Chapitre 2

La Gestion des Risques

Concepts et Méthodes

30 octobre 2025

ECUE : Sécurité des Systèmes d'Information

« Les risques désignent un futur qu'il s'agit d'empêcher d'avenir »

Table des matières

1 Introduction **2**

2 Définition et Finalités **2**

2.1 Définition 2

2.2 Finalités 2

3 Fondements de la Gestion des Risques **3**

3.1 Les Assets (Actifs) 3

3.2 Les Risques 4

3.3 Exigences de Sécurité 4

4 Le Processus de Gestion des Risques **6**

4.1 Identification des Risques 7

4.2 Estimation des Risques 7

4.3 Stratégies de Traitement des Risques 8

5 Les Méthodes de Gestion des Risques **8**

5.1 EBIOS 9

5.2 MARION 9

5.3 MEHARI 11

6 Comparaison des Méthodes **12**

7 Résumé et Points Clés **13**

1 Introduction

Historique du Risk Management

Origine : Années 1950 aux États-Unis
Domaine initial : Finance
Extension :

- Environnement
- Gestion de projet
- Sécurité informatique

Le concept de gestion des risques s'est progressivement étendu à d'autres domaines critiques.

2 Définition et Finalités

2.1 Définition

Gestion des Risques selon l'ISO

La gestion des risques est définie par l'ISO comme **l'ensemble des activités coordonnées** visant à :

- **Diriger** un organisme vis-à-vis du risque
- **Piloter** un organisme vis-à-vis du risque

C'est une approche systématique et structurée pour identifier, évaluer et traiter les risques.

2.2 Finalités

3 Objectifs Principaux

1. **Améliorer la sécurisation des systèmes d'information**
   - Identifier les failles
   - Mettre en place des contre-mesures appropriées
   - Réduire la surface d'attaque
2. **Justifier le budget alloué à la sécurisation du SI**
   - Démontrer la nécessité des investissements
   - Prioriser les dépenses en fonction des risques
   - ROI (Return On Investment) de la sécurité
3. **Prouver la crédibilité du système d'information**
   - Analyses effectuées
   - Conformité aux normes
   - Confiance des parties prenantes

3 Fondements de la Gestion des Risques

3 Blocs Interdépendants

La gestion des risques se compose de trois blocs interdépendants :

1. L'Organisation

- Ses assets (actifs)
- Ses objectifs de sécurité
- Son contexte métier

2. Les Risques

- Pesant sur ces assets
- Menaces et vulnérabilités
- Impacts potentiels

3. Les Mesures

- Prises pour traiter les risques
- Assurer un certain niveau de sécurité
- Contrôles et contre-mesures

3.1 Les Assets (Actifs)

Types d'Assets

Définition : Biens, actifs, ressources ayant de la valeur pour l'organisme et nécessaires à son bon fonctionnement.

Asset Business (Actifs Métier)

- Principalement des **informations**
- Exemples : numéros de carte bancaire, données clients, brevets
- **Processus métier**
- Exemples : gestion des transactions, administration des comptes

Asset System (Actifs Système)

- Éléments **techniques**
- Matériels (serveurs, ordinateurs, routeurs)
- Logiciels (applications, OS, bases de données)
- Réseaux (LAN, WAN, WiFi)
- **Environnement du SI**
- Utilisateurs
- Bâtiments
- Locaux techniques

3.2 Les Risques

Équation du Risque

On définit un risque à l'aide de **l'équation du risque** :

$$\boxed{\text{RISQUE} = \text{MENACE} \times \text{VULNÉRABILITÉ} \times \text{IMPACT}}$$

Composantes :

1. La Menace

- Source du risque
- Attaque possible d'un élément dangereux pour les assets
- Agent responsable du risque
- Exemples : pirate, malware, catastrophe naturelle, erreur humaine

2. La Vulnérabilité

- Caractéristique d'un asset constituant une faiblesse
- Faille au regard de la sécurité
- Exemples : faille logicielle, configuration faible, absence de patch

3. L'Impact

- Conséquence du risque sur l'organisme et ses objectifs
- Peut être financier, réputationnel, opérationnel
- Gravité des dommages

3.3 Exigences de Sécurité

Traitement des Risques

Pour faire face aux risques :
Politique de traitement de risques constituée d'exigences de sécurité permettant de répondre aux risques.
Ces exigences de sécurité entraînent la mise en place de **contrôles (ou contre-mesures)** de sécurité à implémenter.

