# Cartographie des Risques Tiers

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

## Introduction

Cette cartographie des risques tiers fournit une vue consolidée des risques associés aux fournisseurs et partenaires d’OptiValue.ai. Elle prend en compte les risques \*\*cyber\*\*, \*\*conformité réglementaire\*\*, \*\*durabilité (ESG)\*\*, \*\*réputation\*\*, et \*\*continuité opérationnelle\*\*. Elle permet de piloter efficacement la gestion des risques et de prioriser les actions de remédiation.

## 1. Gouvernance

• Supervision par le Chief Compliance Officer (CCO) et le Comité des Risques.  
• Mise à jour trimestrielle via ComplianceHub.ai.  
• Audits externes annuels pour vérification et certification de la méthodologie.

## 2. Synthèse des Risques par Fournisseur

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| ID Fournisseur | Nom | Cyber | Conformité | Durabilité | Réputation | Continuité |
| F-001 | GreenSupply Asia | Moyen | Élevé | Moyen | Moyen | Élevé |
| F-002 | DataCloud Europe | Faible | Moyen | Faible | Faible | Faible |
| F-003 | AICompute Labs | Élevé | Moyen | Élevé | Moyen | Élevé |
| F-004 | EcoPackaging Ltd | Faible | Faible | Faible | Faible | Faible |
| F-005 | TechLegal Advisors | Faible | Faible | Moyen | Faible | Moyen |

## 3. Matrice Criticité / Risque Résiduel

La matrice suivante illustre la position de chaque fournisseur selon deux axes : criticité et niveau de risque résiduel.  
  
\*\*Échelle de criticité\*\* : Faible, Moyenne, Élevée  
\*\*Échelle de risque résiduel\*\* : Faible, Moyen, Élevé

• \*\*Zone 1 (Vert)\*\* : Faible criticité / Faible risque — surveillance standard.  
• \*\*Zone 2 (Jaune)\*\* : Moyenne criticité / Moyen risque — suivi renforcé.  
• \*\*Zone 3 (Orange)\*\* : Criticité élevée / Risque moyen — audits réguliers et remédiations planifiées.  
• \*\*Zone 4 (Rouge)\*\* : Criticité élevée / Risque élevé — priorité absolue avec plan de mitigation immédiat.

|  |  |  |  |
| --- | --- | --- | --- |
| Fournisseur | Criticité | Risque Résiduel | Plan de Suivi |
| GreenSupply Asia | Élevée | Élevé | Audit trimestriel, plan de remédiation et suivi mensuel. |
| DataCloud Europe | Moyenne | Faible | Surveillance standard avec audit annuel. |
| AICompute Labs | Élevée | Élevé | Suivi quotidien, audit de cybersécurité renforcé. |
| EcoPackaging Ltd | Faible | Faible | Surveillance légère, audit biennal. |
| TechLegal Advisors | Moyenne | Moyen | Audit annuel et suivi contractuel renforcé. |

## 4. Suivi et Automatisation

• Tableaux de bord dynamiques sur ComplianceHub.ai pour visualiser les évolutions.  
• IA prédictive pour identifier les signaux faibles (cyber, ESG, réputation).  
• Alertes automatiques envoyées aux responsables métiers en cas de dérive.  
• Documentation des actions de remédiation et des résultats d’audit en temps réel.

## 5. Amélioration Continue

• Revue annuelle de la méthodologie de scoring des risques.  
• Mise à jour des critères selon les évolutions réglementaires et sectorielles.  
• Sessions de formation pour les équipes Achats, IT et Conformité.

## 6. Annexes

• Modèle de grille de scoring détaillée.  
• Historique des incidents critiques par fournisseur.  
• Benchmarks sectoriels et recommandations de l’OCDE.  
• Checklists pour audits sur site et audits documentaires.