

DECISIONFLOW

Quality, Security & Release Readiness Report

Test evidence, operational controls and release gates

Document code	DEV-03
Version	2.0
Status	Final Public Portfolio Edition — Implementation Baseline
Baseline date	14 July 2026
Author	Min Thu Kyaw
Role	AI Product Manager

Evidence transparency: Actual implementation evidence is separated from targets, proposed release actions, and the illustrative DEV-06 continuity bridge. Later commercial outcomes are not presented as actual results.

Document Control

Purpose	Document the Develop phase for Quality, Security & Release Readiness Report.
Primary audience	Hiring managers, product leaders, engineering stakeholders, and pilot reviewers.
Evidence classification	Verified implementation fact / implementation-derived assessment / target / proposed next action.
Source limitation	Implementation status is grounded in the authored implementation baseline and public repository references supplied for the case study.
Change control	Publication rule: retain evidence labels unless content is replaced by documented real-world observations.

Evidence Links

- [Low-Fidelity Prototype](#)
- [High-Fidelity Prototype](#)
- [MVP Frontend Repository](#)
- [MVP Backend Repository](#)

Contents

1. Readiness Summary
2. Current Quality Evidence
3. Test Strategy
4. Defect and Risk Register
5. Security Assessment
6. Privacy Assessment
7. Non-Functional Targets
8. Environment and Deployment
9. Observability
10. Backup and Recovery
11. Release Gates
12. Incident and Rollback Ownership
13. Recommendation

Readiness Summary

Current status: internal development candidate — The MVP has meaningful backend test evidence and a connected workflow, but lacks frontend/E2E regression coverage, verified production build evidence, product analytics, integrated staging, and several external-user security controls.

Current Quality Evidence

Evidence	Result	Interpretation
Backend automated tests	15 passed on 14 July 2026.	Useful API baseline; not full production proof.
Backend coverage areas	Auth, password change, ownership, decision CRUD, transcript validation/extraction, recommendations and AI service behavior.	Covers core API behaviors.
Backend test database	In-memory SQLite.	PostgreSQL integration differences remain a risk.
Frontend lint	Passed.	Static quality only.
Frontend production build	Not verified in the implementation baseline; treated as a release gate rather than an achieved result.	Must be verified in clean CI.
Frontend unit/component tests	None found.	Gap.
End-to-end tests	None found.	Critical workflow gap.
API integration script	Exists but requires a live API and is not default CI.	Useful starting point; automate it.

Test Strategy

Layer	Required coverage	Release evidence
Backend unit/API	Transitions, persistence, finalization, ownership, validation, rate limits and AI error mapping.	CI test report and coverage summary.
Frontend component	Auth, upload rejection, editing, weights, error states, filters and retained settings.	Component test report.
End-to-end	Register, paste/TXT, edit, regenerate, compare, finalize, reload, resume, archive and provider failure.	Browser-run video/log and CI pass.
AI evaluation	Extraction field scores, groundedness, injection resistance, fallback and multilingual scope.	Versioned benchmark report.
Migration	Clean install and upgrade from prior schema.	Migration job pass on PostgreSQL.
Security	Ownership isolation, auth/session, secrets, rate limiting, input abuse and dependency scan.	Security checklist and findings disposition.

Layer	Required coverage	Release evidence
Production smoke	Health, auth, non-sensitive extraction, recommendation, final retrieval and cross-user denial.	Signed smoke-test record.

Defect and Risk Register

Risk	Probability	Impact	Required mitigation
Reviewed edits not durable	High/current	Critical	Persist reviewed version and test reload/resume.
Cross-decision local draft contamination	High/current	Critical	ID-based server hydration.
Synthetic scores misread as AI	High/current	High	Replace or relabel with transparent formula.
Incomplete final record	High/current	High	Store selected option, accepted version and immutable snapshot.
JWT theft through XSS	Medium	High	Prefer HttpOnly session or formally accept and mitigate short-lived-token risk.
Provider outage or quota	Medium	High	Error taxonomy, retry/idempotency and visible fallback.
Sensitive source retention	High	High	Consent, retention, deletion and vendor review.
No E2E regression suite	High/current	High	Automate critical workflow before pilot.
PostgreSQL vs SQLite difference	Medium	Medium	Run CI/staging tests against PostgreSQL.
Duplicate repository/deployment path	High/current	High	Declare one release source of truth.

Security Assessment

Control	Current state	External-pilot requirement
Password storage	bcrypt hash.	Retain and test password policy.
Authorization	Backend ownership checks.	Add explicit cross-user negative tests for every resource route.
Session	JWT in local storage.	Prefer HttpOnly secure cookie + CSRF; otherwise document accepted risk.
Route middleware	Presence cookie for navigation convenience.	Do not treat it as authorization.
JWT secret	Configurable, with unsafe development default.	Fail deployment when default secret is used.
Rate limits	Not evident.	Per-user/IP limits for auth and AI endpoints.
Secrets	AI key backend-only.	Managed secret store and rotation process.
Audit events	Generic history exists.	Semantic actor/time events for review, acceptance and finalization.
Account lifecycle	No reset, verification or revocation found.	Define minimum pilot lifecycle; password reset is likely P0.