Types de Contrôles :

1. Sur la menace ou la vulnérabilité

- Limiter la cause du risque
- Prévention
- Exemples : firewall, antivirus, formation

2. Sur l'impact

- Limiter la conséquence du risque
- Mitigation
- Exemples : sauvegardes, plan de continuité, assurance

Facteurs Influençant les Mesures

Les mesures de sécurité à mettre en place dépendent de :

- L'**activité** de l'organisation
- L'**organisation** elle-même
- La **réglementation** applicable
- Les **contraintes de l'écosystème** de l'entreprise

4 Le Processus de Gestion des Risques

6 Étapes Principales

Ce processus est presque toujours appliqué dans les méthodes pratiques de gestion des risques :

Étape 1 : Connaissance du Contexte

- Prendre connaissance de l'organisation et son environnement
- Comprendre le SI
- Déterminer les limites du système sur lequel va porter l'étude
- Identifier les assets business constituant la valeur
- Faire le lien avec les assets système

Étape 2 : Détermination des Objectifs de Sécurité

- Spécifier les besoins en termes de :
  - Confidentialité
  - Intégrité
  - Disponibilité
- Pour chaque asset identifié

Étape 3 : Analyse des Risques (*cœur de la démarche*)

- Identification et estimation de chaque composante :
  - Menace
  - Vulnérabilité
  - Impact
- Évaluation du risque
- Appréciation de son niveau
- Prise de mesures adéquates

Étape 4 : Définition des Exigences de Sécurité

- Souvent effectuée de manière incrémentale
- Raffinement successif
- Réduire les risques identifiés
- Utilisation de référentiels ou experts

Étape 5 : Sélection des Contrôles

- Instanciation des exigences de bas niveau
- Pour le système cible étudié
- Choix techniques des solutions de sécurité
- Influencés par :
  - Système déjà en place
  - Compétences disponibles
  - Coûts de mise en œuvre

Étape 6 : Implémentation

- Implémentation des contrôles
- Tests
- Évaluation

4.1 Identification des Risques

2 Grandes Écoles

1. **Approche par Audit**
   - Réaliser un audit du système
   - Étudier ses différents acteurs
   - Analyse terrain
   - Interviews et observations
2. **Approche par Bases de Connaissances**
   - Se baser sur des catalogues de risques
   - Utiliser des référentiels existants
   - Bases de données de vulnérabilités
   - Retours d'expérience

4.2 Estimation des Risques

Quantification des Risques

En théorie, il est possible de quantifier les risques à l'aide de :

- **Distributions de probabilités** sur les menaces et vulnérabilités
- **Estimation des coûts** occasionnés par les impacts

En pratique, on utilise souvent des échelles qualitatives (faible, moyen, élevé).

4.3 Stratégies de Traitement des Risques

Matrice Occurrence × Impact

Risques Négligeables (Occurrence faible + Impact faible)
- Acceptation du risque
- Pas de mesure spécifique

Risques Inacceptables (Occurrence forte + Impact important)
- **Évitement du risque** (Avoidance)
- Ne doivent pas exister
- Remise en cause des activités nécessaire

Risques Acceptés (Occurrence forte + Impact faible)
- **Acceptation du risque**
- Coût inclus dans les coûts opérationnels

Risques à Transférer (Occurrence faible + Impact lourd)
- **Transfert du risque**
- Couverts par assurance ou tiers
- Externalisation de la responsabilité

Risques à Traiter (Cas intermédiaires - majoritaires)
- **Mitigation du risque**
- Traités au cas par cas
- Centre du processus de gestion des risques
- Objectif : diminuer les risques à l'aide de contrôles
- Rapprocher au maximum de l'origine de l'axe

5 Les Méthodes de Gestion des Risques

Vue d'Ensemble

Plus de 200 méthodes déclinées à travers le monde
Les plus connues :
- **EBIOS** (France)
- **MEHARI** (France)
- **MARION** (France)
- **OCTAVE** (USA)

5.1 EBIOS

EBIOS - Expression des Besoins et Identification des Objectifs de Sécurité

Origine :

- Développée par la DCSSI (Direction Centrale de la Sécurité des Systèmes d'Information)
- Année : 1995
- Statut : Gratuite

Composition :

- 5 guides :
  1. Introduction
  2. Démarche
  3. Techniques
  4. Outillages pour l'appréciation des risques
  5. Outillages pour le traitement des risques
- Logiciel support

Démarche :

1. Prise en compte du contexte

- Organisation cible
- Périmètre du SI privilégié
- Éléments essentiels
- Fonctions et informations (assets business)
- Entités (assets système)

2. Détermination des besoins

- Grille des services souhaités de sécurité
- Respect des critères CID :
  - Confidentialité
  - Intégrité
  - Disponibilité

3. Analyse des menaces et vulnérabilités

- Prise en compte relative des vulnérabilités
- Menaces s'appliquant sur les assets
- Identification des éléments critiques

4. Définition des exigences

- Exigences de haut-niveau (appelées « objectifs »)
- Exigences de bas-niveau (appelées « exigences »)

5. Sélection des contre-mesures

- Bonnes contre-mesures strictement adaptées
- Aux besoins de l'organisation

5.2 MARION

MARION - Méthodologie d'Analyse et de Réduction des risques Informatiques Optimisés par Niveau

Origine :

— Développée par le CLUSIF
— (Club de la Sécurité de l'Information Français)

Principe :

