# Registre des Risques (COSO / ISO 31000)

Entreprise : OptiValue.ai  
Version : 1.0  
Date : 03/09/2025  
Auteur : Département Risques & Gouvernance

## Introduction

Le registre des risques d’OptiValue.ai centralise et structure l’ensemble des risques identifiés à l’échelle globale. Il est conçu pour répondre aux standards les plus exigeants (ISO 31000, COSO ERM) et intègre des outils d’évaluation et de reporting en temps réel. Ce registre est mis à jour de manière continue grâce à un moteur IA qui surveille l’environnement réglementaire, technologique et géopolitique.

## 1. Méthodologie de Gestion des Risques

Chaque risque est évalué selon les étapes suivantes :  
1. Identification  
2. Analyse  
3. Évaluation  
4. Traitement  
5. Suivi et amélioration continue  
  
Les risques sont scorés sur une échelle de 1 à 5 pour l’impact et la probabilité, avec une matrice 5x5 de criticité pour prioriser les actions.

## 2. Tableau des Risques

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| ID | Processus | Risque | Causes | Conséquences | Contrôles existants | Impact | Prob. | Risque résiduel | Traitement | Propriétaire | Échéance |
| RSK-001 | Infrastructure Cloud | Fuite de données critiques | Mauvaise configuration S3 | Sanctions RGPD, perte réputation | MFA, chiffrement AES-256, segmentation réseau | 5 | 2 | 2 | Audit mensuel + test red team | RSSI | 2025-12-31 |
| RSK-002 | Développement IA | Biais dans les algorithmes | Dataset non équilibré | Atteinte à l’équité, image dégradée | Audits algorithmiques trimestriels, comités éthiques | 4 | 3 | 2 | Retraining trimestriel + IA Explainable | Responsable IA | 2025-09-30 |
| RSK-003 | Chaîne fournisseurs | Défaillance fournisseur critique | Dépendance unique | Rupture service, pertes financières | Clauses SLA, plan BCP fournisseurs | 4 | 2 | 1 | Diversification fournisseurs | Directeur Achats | 2025-06-30 |
| RSK-004 | Conformité RGPD | Violation de données personnelles | Erreur humaine, absence revue | Amende CNIL, litige client | Procédures strictes, DLP, formation annuelle | 5 | 1 | 1 | Contrôles renforcés, revue hebdo DPO | DPO | 2025-05-31 |
| RSK-005 | Sécurité physique | Intrusion dans datacenter | Manque surveillance | Perte de disponibilité, fuite data | Contrôles physiques biométriques, caméras, gardiennage | 4 | 1 | 1 | Audit annuel + tests intrusions | CISO | 2025-11-30 |
| RSK-006 | ESG | Non-conformité reporting CSRD | Données non fiabilisées | Sanctions, perte investisseurs | Process qualité données, audit externe | 3 | 2 | 1 | Mise à jour data quality tools | Directeur ESG | 2025-10-15 |
| RSK-007 | Cyber | Ransomware ciblé | Phishing, patch retardé | Blocage services, perte financière | EDR, SOC 24/7, patch management | 5 | 3 | 2 | Simulations trimestrielles + backups isolés | RSSI | 2025-08-30 |
| RSK-008 | Innovation | IA non conforme AI Act | Absence classification précise | Sanctions, perte marchés publics | Registre IA, audit conformité mensuel | 4 | 2 | 1 | Mise à jour processus et formations IA | Responsable IA | 2025-07-31 |

## 3. Reporting et Suivi

Le suivi des risques se fait via des dashboards interactifs alimentés en temps réel. Les indicateurs clés incluent :  
• Nombre d’incidents par catégorie  
• Niveau de risque résiduel par domaine  
• Respect des échéances des plans d’action  
• Score global de maturité des contrôles

## 4. Automatisation et Intelligence

Le registre est interconnecté avec la plateforme interne RiskHub.ai, intégrant :  
• Détection automatique des signaux faibles via machine learning.  
• Intégration avec les SIEM, GRC et ERP.  
• Génération d’alertes prédictives pour anticiper les défaillances potentielles.

## Annexes

• Modèle de scoring 5x5  
• Exemple de dashboard dynamique  
• Processus d’escalade en cas d’incident critique  
• RACI détaillé par typologie de risque  
• Historique des mises à jour et versions