LEXICA LEDGER PROTOCOL

Master Architecture White Paper v5.4

Audit-Defensible Structural Outline and Content Framework

Cryptographic Control and Decision-Provenance Architecture for Enterprise AI Systems

Jurisdictional operating context: Ontario, Canada (ON_CA)

Document ID: LLP-MAWP-5.4-FRAMEWORK-2026-08-05

Status: CONTROLLED CANDIDATE / PARTIALLY VERIFIED / NOT FOR EXTERNAL RELIANCE

North Star

Lexica Ledger Protocol does not eliminate enterprise responsibility. It is designed to make covered decisions attributable, policy-bound, tamper-evident, economically reconcilable, and independently verifiable within a declared technical and legal scope.

Prepared as a drafting and approval framework for CISO, CFO, General Counsel, auditors, insurers, and board risk committees.

Source basis: attached 42-page Master Architecture White Paper Blueprint. Final publication requires licensed legal review and independent technical verification.

Controlled Front Matter

Control field	Required value
Document identifier	LLP-MAWP-5.4-FRAMEWORK-2026-08-05
Version	5.4 candidate framework
Publication date	2026-08-05
Status	Controlled candidate; deployment claims require artifact verification
Jurisdiction reviewed	Ontario, Canada operating context; EU and US obligations mapped only where the source blueprint provides them
Authors	Protocol architecture, cryptographic systems, security engineering, finance controls, and legal drafting owners to be named
Required reviewers	CISO; CFO; General Counsel; Chief Cryptographer; Smart Contract Auditor; Privacy Officer; External Auditor
Confidentiality	Internal controlled draft until publication gates close
Superseded documents	All v5.2/v5.4 marketing claims that conflict with this framework
Legal status	Technical and legal drafting framework. Not a jurisdiction-specific legal opinion.

Approval Signature Register

Role	Approval question	Name / signature / date
CISO	Are enforcement boundaries, key custody, tenant isolation, failure modes, and recovery independently tested?	OPEN
CFO	Are all costs, reserves, treasury rights, stress losses, and settlement controls included?	OPEN
General Counsel	Are role classifications, legal claims, evidence limits, retention duties, and licensing assumptions supportable?	OPEN
Chief Cryptographer	Are primitives, parameters, setup, proofs, and test vectors complete and independently reviewed?	OPEN
External Auditor	Can the package be reproduced without trusting the Lexica dashboard?	OPEN
Board / Risk Committee	Are residual risks owned, funded, escalated, and accepted?	OPEN

Claim-Status Legend

Label	Meaning	Publication rule
[DEPLOYED]	Publicly deployed and independently inspectable.	Requires public endpoint, source or configuration evidence, release tag, and operating record.
[VERIFIED]	Confirmed by independent audit, test, certificate, or chain record.	Name reviewer, date, scope, method, and report hash.
[MEASURED]	Produced by a documented reproducible benchmark.	State environment, payload, region, sample size, percentiles, and exclusions.
[DESIGN TARGET]	Intended performance or control goal.	Never write as a present fact or guarantee.
[ASSUMPTION]	Required condition not enforced or independently proven.	State owner, validation method, and failure impact.
[LEGAL INTERPRETATION]	Counsel interpretation of a legal requirement.	Cite controlling authority and identify jurisdiction and role.
[THIRD-PARTY DEPENDENCY]	Relies on Base, Ethereum, Circle, Cloudflare, HSM, RPC, or another provider.	State outage, governance, security, and exit assumptions.
[ROADMAP]	Not production deployed.	State entry criteria, exit criteria, owner, target horizon, and compatibility plan.

Mandatory claim discipline

Every material sentence in the final paper shall carry a status label in the drafting source. The published prose may hide the label only after a linked claim register preserves it.

Contents and Decision Path

Reading order

Executives should read the blockers, decision summary, their relevant section, the assurance gates, and the final approval questions. Drafting teams should use every section and appendix as a controlled work breakdown structure.

Executive Publication Blockers

Blocking correction: contract identity

The address 0x833589fCD6eDb6E08f4c7C32D4f71b54bdA02913 is Circle native USDC on Base. It shall not be described as a Lexica query contract or LexicaVault.sol. A real Lexica settlement contract requires its own verified address, ABI, bytecode hash, deployment transaction, audit, owner, proxy, timelock, and emergency-control package.

