation)

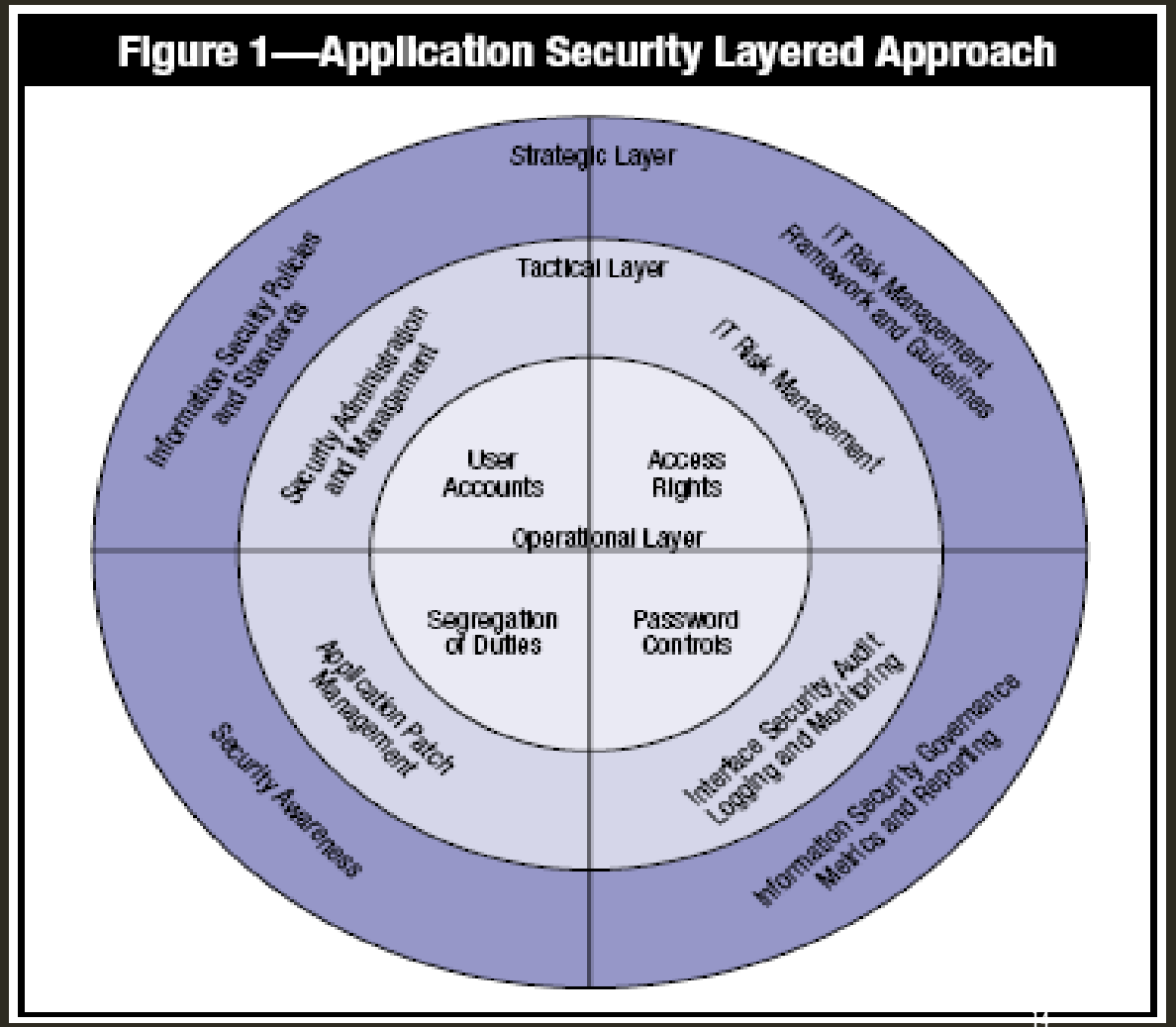
Acceptation (abandon)

Résiliation (Termination)

STRATÉGIE DE CONTRÔLE DES RISQUES: DÉFENSE

Défense: Empêcher l'exploitation du système via l'application de politiques, la formation / éducation et la technologie. Sécurité de préférence stratifiée (défense en profondeur)

- Contrer les menaces
- Supprimer les vulnérabilités d'evaluation
- Limiter l'accès aux actifs
- Ajouter des protections