Privacy Assessment

- Organizations/users retain ownership of source content and decision records.
- Raw source and AI results require a documented retention period.
- Users need a deletion path and disclosure of third-party AI processing.
- Analytics must use metadata and counts, not transcript or decision content.
- Pilot consent should state whether source data is stored, where it is processed and how long it remains.

Non-Functional Targets

Category	Pilot target	Evidence required
Availability	99% monthly excluding announced maintenance.	Uptime monitor.
Non-AI API latency	p95 < 500 ms under expected pilot load.	Load test and telemetry.
AI latency	p95 < 35 seconds with recoverable timeout.	Provider telemetry.
Data isolation	100% owner enforcement.	Automated negative tests.
Accessibility	Keyboard-operable core flow and WCAG 2.1 AA contrast target.	Accessibility test record.
Browser support	Latest two stable Chrome, Edge, Firefox and Safari.	Cross-browser matrix.
Recovery	Backup/restore tested before real pilot data.	Restore drill record.

Environment and Deployment

Environment	Purpose	Policy
Local	Developer iteration.	Synthetic/test data; optional fallback AI.
CI/Test	Automated verification.	Synthetic fixtures and mocked AI by default.
Staging	Integrated release candidate.	Approved test data; capped AI budget; production-like PostgreSQL.
Production pilot	Controlled external/internal users.	Managed secrets, monitoring, backups and retention.

- Backend includes Railway-oriented migration and health-check configuration according to the baseline.
- Frontend workflow installs, lints and builds on main, but integrated deployment evidence is incomplete.
- Repository documentation must match the backend-connected implementation rather than describe mock-only behavior.
- One release source of truth must be declared before CI/CD hardening.

Observability

Signal	Required telemetry
--------	--------------------

Signal	Required telemetry
API health	Request rate, p95 latency, 4xx/5xx and dependency failures.
AI operations	Provider/model, latency, tokens, cost, fallback and error category.
Workflow	Started, extracted, reviewed, recommended, compared, finalized and resumed.
Security	Failed login, rate-limit, invalid token and cross-owner denial.
Data	Migration failure, persistence error and backup status.

Backup and Recovery

1. Define backup frequency and retention.
2. Run a restore into a clean staging environment.
3. Verify decisions, transcripts, recommendations and history after restore.
4. Document recovery-time and recovery-point objectives appropriate for pilot.
5. Assign a named incident and restore owner.

Release Gates

Gate	Pass condition
Source of truth	Frontend and backend release repositories and branches are declared.
Data integrity	Reviewed values, weights, resume and final outcome are durable.
AI trust	Provenance, fallback, versions and benchmark thresholds are implemented.
Quality	Backend, frontend build, integration, E2E and migration jobs pass in CI.
Security/privacy	Session decision, secrets, rate limits, disclosure, retention and deletion approved.
Operations	Staging, monitoring, backups, rollback and smoke tests pass.
Learning	Funnel analytics and pilot measurement dashboard are visible.
Defects	No open critical/high defect affects auth, ownership, persistence, AI transparency or finalization.

Incident and Rollback Ownership

Area	Accountable role	Minimum runbook
Product scope	Product Manager	Pilot pause and user communication decision.
Application	Engineering owner	Rollback deploy and error triage.
Database	Backend/platform owner	Migration rollback and restore.
AI provider	AI/backend owner	Provider disable, model rollback and budget control.

Area	Accountable role	Minimum runbook
Security/privacy	Technical/security owner	Containment, access review and notification assessment.

Recommendation

Release recommendation: NO-GO for uncontrolled external availability — Proceed with internal testing and staging. Move to a controlled pilot only after all critical integrity, transparency, security and regression-test gates pass or are explicitly waived by accountable owners.

Evidence and References

Source	Use in this document
Implementation-derived baseline	DECISIONFLOW_MVP_DEVELOPMENT_PHASE.md, baseline date 14 July 2026.
Low-fidelity prototype	https://minthukyawdev-droid.github.io/decision-flow/
High-fidelity prototype	https://minthukyawdev-droid.github.io/decisionflow-hifi-prototype/
Frontend repository reference	https://github.com/minthukyawdev-droid/decisionflow-webapp
Backend repository reference	https://github.com/minthukyawdev-droid/decisionflow-api
Plan-phase package	DecisionFlow Plan Phase Document Set, version 1.0.

Interpretation rule — Targets, proposed metrics, future releases, and pilot thresholds are not reported as achieved results. Actual results must be added only after executing the relevant test or study.