Blocking correction: no absolute leakage promise

The final paper shall not promise zero raw-data retention or zero disk leakage across the whole system. The bounded target is no plaintext payload persistence in the declared stateless edge tier, plus tenant-controlled encrypted evidence retention with documented legal holds, deletion rules, and failure tests.

Blocking correction: no stealth treasury daemon

Treasury sweeps shall be observable, access-controlled, rate-limited, policy-bound, reconciled, and signed. The word "stealth" is prohibited. scripts/sweep_treasury.js may be cited only after source review, hash publication, deployment evidence, key-boundary review, and run-log verification.

Claim or artifact	Framework status	Evidence required before external publication
Cloudflare edge WAF	[ASSUMPTION] Reported current control.	Zone identifier, ruleset export, change history, bypass test, owner, and coverage map.
/api/v1/chat	[ASSUMPTION] Reported current endpoint.	Endpoint availability test, version header, authentication policy, schema, error states, and deployment tag.
$0.0015 USDC standard micro-toll	[ASSUMPTION] Public schedule.	Contract or accounting rule, invoice sample, rate version, customer agreement, and reconciliation.
$0.0075 exception surcharge	[DESIGN DECISION REQUIRED]	State whether incremental or total. This framework assumes incremental unless changed by approved pricing policy.
scripts/sweep_treasury.js	[ASSUMPTION] Repository artifact.	Source hash, code review, scheduler configuration, signer policy, limits, logs, and rollback plan.
v5.4 mainnet	[ASSUMPTION] Not established by the blueprint.	Release tag, deployment records, verified contracts, runbook, audit reports, and production SLO evidence.
v6.0+ decentralized node federation	[ROADMAP]	Federation threat model, consensus or coordination design, validator admission, slashing or accountability model, and migration plan.

Executive Decision Summary

Executive	Decision to be secured	Minimum reserve or evidence consequence
CISO	Approve bounded enforcement, tenant isolation, key custody, durable evidence, and recovery controls.	No approval until bypass, cross-tenant, queue-loss, key-failure, and disaster-recovery tests pass.
CFO	Approve unit economics, treasury structure, circuit breakers, and residual-risk reserves.	No margin claim without all-in COGS, gas stress, low-volume case, exception storm, depeg, and customer-concentration analysis.
General Counsel	Approve role mapping, legal claims, retention, evidence positioning, and payment-regulatory assumptions.	No safe-harbor language. No categorical personal-liability claim. No custody claim without legal opinion.
Board / Risk Committee	Fund Lexica as a preventive control, evidence system, and investigation-cost reducer.	Maintain separate legal, security-incident, treasury, and customer-credit reserves.

Budget framing

The budget case shall not say "buy Lexica to eliminate liability." It shall say: fund Lexica as a preventive control, evidence system, and investigation-cost reducer, while maintaining a separate residual-risk reserve.

Section I - Executive Abstract and the Executive Liability Trap

I.1 Draft Executive Abstract

[LEGAL INTERPRETATION] Enterprises deploying autonomous or semi-autonomous AI systems retain duties that cannot be eliminated through a model-provider contract. These duties may include risk management, record-keeping, quality management, incident assessment, disclosure, supervision, privacy, and evidentiary preservation.

[DESIGN TARGET] Lexica Ledger Protocol is designed as an enforcement and evidence layer. It does not determine legal compliance. It creates signed, policy-bound, tamper-evident records that permit authorized parties to reconstruct the requested decision, applied policy, authority, exception path, and external settlement status.

[LIMITATION] Lexica does not replace governance, human supervision, legal analysis, incident response, privacy programs, financial controls, or the evidentiary foundation required in a proceeding.

I.2 The Liability Squeeze

> **Definition**
>
> The Liability Squeeze is the condition in which an enterprise depends on third-party AI systems while retaining non-transferred or non-delegable duties concerning supervision, risk management, records, disclosure, quality controls, and legal accountability.

