DECISIONFLOW

Retirement Risk, Issue and Compliance Register

Managing customer, data, AI, commercial, technical, legal, and reputation risks through closure

RETIRE PHASE | Version 1.0 | Illustrative controlled retirement and knowledge-preservation 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	RET-06
Version / status	2.0 — Final Public Portfolio Edition — Simulated Retirement Scenario
Baseline / author	14 July 2026 - Min Thu Kyaw
Scenario horizon	Illustrative 24-month post-scale operating period followed by a 180-day retirement program.
Lifecycle continuity	Actual MVP -> assumed productionization -> simulated Launch -> Qualify -> Deliver -> Controlled Scale -> Retire.
Retirement decision	Retire the standalone service through a controlled transition while preserving reusable product, AI, and technical assets.
Scope boundary	No new collaboration, integration, richer-ingestion, multilingual, SSO, or enterprise-platform build is assumed.
Evidence rule	Actual, assumed, simulated, target, recommendation, and verified-shutdown statements are 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	Risk governance
02	Retirement risk register
03	Issue and escalation model
04	Compliance control checklist
05	Evidence and exception management
06	Residual risk acceptance

Risk Governance

Risk rule - A schedule delay is preferable to an uncontrolled customer, privacy, security, billing, or data-integrity failure. Critical risks pause the dependent retirement step.

Cadence	Purpose	Participants
Weekly steering review	Decisions, milestones, high risks, exceptions, customer status.	Product, engineering, privacy/legal, security, finance, customer success, support.
Daily shutdown stand-up	Open incidents and technical/data dependencies during T-7 to T+7.	Execution owners and incident commander.
Deletion review	Legal holds, deletion exceptions, backup expiry, processor confirmation.	Privacy/legal, security, platform, data owner.
Commercial reconciliation	Billing, refunds, disputes, receivables, vendors.	Finance, procurement, customer success.
Final closure review	Accept residual risk and approve program closure.	Executive sponsor and cross-functional owners.

Retirement Risk Register

ID	Risk	P	Impact	Mitigation	Owner	Status
R-01	Customer misses announcement	Medium	High	Multi-channel notice, direct outreach, non-response escalation.	Customer Success	Closed
R-02	Customer cannot export before deadline	Medium	Critical	Self-service validation, assisted export, extension exceptions.	Support / Engineering	Closed
R-03	Eligible data deleted too early	Low	Critical	Cooling-off period, legal-hold check, two-person approval, rollback window.	Privacy / Platform	Closed
R-04	Customer data retained too long	Medium	High	Authoritative inventory, deletion jobs, backup expiry, processor confirmations.	Privacy / Data	Closed
R-05	AI credential or provider job remains active	Low	High	Credential inventory, usage monitoring, revocation verification.	AI / Security	Closed
R-06	Billing continues after service closure	Medium	High	Renewal block, mandate audit, reconciliation, customer monitoring.	Finance	Closed
R-07	Hidden infrastructure dependency prevents shutdown	Medium	High	Dependency map, staged removal, cloud inventory, final bill review.	Platform	Closed
R-08	Repository archive contains secrets	Medium	High	History scan, key revocation, read-only archive, access review.	Security / Engineering	Closed
R-09	Support demand exceeds capacity	Medium	Medium	Dedicated queue, staffing reserve, templates, assisted-export appointments.	Support	Closed
R-10	Retirement damages customer trust	Medium	High	Transparent rationale, long notice, no surprise billing, migration support.	Product / CS	Monitored
R-11	Licensing talks delay customer clarity	Low	Medium	Separate workstream; no dependency on retirement dates.	Executive / Legal	Closed
R-12	Legal hold scope is ambiguous	Low	Critical	Counsel authority, hold register, segregated encrypted archive.	Legal / Privacy	Open-controlled

Issue and Escalation Model

Severity	Definition	Action
Critical	Customer-data loss, unauthorized access, deletion outside scope, unresolved legal obligation, or service closure without required export.	Stop dependent steps, activate incident command, notify executives and specialists, preserve evidence.
High	Material export mismatch, billing failure, provider exposure, or customer transition block.	Resolve before next gate or obtain explicit executive exception.
Medium	Non-critical delay, documentation gap, vendor variance, or support backlog.	Assign owner and due date; review weekly.
Low	Cosmetic, low-impact, or post-closure improvement.	Track in final retrospective and knowledge archive.

Compliance Control Checklist

Control area	Required evidence	Illustrative status
Privacy notice	Published retirement and data-disposition communication.	Complete
Customer rights	Export, deletion, access, billing dispute, and support channels.	Complete

Control area	Required evidence	Illustrative status
Retention schedule	Account, content, audit, billing, analytics, backup, and legal-hold rules.	Complete
Processor closure	AI, cloud, support, payment, monitoring, and email vendors.	Complete
Security	Access review, secret revocation, repository scan, evidence protection.	Complete
Contract	Renewal, termination, refund, liability, and notice obligations.	Complete
Finance / tax	Final invoices, credits, receivables, records, and vendor settlement.	Complete
Auditability	Account dispositions, deletion evidence, approvals, incidents, and exceptions.	Complete

Evidence and Exception Management

- Evidence artifacts use stable IDs, owners, dates, retention class, and access restrictions.
- Exceptions identify the affected account/system, authority, risk, compensating control, expiry, and approver.
- Verbal approval is not sufficient for legal hold, deletion, service-date, billing, or customer-access exceptions.
- The evidence archive is read-only after final closure and separated from the retired production environment.
- Customer content is not copied into the evidence archive unless strictly necessary and legally approved.

Residual Risk Acceptance

Residual risk	Disposition
Two legal holds remain after normal deletion window.	Accepted with counsel ownership, encrypted segregation, quarterly review, and scheduled release.
Public references to the retired product may persist.	Maintain defensive domain and closure page for approved period; monitor impersonation risk.
Archived open-source dependencies may later show vulnerabilities.	Repositories remain non-running and read-only; retain software bill of materials and reuse review requirement.
Some customers may remain dissatisfied despite successful transition.	Record feedback and preserve communication evidence; no unresolved contractual or data issue remains.

Evidence discipline: replace all simulated retirement values with observed, reproducible records before presenting them as actual product performance or compliance evidence.