— Repose sur des questionnaires
— Relatifs à 6 domaines
— 27 indicateurs répartis selon les 6 domaines
— Résultat : Rosace de sécurité

6 Domaines :

1. Sécurité organisationnelle

— Politique de sécurité
— Organisation de la sécurité
— Gestion des ressources humaines

2. Sécurité physique

— Contrôle d'accès physique
— Protection des locaux
— Sécurité environnementale

3. Continuité

— Plan de continuité d'activité
— Plan de reprise d'activité
— Sauvegardes

4. Organisation informatique

— Structure de l'équipe IT
— Procédures et documentation
— Gestion des projets

5. Sécurité logique et exploitation

— Contrôles d'accès logiques
— Gestion des comptes
— Supervision et logs

6. Sécurité des applications

— Développement sécurisé
— Tests de sécurité
— Gestion des vulnérabilités

Déroulement :

Phase 0 : Préparation

— Définition des objectifs de sécurité
— Définition du champ d'action

Phase 1 : Audit des vulnérabilités

— Questionnaires sur les 6 domaines
— Résultat : Rosace de sécurité
— Visualisation graphique du niveau de sécurité

Phase 2 : Analyse des risques

— Répartir les risques en :
  — Risques Majeurs (RM)
  — Risques Simples (RS)

Phase 3 : Élaboration du plan d'action

- Décision du degré d'amélioration à apporter
- Objectif idéal : note globale de 3 (sécurité correcte)
- Échelle : 0 (insécurité) à 4 (excellent)
- Définition des moyens nécessaires

5.3 MEHARI

MEHARI - Méthode Harmonisée d'Analyse de RIsques **Origine :**

- Une des méthodes les plus utilisées
- Développée par le CLUSIF
- Outil : RISICARE (développé par BUC SA)

Phase 1 : Préparatoire

Étudier le contexte

- Périmètre de l'étude
- Identifier les événements pouvant impacter le fonctionnement du SI

Recenser et classifier

- Ensemble des actifs du SI
- Classification par importance

Fixer les objectifs de sécurité

- Niveau de sécurité requis pour chaque actif :
  - Confidentialité
  - Intégrité
  - Disponibilité

Phase 2 : Analyse du Risque

Identifier les situations

- Susceptibles de remettre en cause les objectifs de sécurité

Élaborer des scénarios de risque

- Scénarios d'attaque
- Chemins possibles d'exploitation

Diagnostic des services de sécurité

- Évaluation des mesures existantes

Évaluation des risques

- Probabilité d'occurrence
- Impact potentiel

Expression des besoins

- Besoins de sécurité
- Mesures nécessaires au traitement du risque

Phase 3 : Planification du Traitement

Analyser les scénarios de risque identifiés pour décider du traitement :

1. Accepter le risque tel quel

- Risque faible ou acceptable
- Coût de traitement supérieur à l'impact

2. Réduire le risque

- Prendre des mesures pour réduire l'impact
- Ou réduire la potentialité du risque
- Mise en place de contrôles

3. Éviter le risque

- Supprimer l'origine du risque
- Mesures structurelles ou organisationnelles
- Changement de processus

4. Transférer le risque

- Assurance
- Externalisation
- Partage de responsabilité

6 Comparaison des Méthodes

Critère	**EBIOS**	**MARION**	**MEHARI**
Origine	DCSSI (France)	CLUSIF (France)	CLUSIF (France)
Approche	Complète et détaillée	Questionnaires	Scénarios de risque
Outils	Logiciel gratuit	Rosace de sécurité	RISICARE
Complexité	Élevée	Moyenne	Élevée
Public cible	Experts sécurité	PME/PMI	Grandes organisations
Points forts	Très complète, reconnue	Simple, visuelle	Scénarios détaillés

7 Résumé et Points Clés

À Retenir

Équation du Risque

$$\boxed{\text{RISQUE} = \text{MENACE} \times \text{VULNÉRABILITÉ} \times \text{IMPACT}}$$

3 Blocs de la Gestion des Risques

1. Organisation (assets, objectifs)
2. Risques (menaces, vulnérabilités, impacts)
3. Mesures (contrôles, contre-mesures)

6 Étapes du Processus

1. Connaissance du contexte
2. Détermination des objectifs de sécurité
3. Analyse des risques (cœur)
4. Définition des exigences
5. Sélection des contrôles
6. Implémentation et évaluation

4 Stratégies de Traitement

1. Accepter le risque
2. Réduire le risque (mitigation)
3. Éviter le risque (avoidance)
4. Transférer le risque (assurance)

Méthodes Principales

— **EBIOS :** Complète, gratuite, française
— **MARION :** Questionnaires, rosace, 6 domaines
— **MEHARI :** Scénarios, RISICARE, 3 phases

La gestion des risques est un processus continu !

« Les risques désignent un futur qu'il s'agit d'empêcher d'avenir »

Ressource :

— MEHARI : `http://infoqualite.accordance.fr/dossiers/dossiers.php?id_dossier=176`