Exposure category	Possible owner	Lexica contribution	Residual duty
EU AI Act provider duty	Provider or modified-system operator	Control evidence, policy lineage, risk and test records	Design and operate the full provider compliance system.
EU AI Act deployer duty	Deploying enterprise	Automatic event records, supervision evidence, exception and approval trail	Classify use, supervise, preserve context, and meet deployer duties.
Contract claim	Customer, vendor, or integrator	Attribution, sequence, policy version, and approval evidence	Interpret contract, prove breach, causation, damage, and allocation.
Securities disclosure	Issuer and governance bodies	Incident chronology, system scope, decision history, materiality inputs	Make and document the materiality decision and file required disclosures.
Criminal concealment or obstruction	Individuals involved in conduct	Makes concealed alteration harder and preserves escalation records	Lexica cannot eliminate individual exposure for conduct.
Data protection	Controller, processor, or joint actors	Minimization, access history, encryption, purpose and retention metadata	Establish legal basis, rights handling, transfers, notices, and processor governance.
Investigation cost	Enterprise and insurers	Faster evidence reconstruction and independent verification	Staff investigation, preserve privilege, engage experts, and remediate.
Evidentiary dispute	Party offering the record	Integrity, authentication, chronology, and system-process evidence	Establish admissibility, relevance, authenticity, and foundation.

I.3 EU AI Act Control Framing

Article	Duty focus	Lexica evidence contribution	Prohibited overstatement
Article 9	Lifecycle risk-management system	Risk decision, policy version, test result, exception, mitigation, approval, monitoring, and residual-risk evidence.	A Merkle root alone satisfies Article 9.
Article 12	Automatic logging capabilities	Event type, time, attribution, operation context, action, continuity, and reconstructable underlying evidence.	A hash without accessible context automatically satisfies logging duties.
Article 17	Documented quality management system	Policy and QMS linkage, approvals, testing, monitoring, exception handling, accountability, incident handling, and resource controls.	Lexica alone is the customer quality management system.

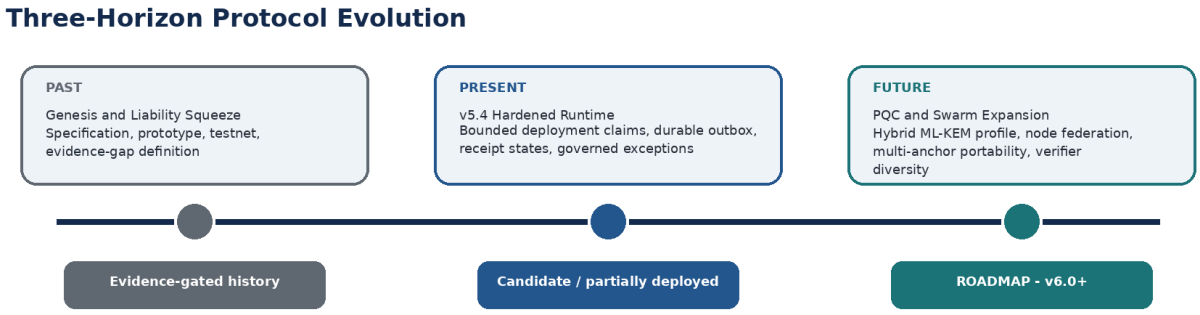
I.4 SEC and Individual-Exposure Framing

- Use the SEC cybersecurity rules as disclosure-control and governance duties, not as a general criminal-liability statute for AI decisions.
- Use SolarWinds as a disclosure-control case study. Do not describe it as categorical precedent for direct CISO liability.
- Use the former Uber security chief case only to explain that concealment, obstruction, and inaccurate escalation can create individual exposure in exceptional cases.
- Separate corporate, regulatory, securities, contractual, civil, and possible individual exposure. Do not merge them.

