

Risk Management Plan: AI Resume Screener

1.0 Introduction

This Risk Management Plan outlines the potential risks associated with the development, deployment, and operation of the AI Resume Screener application. The primary goal is to proactively identify, assess, and mitigate these risks to ensure the project's success, maintain system integrity, and protect the interests of all stakeholders, including the development team, end-users (HR professionals), and job applicants.

2.0 Risk Identification & Assessment

The following table catalogs the potential risks for the AI Resume Screener project. Risks are assessed based on their Likelihood (L: Low, Medium, High) and Impact (I: Low, Medium, High, Critical) on the project's success. The Severity level is derived from this assessment to prioritize mitigation efforts.

Risk ID	Category	Specific Risk	Likelihood	Impact	Severity	Description
T-1	Technical	Data Extraction Failure	Medium	High	High	Text extraction from complex formatted, scanned, or image-heavy PDFs may fail or be inaccurate, leading to incomplete data and incorrect similarity scoring.

T-2	Technical	Model Bias & Fairness	Medium	Critical	Critical	The AI model may perpetuate or amplify biases present in its training data, leading to discriminatory screening against protected attributes (gender, ethnicity, etc.).
T-3	Technical	Performance & Scalability	Medium	Medium	Medium	Processing a large batch of resumes, especially with OCR, may lead to slow response times, timeouts, and a poor user experience.
T-4	Technical	Dependency Vulnerabilities	Low	High	High	Security vulnerabilities in open-source libraries (e.g., FastAPI, PyMuPDF) could expose the system to security breaches.
DL-1	Data & Legal	Data Privacy & Security Breach	Medium	Critical	Critical	Resumes contain sensitive Personal Identifiable Information (PII). A breach from insecure storage or transmission could lead to significant

						legal and reputational damage.
DL-2	Data & Legal	Lack of Explainability (Black Box)	High	High	High	Providing only a match score without justification makes it difficult for HR to trust the results or defend against legal challenges regarding hiring decisions.
DL-3	Data & Legal	Non-Compliance with Regulations	Medium	Critical	Critical	The system may violate data protection laws (e.g., GDPR, CCPA) concerning user consent, data processing purposes, storage duration, and a candidate's "right to explanation."
F-1	Functional	Semantic Matching Inaccuracy	High	High	High	The model may misunderstand context, leading to false positives (matching irrelevant jargon) or false negatives (missing qualified candidates who use different terminology).

F-2	Functional	Over-reliance on Automation	High	Medium	High	Users may abdicate human judgment and blindly trust the AI's ranking, potentially leading to the rejection of excellent candidates and homogenization of the workforce.
P-1	Project	Scope Creep	High	Medium	High	Uncontrolled addition of new features from the future roadmap without proper planning can delay the core product's release and increase development costs.

3.0 Risk Mitigation Strategies

For each identified risk, a corresponding mitigation strategy is proposed.

- T-1: Data Extraction Failure
 - Mitigation: Implement a robust pre-processing pipeline with fallback mechanisms. Use Tesseract OCR with multiple image pre-processing techniques (e.g., deskewing, noise removal). Log all extraction failures and provide clear error messages to the user (e.g., "Could not read file X, please upload a text-based PDF").
- T-2: Model Bias & Fairness
 - Mitigation: Conduct bias audits on the model using standardized datasets. In the future roadmap, plan to integrate de-biasing techniques or use models specifically fine-tuned for fair HR tasks. Document clearly that the tool is an aid, not a decision-maker, and that human oversight is mandatory.

- T-3: Performance & Scalability
 - Mitigation: Implement asynchronous processing for large batches to prevent UI blocking. Use a task queue (e.g., Celery with Redis). Set file size and batch limits in the UI. Cache model embeddings for the same JD to avoid recomputation.
- T-4: Dependency Vulnerabilities
 - Mitigation: Use tools like `safety` or `dependabot` to continuously scan for and update vulnerable dependencies. Establish a regular schedule for updating project libraries.
- DL-1: Data Privacy & Security Breach
 - Mitigation: Do not store resumes or JD data permanently. Process files in memory or temporary storage and delete them immediately after processing. Use HTTPS for all data in transit. If storage is necessary for a short period, encrypt the data at rest.
- DL-2: Lack of Explainability
 - Mitigation: This is a critical short-term limitation. The top priority from the Future Roadmap should be the "Skill Gap Analyzer" to highlight matched and missing skills. This provides the necessary transparency for HR to understand and justify the scores.
- DL-3: Compliance with Regulations
 - Mitigation: Create a clear Privacy Policy that states what data is collected, how it is used (processing for screening), and that it is not stored. Provide a mechanism for users and candidates to request data deletion. Seek legal counsel to ensure compliance before commercial deployment.
- F-1: Semantic Matching Inaccuracy
 - Mitigation: Continuously validate the model's performance with a test suite of resumes and JDs. Allow users to provide feedback on the ranking (e.g., "This result was helpful/not helpful"). Consider fine-tuning the model on a domain-specific corpus of HR documents in the future.
- F-2: Over-reliance on Automation
 - Mitigation: Design the UI to emphasize that the tool is a "Screener" not a "Selector." Include prominent disclaimers like, "Scores are based on semantic similarity and should be used as a preliminary filter only. Final hiring decisions require human judgment."
- P-1: Scope Creep
 - Mitigation: Adhere to a strict product roadmap. Use an issue-tracking system (e.g., Jira, GitHub Projects). Formalize a change request process where new features must be approved only after the core Minimum Viable Product (MVP) is stable and delivered.

4.0 Monitoring and Review

- Technical Monitoring: Implement application logging and monitoring (e.g., using Prometheus/Grafana) to track extraction success rates, response times, and error rates.
- Fairness Monitoring: Periodically re-run bias audits, especially after any model updates.
- User Feedback: Actively collect and review user feedback to identify new functional risks or inaccuracies not caught during testing.
- Plan Review: This Risk Management Plan will be reviewed and updated on a quarterly basis or following any major incident or significant change to the application.