STRATÉGIE DE CONTRÔLE DES RISQUES: TRANSFERT

Transfert: transfert des risques vers d'autres zones ou des entités extérieures à gérer

Peut inclure:

- Assurance achat
- Externalisation vers d'autres organisations
- Mise en œuvre de contrats de service avec des fournisseurs
- Révision des modèles de déploiement

STRATÉGIE DE CONTRÔLE DES RISQUES: ATTÉNUATION

Atténuation: créer des plans et des préparatifs pour réduire les dégâts causés par l'actualisation de la menace

La préparation devrait inclure:

- Plan d'intervention en cas d'incidence
- Plan de reprise après sinistre
- Plan de continuité d'activité

TABLE 8-1 Summaries of Mitigation Plans

Plan	Description	Example	When deployed	Timeframe
Incident Response Plan (IRP)	Actions an organization takes during incidents (attacks)	■ List of steps to be taken during disaster ■ Intelligence gathering ■ Information analysis	As incident or disaster unfolds	Immediate and real-time reaction
Disaster Recovery Plan (DRP)	■ Preparations for recovery should a disaster occur ■ Strategies to limit losses before and during disaster ■ Step-by-step instructions to regain normalcy	■ Procedures for the recovery of lost data ■ Procedures for the reestablishment of lost services ■ Shutdown procedures to protect systems and data	Immediately after the incident is labeled a disaster	Short-term recovery
Business Continuity Plan (BCP)	Steps to ensure continuation of the overall business when the scale of a disaster exceeds the DRP's ability to quickly restore operations	■ Preparation steps for activation of secondary data centers ■ Establishment of a hot site in a remote location	Immediately after the disaster is determined to affect the continued operations of the organization	Long-term operation

STRATÉGIE DE CONTRÔLE DES RISQUES: ACCEPTATION

Acceptation: Identifier et reconnaître correctement les risques et choisir de ne pas les contrôler

Approprié quand:

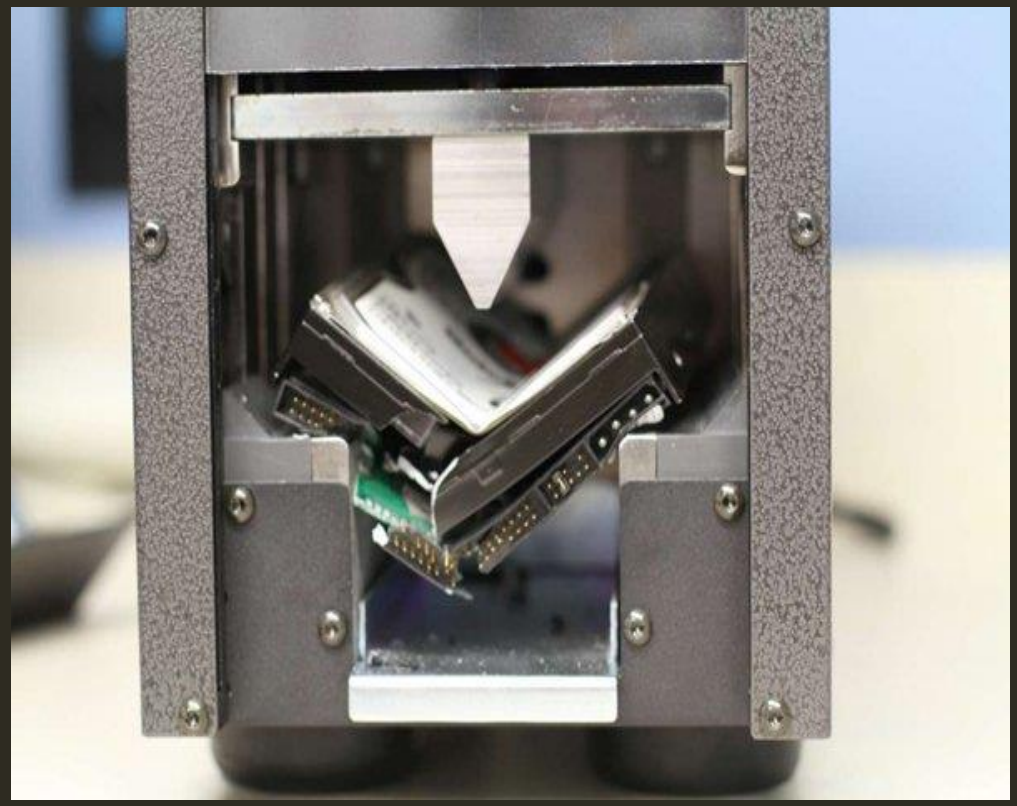
- Le coût pour protéger un ou plusieurs actifs dépasse le coût pour le remplacer / les remplacer
- Lorsque la probabilité de risque est très faible et que l'actif est prioritaire
- Sinon acceptation = négligence