I.5 Drafting Matrix

Subsection	Control objective and required content	Required artifact	Sign-off gate
Executive abstract	Open with enterprise duty. Define Lexica as enforcement and evidence support. State limitations.	One-page approved abstract and claim register.	GC accepts legal framing; CISO accepts control objective.
Liability squeeze	Map role, contract, jurisdiction, knowledge, control failure, disclosure, and evidence consequences.	Role map, contract-risk example, residual-risk table.	GC and CFO accept exposure categories.
Evidence gap	Explain mutable logs, missing policy versions, missing approvals, weak identity, and missing chain of custody.	Threat examples and log-control comparison.	CISO accepts evidence problem statement.
Control outcome	Define attributable, policy-bound, tamper-evident, economically reconcilable, independently verifiable records.	Bounded assurance statement.	Auditor confirms reproducibility objective.
Limitations	State no safe harbor, no immunity, no automatic admissibility, no absolute non-bypassability.	Published limitations and residual-risk owner map.	Board accepts retained risks.

Section II - Protocol Evolution Timeline



Rule: actual dates and production labels require release tags, source hashes, deployment records, audit reports, and reproducible tests.

II.1 Three-Horizon Chronology

Horizon	Narrative	Status discipline	Required evidence
Past - Genesis and Liability Squeeze	Specification genesis; prototype; Base Sepolia testnet; closed enterprise pilot; adversarial testnet; cryptographic readiness.	Do not invent dates. State only artifact-supported milestones.	Signed architecture decision record; threat model; schema; test vectors; testnet contract; pilot scope; measurements; audit and ceremony records.
Present - v5.4 Hardened Runtime	Bounded edge enforcement, identity, canonical records, durable outbox, receipt state machine, governed Exception Oracle, tenant roots, Base anchoring, toll accounting, and dossier generation.	Split [DEPLOYED], [VERIFIED], [MEASURED], [DESIGN TARGET], and [ASSUMPTION].	Release tag; deployment manifests; gateway config; queue and outbox tests; contract package; reconciliations; sample dossier.
Future - PQC and Swarm Expansion	Hybrid ML-KEM transition; key and algorithm agility; decentralized node federation; verifier diversity; multi-anchor portability; sovereign enterprise nodes.	Every item is [ROADMAP] until independently inspectable.	Federation threat model; node protocol; governance; compatibility; exit and migration tests; PQC profile and downgrade policy.

II.2 Maturity Gates

Stage	Entry evidence	Exit evidence
Specification genesis	Signed architecture decision record.	Frozen threat model and protocol schema.
Prototype	Local commitment and verifier.	Reproducible test vectors.
Base Sepolia testnet	Verified test contract and funded accounts.	Epoch, debit, proof, dispute, pause, and recovery tests.
Closed pilot	Signed customer scope and controlled workload.	Measured latency, loss, exception, support, and reconciliation data.
Adversarial testnet	Public challenge rules and monitoring.	Resolved findings and independent report.
Cryptographic readiness	Frozen circuit, parameters, and key lifecycle.	Audit, setup ceremony, transcript, verifier key, and test vectors.
Controlled mainnet	Production contract, limited caps, pause controls, support runbook.	Stable operations, reconciled financials, incident record, and SLO evidence.
Sovereign enterprise deployment	Customer key custody and isolated data plane.	Independent customer verification and tested exit.
Federated node network	Approved federation design and adversarial test plan.	Multi-node consistency, equivocation detection, governance, and migration evidence.

II.3 Present-State Claim Register

Item	Permitted v5.4 wording	Artifact needed
Cloudflare edge WAF	[ASSUMPTION] Reported as a current edge control within a declared coverage boundary.	Ruleset export, owner, change log, test evidence, and uncovered routes.
/api/v1/chat	[ASSUMPTION] Reported production request path.	Versioned OpenAPI schema, authentication controls, state response examples, and release tag.
Base address 0x833589...	[THIRD-PARTY DEPENDENCY] Circle native USDC contract on Base. Not a Lexica protocol contract.	Circle/Base identity evidence. Remove all LexicaVault claims tied to this address.
$0.0015 USDC toll	[ASSUMPTION] Published standard attestation price.	Approved pricing policy, rate version, customer terms, accounting rule, and reconciliation.
scripts/sweep_treasury.js	[ASSUMPTION] Candidate automated treasury operation artifact.	Source hash, review, scheduler, signer policy, logs, limits, and rollback evidence.
v6.0+ node federation	[ROADMAP] Proposed decentralized or distributed node federation.	Protocol specification, trust model, node identity, consistency model, governance, and exit plan.

