# VRIKSHA AI

Enterprise AI Governance Stack

# Compliance Readiness Checklist

A comprehensive guide for regulated industries

## 1. DATA PRIVACY & PROTECTION

[ ] Data inventory documented - catalog all AI training and inference data
[ ] Consent management in place - track user permissions for data usage
[ ] Data anonymization protocols - PII masking and de-identification
[ ] Right-to-erasure procedures - GDPR/CCPA deletion workflows
[ ] Cross-border transfer compliance - data sovereignty requirements met

## 2. AUDIT TRAIL & LOGGING

[ ] Immutable audit logs enabled - tamper-proof decision records
[ ] Decision logging configured - capture all AI model outputs
[ ] Data access logs tracked - who accessed what and when
[ ] Log retention policy defined - compliance with industry requirements
[ ] Tamper-proof storage implemented - blockchain or WORM storage

## 3. MODEL DOCUMENTATION

[ ] Model cards maintained - purpose, limitations, intended use
[ ] Training data documented - sources, preprocessing, biases
[ ] Version history tracked - all model iterations recorded
[ ] Performance metrics recorded - accuracy, fairness, drift
[ ] Bias testing documented - demographic parity, equal opportunity

## 4. EXPLAINABILITY & TRANSPARENCY

[ ] Decision explanations available - SHAP, LIME, attention maps
[ ] Feature importance documented - key decision factors
[ ] User-facing explanations designed - plain language summaries
[ ] Audit-ready reports generated - regulator-friendly documentation

## 5. ACCESS CONTROL & SECURITY

[ ] Role-based access configured - principle of least privilege
[ ] Multi-factor authentication enabled - secure user verification
[ ] API key management - rotation, scoping, monitoring
[ ] Session management - timeout, single sign-on
[ ] Privileged access monitoring - admin action logging

## 6. REGULATORY ALIGNMENT