STRATÉGIE DE CONTRÔLE DES RISQUES: RÉSILIATION

Résiliation: suppression ou interruption de l'actif informationnel de l'organisation

Les exemples comprennent:

- Mise a l’ écart de l'équipement
- Interrompre un service fourni
- Renvoyer un employé



AVANTAGES ET INCONVÉNIENTS DE CHAQUE STRATÉGIE

Avantages

Défense: approche globale privilégiée

Transfert: facile et efficace

Atténuation: efficace lorsque tout le reste échoue

Acceptation: pas cher et facile

Résiliation: relativement bon marché et sûr

Inconvénients

Défense: cher et laborieux

Transfert: Dépendance à l'égard d'entités externes

Atténuation: retarder la perte de l'entreprise

Acceptation: rarement approprié, dangereux

Résiliation: rarement approprié, nécessite une perte de la part de l'entreprise

APPROCHES STANDARD DE LA GESTION DES RISQUES

La norme ISO/IEC 27005 / La méthode EBIOS / La méthode MEHARI / La méthode OCTAVE

La méthode CRAMM / La méthode IASME / La méthode FAIR / La méthode IT-Grundschutz / La méthode MAGERIT / La méthode CORAS / La méthode ITIL / La méthode COBIT

Modèle de gestion des risques du NIST

Approche de gestion des risques Microsoft

L'analyse factorielle du risque d'information (FAIR) de Jack A. Jones

Technique Delphi

EBIOS (EXPRESSION DES BESOINS ET IDENTIFICATION DES OBJECTIFS DE SÉCURITÉ)