II.4 Version Compatibility and Migration

- Every receipt shall carry protocol version, schema version, circuit identifier, canonicalization profile, policy hash, and cryptographic suite.
- A v5.2 record shall not be relabeled v5.4 without a signed migration manifest that preserves original bytes, signatures, timestamps, and settlement state.
- Unknown or deprecated policy, schema, or circuit versions shall fail closed for high-risk actions.
- Migration shall include verifier compatibility, proof regeneration policy, key rotation, contract transition, tenant notice, and rollback criteria.

Section III - Cryptographic Primitives and Multi-Tenant Zero-Knowledge Isolation

III.1 Security Objectives and Threat Model

Threat	Control objective	Failure condition	Verification
Record forgery	Only authorized tenant or workload keys can produce accepted signatures.	Invalid, expired, revoked, or wrong-tenant credentials are accepted.	Signature vectors, certificate-path test, revocation test, HSM evidence.
Record substitution	One canonical record maps to one digest and commitment under specified encoding.	Ambiguous encoding, field reduction, or parameter mismatch permits alternate opening.	Canonical encoding vectors, parser fuzzing, collision analysis.
Replay or rollback	Event identity, sequence, previous event, previous root, and epoch number remain monotonic.	Duplicate body mismatch, sequence rollback, expired receipt, or conflicting epoch is accepted.	Replay suite, contract invariants, conflicting-epoch test.
Cross-tenant access	One tenant cannot open, prove, debit, retrieve, or administer another tenant record.	Shared keys, namespaces, balances, operators, or queues cross boundaries.	Cross-tenant penetration tests and access-control proofs.
Metadata leakage	Public commitments disclose no raw payload and minimize tenant, time, and volume correlation.	Low-entropy guessing, repeated blind, public tenant ID, or public per-event settlement leaks context.	Low-entropy attack analysis, randomness tests, padding and disclosure tests.
Key compromise	Compromise impact is bounded by tenant, role, time, rate, and revocation controls.	Exportable master keys or indefinite credentials enable uncontrolled signing.	Key-boundary review, rotation, revocation, break-glass, and recovery test.
Proof-system failure	A proof establishes only the declared relation with named parameters and trusted components.	Paper claims zero knowledge without a defined relation or claims formal verification without artifacts.	Circuit audit, setup transcript, verifier key hash, known-answer and differential tests.

III.2 Authorization Chain Record

Field group	Minimum fields
Protocol	Protocol version; schema version; circuit ID; canonicalization profile; cryptographic suite.
Identity	Tenant pseudonym; workload identity; agent identity; service account; certificate reference; human authority.
AI system	Provider; model family and version; deployment ID; system-prompt digest; retrieval-set digest; tool-adapter version.
Action	Requested-action digest; target resource; purpose; data class; expected side effect.
Policy	Policy-bundle hash; rule ID; risk class; decision; reason code; override conditions.
Human control	Approver reference; scope; approval time; authentication method; separation-of-duties evidence.
Time	Client time; gateway time; epoch window; secure-clock status; maximum skew.
Continuity	Event sequence; previous event commitment; previous epoch root; idempotency identifier.
Privacy	Retention class; legal-hold flag; data-region code; encryption-key reference; disclosure class.
Cryptography	Record digest; Poseidon commitment; signature; certificate-chain reference; proof reference.
Settlement	Standard count; exception status; toll class; epoch ID; chain transaction reference.

III.3 Canonical Commitment Construction

Approved bounded wording

The construction is computationally binding under the specified SHA-256, Poseidon, signature, parameter, and

canonical-encoding assumptions. It is not "mathematically immutable."

```
d_i = SHA256(CanonicalEncode(A_i))
C_i = Poseidon(DST_leaf, Field(d_i), Field(b_i), Field(P_i), s_i)
sig_i = Sign_sk_t(SHA256(DST_acr || d_i || C_i || event_id_i))
L_i = Poseidon(DST_node, C_i, Field(SHA256(sig_i)))
R_e = MerkleRoot(L_1, ..., L_n)
E_e = SHA256(DST_epoch || tenant_pseudonym || e || R_e || R_(e-1) || n || P_e || V_e || t_open || t_close)
```

- The specification shall define byte encoding, field conversion, domain-separation constants, tree arity, padding, odd-leaf handling, empty-tree handling, hash parameters, and test vectors.
- Canonical CBOR or another deterministic typed binary schema shall be used. Ambiguous string concatenation is prohibited.

