# Preuves des Contrôles

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

## Introduction

Ce document présente l’ensemble des preuves de contrôles mises en œuvre par OptiValue.ai dans le cadre de son système intégré de conformité, de gouvernance et de gestion des risques. Ces preuves attestent de la robustesse et de la maturité des dispositifs, conformes aux standards ISO 37301, ISO 31000, ISO 27001 et aux exigences réglementaires telles que RGPD, AI Act, DORA, et NIS2.

## 1. Preuves de Formation

• Attestations de formation annuelle pour 100% des collaborateurs.  
• Modules spécialisés pour les équipes techniques, juridiques, et produits.  
• Rapports consolidés de suivi avec taux de complétion : \*\*98%\*\*.  
• Sessions interactives trimestrielles sur les thématiques émergentes : sécurité IA, éthique algorithmique, RGPD avancé.

## 2. Attestations d’Audit

• Rapports d’audit interne trimestriels (ISO 27001, ISO 31000).  
• Certifications délivrées par des tiers indépendants (PwC, Deloitte, EY).  
• Scores supérieurs à 95% sur tous les contrôles critiques.  
• Traçabilité des actions correctives et suivi dans l’outil GRC interne.

## 3. Campagnes de Sensibilisation

• Newsletters mensuelles sur les bonnes pratiques de cybersécurité et conformité.  
• Ateliers live interactifs pour sensibiliser aux risques IA.  
• Tableaux de bord de participation avec des KPIs en temps réel.  
• Documentation des supports de formation et retours des participants.

## 4. Revue des Obligations

• Comptes rendus des comités mensuels de conformité.  
• Mise à jour automatique du registre des obligations avec horodatage.  
• Validation systématique des changements par le Comité Conformité.  
• Traçabilité des ajustements dans le registre centralisé (REG-01).

## 5. Contrôles Techniques et Organisationnels

• Captures d’écran des configurations critiques : MFA, segmentation réseau, chiffrement AES-256.  
• Logs d’audit des systèmes SIEM et des plateformes cloud.  
• Rapports de tests de pénétration internes et externes.  
• Relevés de surveillance SOC 24/7 et interventions documentées.

## 6. Indicateurs et Tableaux de Bord

• Tableaux de bord mensuels consolidés (KPI/KRI).  
• Heatmaps de risques actualisées trimestriellement.  
• Reporting automatique vers le Comité Exécutif et le Conseil d’Administration.  
• Historique des tendances et analyses prédictives issues de la plateforme ComplianceHub.ai.

## 7. Exemple de Traçabilité d’Incident

• Journal des événements horodatés.  
• Analyse de cause racine (RCA) détaillée.  
• Plan de remédiation validé par les responsables de domaines.  
• Rapport de clôture et suivi des actions avec preuves documentées.

## 8. Automatisation et Veille

• Intégration d’IA pour surveiller en continu les écarts de conformité.  
• Alertes automatisées en cas de déviation de contrôle.  
• Rapports de veille réglementaire consolidés hebdomadairement.  
• Documentation des ajustements en temps réel dans les registres associés.

## Annexes

• Copies des certificats de conformité.  
• Modèles de rapports d’audit.  
• Exemples de dashboards.  
• Templates de checklists de conformité pour audit interne.  
• Historique des améliorations continues depuis 2022.