

DECISIONFLOW

Reliability, Security and Service Operations Report

SLOs, observability, capacity, incidents, security operations, backup, recovery, vendors, and controlled-growth limits

DELIVER PHASE | Version 1.0 | Illustrative 90-day controlled-scale program

EVIDENCE & PUBLISHING INTEGRITY

This public portfolio edition distinguishes actual evidence, assumed continuity steps, simulated case-study outcomes, targets, and recommendations. Simulated customers, commercial results, benchmarks, incidents, quotations, and later-lifecycle outcomes are illustrative and must not be interpreted as results from a live commercial product. Evidence labels are retained throughout the package to support transparent and responsible interpretation.

Document Control

Control	Definition
Document code	DEL-06
Version / status	2.0 — Final Public Portfolio Edition — Simulated Delivery Scenario
Baseline / author	14 July 2026 - Min Thu Kyaw
Lifecycle continuity	Actual MVP -> DEV-06 assumed productionization -> simulated launch -> Conditional Scale -> Deliver phase.
Delivery decision	Execute a 90-day controlled-scale program; keep collaboration, integrations, richer ingestion, and enterprise features evidence-gated.
Evidence rule	Actual, assumed, simulated, target, and recommendation statements are explicitly separated.

Actual Project Artifacts

Artifact	Reference
Low-Fidelity Prototype	View prototype
High-Fidelity Prototype	View prototype
MVP Frontend Repository	Open repository
MVP Backend Repository	Open repository

Contents

01	Service objective and operating boundary
02	SLOs and error budgets
03	Observability and alerting
04	Capacity and performance
05	Incident and change operations
06	Security and privacy operations
07	Backup, recovery, and vendor resilience
08	Operational qualification decision

Service Objective and Operating Boundary

Service Operations keeps DecisionFlow reliable and secure within a declared usage range. Controlled scale means that acquisition, concurrency, support, and feature scope remain bounded by tested capacity and incident readiness. Passing the 40-job gate does not imply unlimited scale.

Approved boundary - The simulated delivery program approves normal product growth and up to 40 concurrent AI jobs under the tested configuration. The 80-job profile remains a scale condition and is not marketed as supported capacity.

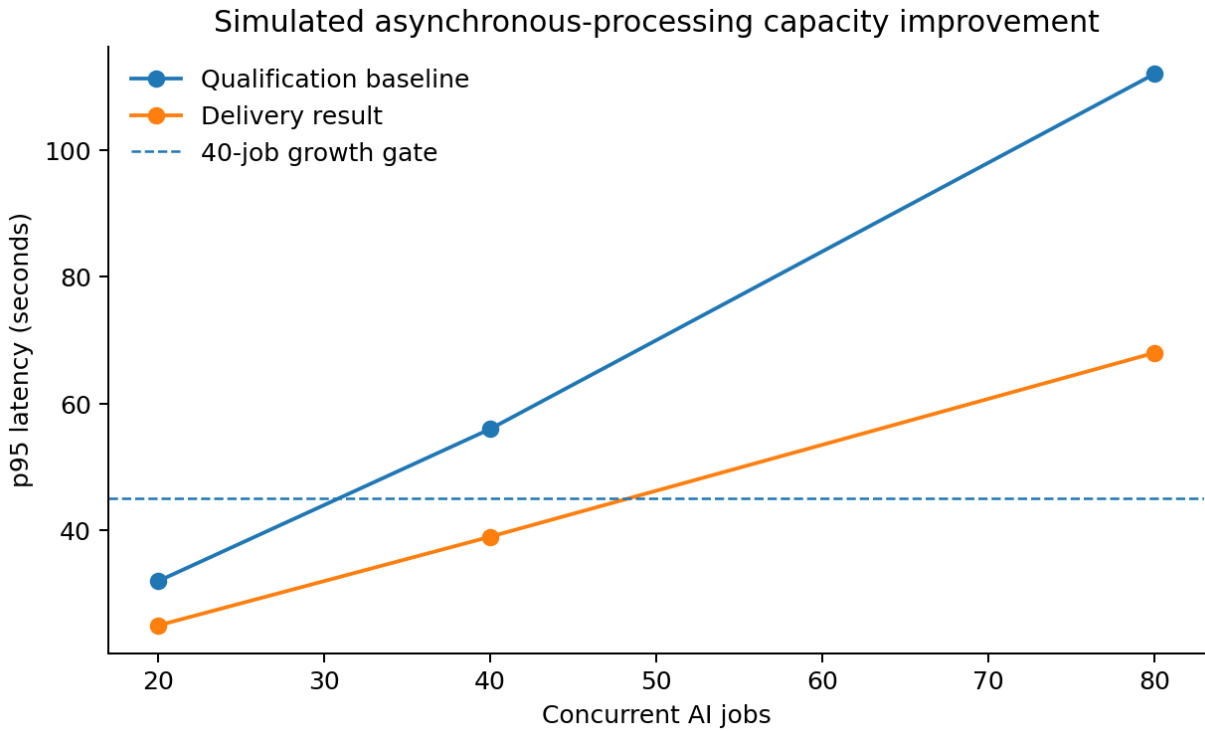
SLOs and Error Budgets

Service indicator	Objective	Simulated result	Status
Monthly availability	>=99.9%	99.96%	Pass
p95 non-AI API latency	<500 ms	340 ms	Pass
p95 AI generation normal load	<=35 sec	27 sec	Pass
40-job p95 AI latency	<=45 sec	39 sec	Pass
40-job AI failure rate	<1%	0.7%	Pass
Duplicate generation from one action	0	0 in test and sampled production	Pass
Critical/high unresolved security finding	0	0	Pass
Restore RTO / RPO	<=45m / <=5m	35m / 3m	Pass
Error-budget policy		Action	
Healthy budget		Continue planned delivery with normal review.	
50% consumed before mid-period		Reduce risky change and prioritize reliability.	
Budget exhausted		Freeze non-essential releases until root cause and corrective evidence are approved.	
Security or data-isolation event		Does not wait for budget; activate incident response immediately.	