III.4 Tenant-Salted HMAC Nonces

Status

[DESIGN TARGET] Tenant-salted HMAC nonces are included as a v5.4 hardening mechanism. The source blueprint does not establish them as deployed.

```
nonce_i = HMAC-SHA256(K_nonce,t, DST_nonce || workload_id || tool_call_id || sequence_i || client_nonce)
```

- K_nonce,t shall be unique per tenant and separated from encryption and signing keys.
- The client nonce shall contain high entropy. Sequence and context binding shall prevent replay and cross-route reuse.
- The resulting nonce may contribute to event identity. It shall not replace signature authentication or high-entropy commitment blinding.
- Required tests: nonce uniqueness, tenant separation, rollback, duplicate-body mismatch, key rotation, failover, and deterministic recovery rules.

III.5 Poseidon Leaf Masking and Hiding Limits

Requirement	Approved position	Evidence
High-entropy blind	Fresh 256-bit blind from an approved random source. No blind reuse.	Randomness-source design, health tests, reuse detection, and incident procedure.
Tenant separation	Tenant-specific domain tags, keys, queues, storage, rate limits, and proof jobs.	Cross-tenant tests and namespace policy.
Low-entropy protection	Sensitive records remain encrypted off-chain. Commitments alone do not prevent guessing.	Dictionary and low-entropy attack analysis.
Public metadata	Use pseudonymous tenant identifiers, coarse or concealed time fields, no public per-event settlement, and optional batch padding.	Metadata leakage test and disclosure policy.
Public chain content	Publish commitments and settlement evidence, not raw enterprise payloads.	Chain-event schema and privacy review.

III.6 Bounded Plaintext Persistence Objective

Prohibited claim

Do not state "zero disk-leakage guarantee." State a bounded, testable component property instead.

Boundary	Design target	Failure condition	Test artifact
Stateless edge request tier	No plaintext AI payload is intentionally written to persistent local disk. Memory buffers are short-lived and process-scoped.	Crash dumps, swap, debug logs, temporary files, tracing, or queue payloads persist plaintext.	Disk and temp-file inspection, crash test, debug-mode test, log scan, configuration attestation.
Durable outbox and queue	Store minimized canonical data or encrypted evidence references.	Queue or DLQ contains unrestricted plaintext.	Payload schema review, encryption test, access test, DLQ audit.
Evidence store	Tenant-controlled encrypted evidence	Unencrypted data, shared keys,	Encryption, access, key-rotation,

Boundary	Design target	Failure condition	Test artifact
	with configurable retention and legal holds.	unauthorized access, or deletion outside policy.	retention, deletion, and legal-hold tests.
Backups and DR	Encrypted backups with documented region, key, retention, and restoration controls.	Backup exposes plaintext or restores without authorization and audit.	Backup scan, restore test, key-separation review.
Observability	No prompt, response, credential, secret, or raw sensitive field in logs by default.	Telemetry captures sensitive values.	Structured log allowlist, DLP scan, incident test.

III.7 Zero-Knowledge Relation

Category	Required definition
Public inputs	Commitment; policy-bundle hash; approved identity-registry root; risk class; decision code; circuit ID; epoch ID.
Private witness	Canonical record; blind; workload credential; identity inclusion path; sensitive policy inputs; human-approval credential where required.
Circuit assertions	Typed field constraints; approved workload membership; policy version equality; declared policy decision; required approval; sequence and epoch constraints; absence or digest-only representation of disallowed fields; consistency of hidden values.
Trusted outside circuit	Canonical parser, schema compiler, clock, credential issuance, policy compiler, and evidence encryption shall be explicitly listed.
Setup and lifecycle	Groth16 requires circuit-specific setup material, ceremony transcript, contribution verification, toxic-waste statement, proving-key hash, verifier-key hash, rotation, and deprecation rules.

