# Politique Gestion des Risques (POL-02)

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

## Introduction

La Politique de Gestion des Risques d’OptiValue.ai définit le cadre, les principes, et les responsabilités pour identifier, évaluer, traiter et surveiller les risques. S’appuyant sur les standards internationaux (ISO 31000, COSO ERM, DORA, NIS2, AI Act), cette politique garantit une résilience optimale et une prise de décision éclairée dans toutes nos activités.

## 1. Cadre et Objectifs

• Protéger les actifs, les données et la réputation de l’entreprise.  
• Intégrer une culture du risque à tous les niveaux hiérarchiques.  
• Anticiper les menaces émergentes, notamment cyber, réglementaires, IA et ESG.  
• Optimiser la continuité des activités et la performance globale.

## 2. Gouvernance des Risques

La gouvernance repose sur un Comité des Risques présidé par le Chief Risk Officer (CRO), rapportant directement au CEO et au Conseil d’administration.  
  
\*\*Rôles et responsabilités :\*\*  
• \*\*CRO\*\* : Supervision de la stratégie et validation des plans de traitement.  
• \*\*RSSI\*\* : Identification et traitement des risques cyber.  
• \*\*DPO\*\* : Gestion des risques liés aux données et conformité RGPD.  
• \*\*Responsable IA\*\* : Supervision des risques algorithmiques (AI Act).  
• \*\*Directeurs de BU\*\* : Identification des risques métiers spécifiques.  
• \*\*Audit Interne\*\* : Vérification et évaluation indépendante des dispositifs.

## 3. Processus de Gestion des Risques

Le processus suit la méthodologie ISO 31000 et inclut :  
1. \*\*Identification\*\* : Cartographie initiale des risques internes et externes.  
2. \*\*Analyse\*\* : Évaluation de l’impact et de la probabilité sur une échelle de 1 à 5.  
3. \*\*Évaluation\*\* : Classification selon l’appétence au risque définie par le Comité.  
4. \*\*Traitement\*\* : Définition et déploiement des mesures de mitigation.  
5. \*\*Suivi et contrôle\*\* : Reporting trimestriel et revue annuelle.  
6. \*\*Amélioration continue\*\* : Ajustements basés sur les leçons apprises et benchmarks.

## 4. Typologie des Risques

• \*\*Risques Stratégiques\*\* : Transformation marché, réputation, innovations IA.  
• \*\*Risques Opérationnels\*\* : Processus internes, erreurs humaines, qualité des données.  
• \*\*Risques Technologiques\*\* : Vulnérabilités systèmes, IA non maîtrisée, incidents cloud.  
• \*\*Risques de Conformité\*\* : RGPD, AI Act, NIS2, DORA, CSRD.  
• \*\*Risques Financiers\*\* : Change, liquidité, crédits.  
• \*\*Risques ESG\*\* : Social, environnement, gouvernance.  
• \*\*Risques liés aux tiers\*\* : Dépendance fournisseurs critiques et sous-traitants.

## 5. Méthodologie d’Évaluation des Risques

Chaque risque est évalué selon :  
• \*\*Impact\*\* : Financier, opérationnel, réputationnel, réglementaire.  
• \*\*Probabilité\*\* : Historique, tendances, intelligence prédictive.  
• \*\*Criticité Résiduelle\*\* : Score combiné post-contrôles.  
  
Une matrice 5x5 est utilisée pour visualiser et prioriser les risques.

## 6. Plan de Traitement et Suivi

Chaque risque critique dispose d’un plan d’action :  
• Mesures préventives (politiques, formations, outils techniques).  
• Mesures correctives (plans de remédiation, actions d’urgence).  
• Indicateurs de performance pour suivre l’efficacité.  
• Révisions trimestrielles et mises à jour en temps réel dans le registre centralisé.

## 7. Indicateurs de Suivi

• \*\*KRIs\*\* : Taux d’incidents cyber, vulnérabilités critiques, non-conformités détectées.  
• \*\*KPIs\*\* : % de plans de traitement réalisés, temps de réponse moyen aux incidents, taux de couverture des formations.  
Ces indicateurs sont présentés sous forme de tableaux de bord interactifs pour le comité exécutif.

## 8. Communication et Formation

La gestion des risques est intégrée dans les parcours de formation et de communication interne :  
• Modules e-learning obligatoires pour tous.  
• Ateliers spécifiques pour managers et équipes techniques.  
• Simulations annuelles d’incidents majeurs.

## 9. Amélioration Continue

La politique est révisée chaque année et mise à jour en fonction :  
• Des évolutions réglementaires et technologiques.  
• Des recommandations issues des audits internes et externes.  
• Des benchmarks sectoriels et analyses de marché.

## Annexes

• Modèle de matrice des risques.  
• Procédures types de traitement.  
• Exemple de rapport trimestriel.  
• Organigramme de gouvernance des risques.  
• Exemples de dashboards dynamiques.