Observability and Alerting

Layer	Key telemetry	Privacy control
Frontend	Route failures, task timing, error category, correlation ID.	No decision content or auth token.
API	Request rate, status, latency, ownership failures, rate-limit events.	Structured fields only; no raw transcript.
AI jobs	Queue age, status, retry, provider, model, prompt, tokens, latency, fallback.	Content excluded; secure references only.
Database	Connections, query latency, migration, backup, storage and restore.	Least privilege and encrypted backups.
Billing	Event ID, entitlement transition, reconciliation status.	No full payment credentials.
Product metrics	Activation, finalization, retention, retrieval and paid state.	Aggregate behavior and stable metric contracts.
Alert	Threshold example	Owner
AI queue age	p95 exceeds normal threshold for 10 minutes	Platform / AI
Provider failures	Failure rate >2% or quota/auth error spike	AI/Backend
Ownership / auth anomalies	Unexpected increase or confirmed cross-user access	Security / Backend
Billing reconciliation	Unmatched or failed entitlement events	Backend / Commercial
Metric pipeline	Event volume or denominator contract deviates	Product / Data owner
Backup / restore	Backup missed or restore drill fails	Platform

Capacity and Performance



Load capacity improvement

Load profile	Qualification baseline	Simulated delivery result	Decision
20 concurrent jobs	32s p95; 0.8% failures	25s; 0.4%	Supported
40 concurrent jobs	56s; 1.9%	39s; 0.7%	Supported controlled-growth ceiling
80 concurrent jobs	112s; material failure risk	68s; 1.4%	Not qualified

- Queue depth, worker concurrency, provider quotas, database connections, and retry policy are capacity parameters, not hidden implementation details.
- Growth caps are reviewed against observed peak jobs, queue age, support demand, and provider resilience.
- A higher ceiling requires a new load test, failure drill, cost review, and documented operating decision.

Incident and Change Operations

Incident phase	Required action
Detect	Alert, support report, evaluation failure, operator review, or customer disclosure.
Declare	Severity, incident commander, affected system and current customer impact.
Contain	Disable route/model/release, reduce load, revoke secret, block affected workflow, or apply safe fallback.
Communicate	Accurate status, affected boundary, workaround and next update without unsupported certainty.
Recover	Restore qualified service and validate data integrity, ownership and billing state.
Learn	Root cause, timeline, contributing controls, follow-up owners, regression and runbook updates.
Change type	Required control
Application release	CI tests, migration plan, staged deploy, smoke test, monitoring and rollback.
Database migration	Forward/backward compatibility, backup, restore path and ownership validation.
AI model/prompt/routing	Fixed evaluation, cost/latency comparison, provenance, canary and rollback.
Secret/configuration	Managed secret store, least privilege, validation and rotation plan.

Incident phase	Required action
Capacity change	Load evidence, cost model, alert tuning and updated operating boundary.

Security and Privacy Operations

Control area	Operating practice
Identity and session	Secure cookie/session design, expiry, logout, password recovery, rate limits and anomaly monitoring.
Authorization	Owner-scoped queries for every decision, transcript and recommendation; negative tests in CI.
Secrets	No defaults in production; managed storage, rotation and access review.
Data handling	Raw source retention policy, deletion path, encrypted transport/storage and provider disclosure.
Logging	No raw decision content, credentials or tokens in analytics and standard logs.
Dependencies	Patch review, vulnerability response and controlled upgrade cadence.
Security review	Threat review for each new input, external integration, billing, multi-user or enterprise surface.

Backup, Recovery, and Vendor Resilience

Scenario	Recovery evidence
Database restore	Encrypted backup restored in 35 minutes with 3-minute RPO in simulated drill.
Application rollback	Previous release restored after smoke-test failure without schema/data loss.
AI provider outage	Queued jobs paused or approved alternate used with explicit provenance; no silent route change.
Billing provider delay	Entitlements reconciled from event IDs and provider state; manual path documented.
Lost worker / stuck job	Visibility, retry cap, dead-letter review and customer-safe status available.

Operational Qualification Decision

Operations decision - APPROVED FOR CONTINUED CONTROLLED SCALE within the tested 40-concurrent-job boundary. The 80-job profile, broader provider independence, and any multi-user or enterprise surface require new qualification.

- No simulated critical or high-severity customer-impacting incident remained open at program close.
- Availability, normal latency, 40-job capacity, restore, and security gates pass.
- Provider concentration and higher-load behavior remain the principal operational constraints.

Evidence discipline: replace all simulated delivery values with observed, reproducible results before presenting them as actual product performance.