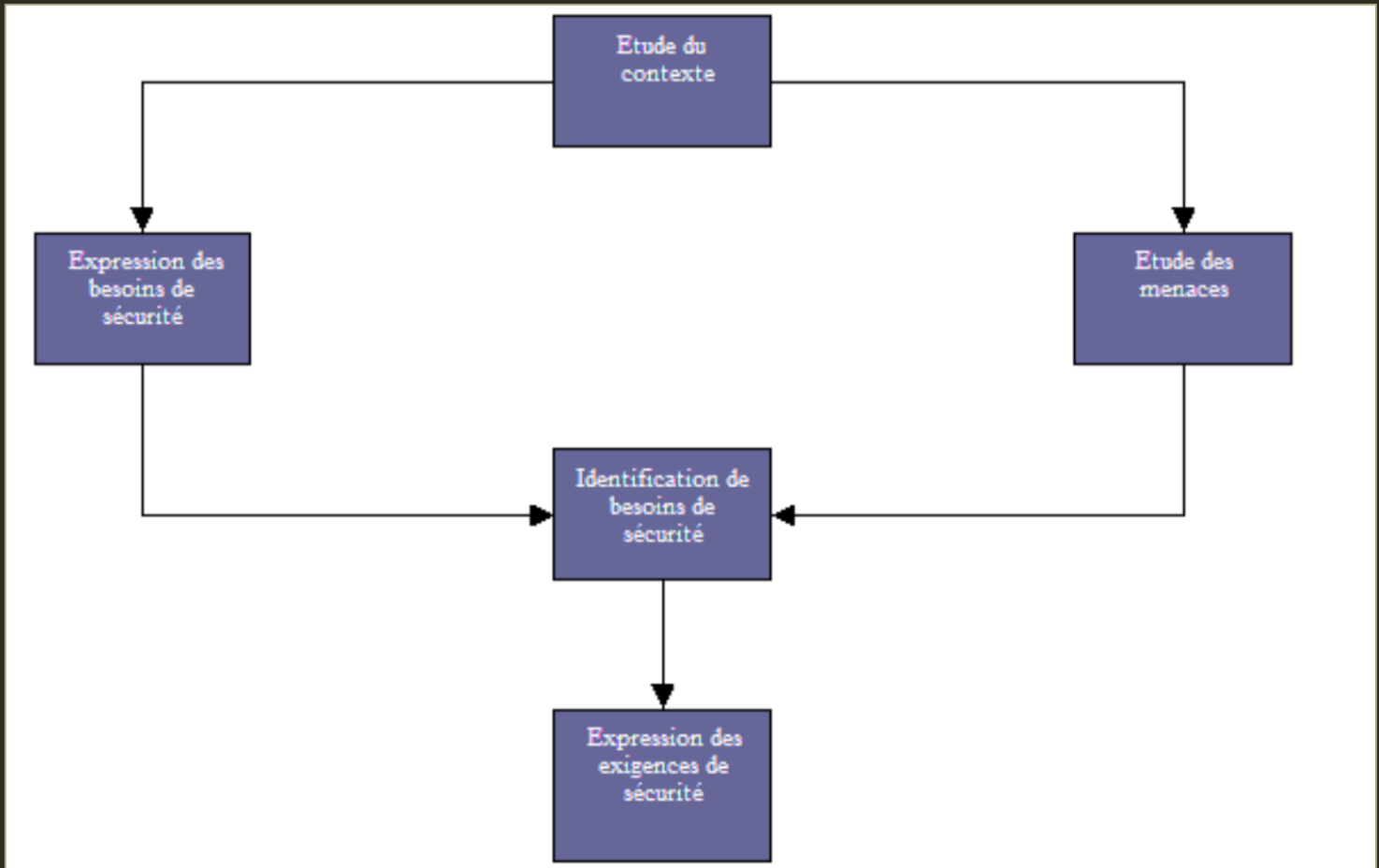


Figure 4 : Démarche EBIOS globale

OCTAVE (OPERATIONALLY CRITICAL THREAT, ASSET, AND VULNERABILITY EVALUATION)

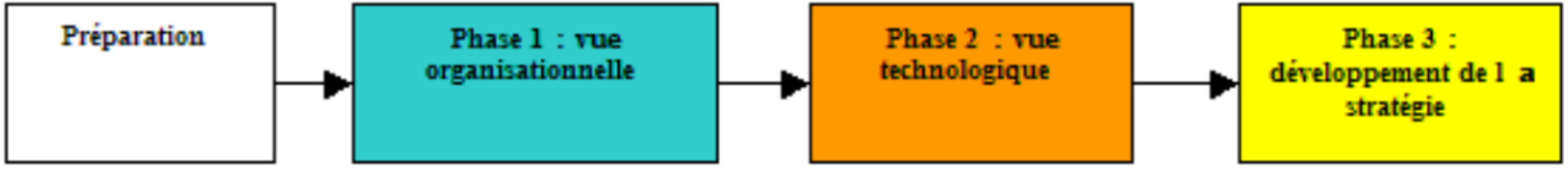
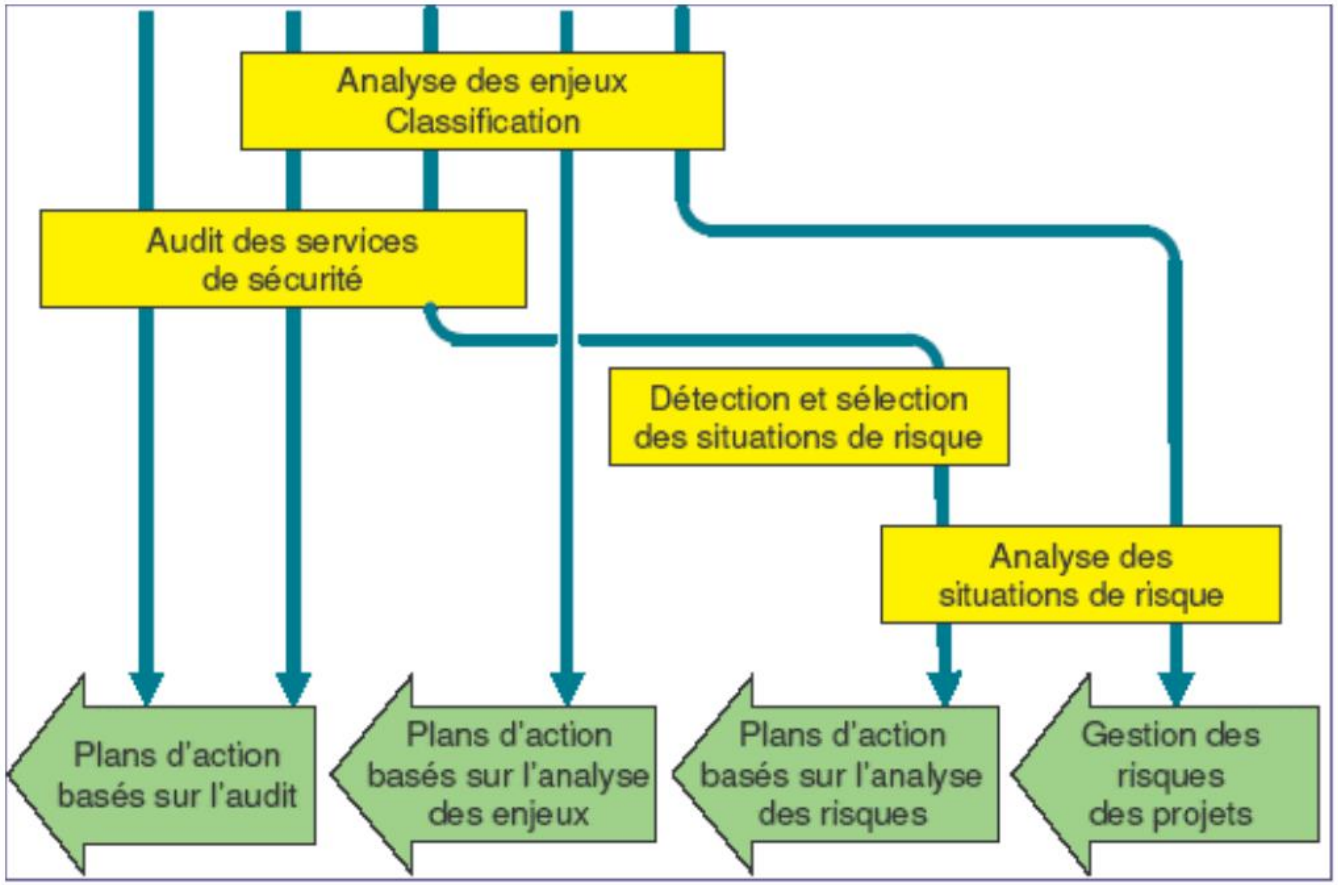


Figure 5 : Les phases principales d'OCTAVE

MEHARI (MÉTHODE HARMONISÉE D'ANALYSE DE RISQUES)



Source CLUSIF

Figure 6 : Démarche MEHARI globale

COMPARATIF DES TROIS METHODES

Méthodes	EBIOS	MEHARI	OCTAVE
Langue	Français	Français, anglais, allemand,…	Anglais
Pays	France en 1995	France en 1995	USA en 1999
Conformité	ISO 31000, 27001, 27005	ISO 27001, 27002, 27005	ISO 31010
Documentation	Riche et disponible	Riche et disponible	Catalogue de pratiques de sécurité
outils	Logiciel EBIOS 2010, gratuit et téléchargeable	Base de connaissances, Excel et Open Office. Un manuel de référence	Logiciel payant
Fonctionnalités principale	• Analyse des risques • Maturité SSI	• Analyse des risques • Tableau de bord • Indicateurs • Maturité SSI	• Analyse des risques

LOGICIEL DE GESTION DES RISQUES

Logiciel Risk Management BarnOwl

https://www.youtube.com/watch?v=lUZy7je-nMY

EBIOS 2010

https://adullact.net/projects/ebios2010/

SOURCES

M. Whitman, H. Mattford. , *Management of information security*, Fourth Edition, Stamford, CT: Cengage Learning, 2014, p. 279-313.

www.youtube.com

La gestion des risques pour les systèmes d'information, Nicolas Mayer et Jean-Philippe Humbert

RISQUES INFORMATIQUES : Maîtriser ou périr / http://www.clusib.be/

Gestion des risques liés à la cybersécurité / Guide pratique pour les entreprises / McCarthy Tétrault LLP / mccarthy.ca

https://www.business.qld.gov.au/starting-business/protect-business/managing-risk/analysing

https://www.nacs.tn/fr/documents/comparatif_methodes_Audit_AR.pdf