III.8 Proof Obligations

Obligation	Formal claim	Core assumption	Required artifact
Commitment binding	An efficient adversary cannot open one commitment to two distinct valid records and blinds.	SHA-256 and Poseidon collision resistance; deterministic encoding; specified field conversion.	Parameter files, rationale, test vectors, cryptographic review.
Commitment hiding	Observing a commitment does not enable practical record recovery.	Fresh high-entropy blind, sufficient payload entropy, no reuse, controlled metadata.	Randomness tests, low-entropy analysis, privacy test.
Signature authenticity	An attacker without an authorized signing key cannot create an accepted signature.	EUF-CMA scheme security and secure key custody.	Certificates, HSM evidence, revocation and signature vectors.
Merkle inclusion soundness	No valid inclusion proof exists for a leaf outside the committed tree.	Tree-hash collision resistance and correct construction.	Open verifier, adversarial proofs, root reconstruction.
Append-only continuity	Each accepted epoch extends the previous accepted epoch.	Contract monotonicity and previous-root equality.	Contract property and conflicting-epoch tests.
Equivocation detectability	Two roots for one tenant and epoch produce detectable conflict.	Public events and independent monitoring.	Watcher, alert test, fork simulation.
Tenant isolation	One tenant cannot open, prove, debit, or retrieve another tenant record.	Domain, key, authorization, storage, queue, and contract separation.	Cross-tenant penetration and access-control tests.
Policy-decision correctness	Declared decision equals approved policy output over committed inputs.	Circuit and policy compiler correctness.	Circuit audit, reproducible compiler, known-answer and differential tests.
Settlement conservation	Epoch debit equals authenticated event counts under the approved toll schedule.	Correct arithmetic and authenticated batch counts.	Invariant test, reconciliation, overcharge simulation.
Anchor persistence	After declared finality, alteration violates the stated settlement assumptions.	Base, Ethereum, sequencer, data availability, contract, and governance assumptions.	Dependency statement, finality policy, chain verification procedure.

III.9 FIPS and Post-Quantum Transition

- A FIPS 140-3 claim requires the named validated module, certificate number, exact product, firmware, software version, approved mode, physical and logical boundary, and operating configuration.
- The paper shall use ML-KEM terminology. A production claim requires an exact hybrid TLS 1.3 profile, peer capability behavior, downgrade policy, telemetry, and fallback limits.
- [ROADMAP] v6.0+ shall include algorithm agility, dual-signature or hybrid-handshake transition rules, cryptographic inventory, re-anchoring or re-signing policy, and long-term verification strategy.

Section IV - The Nine-Layer Execution Spine and Exception Oracle Governance

High-risk routes fail closed. Low-risk degraded mode must be signed, time-bounded, visible, and later reconciled.

IV.1 Layer-by-Layer Drafting Matrix

Layer	Control objective	Mandatory implementation	Failure rule / evidence
1. Enterprise enforcement	Force covered AI actions through the protocol boundary.	Egress proxy, service mesh, API gateway, signed SDK policy, workload identity, destination allowlist, downstream receipt check.	High-risk routes fail closed. Evidence: network policy, gateway config, bypass tests, workload inventory.
2. Identity and authority	Bind action to tenant, workload, agent, service account, and human authority.	mTLS, short-lived credentials, SCIM, OAuth scopes, hardware-backed signing when required.	Invalid or missing identity blocks execution. Evidence: chain, IAM, key provenance, revocation, role map.
3. Canonicalization and minimization	Convert event into one deterministic typed record.	Versioned schema, canonical encoding, strict field order, normalization and minimization rules.	Invalid record enters quarantine and is never silently normalized. Evidence: vectors, redaction, parser fuzzing.

Layer	Control objective	Mandatory implementation	Failure rule / evidence
4. Policy decision	Apply the exact policy in force at decision time.	Versioned bundle, risk class, allow/deny/escalate, human approval and override rules.	Unknown policy fails closed. Evidence: policy hash, source commit, approval, tests.
5. Commitment and proof	Commit while hiding sensitive fields and prove required private predicates.	High-entropy blind, Poseidon commitment, encrypted evidence, defined ZK proof relation.	Mandatory proof failure blocks settlement and execution. Evidence: circuit, parameters, key hashes, transcript, audit.
6. Durable edge outbox	Accept without putting on-chain settlement in the request path.	Idempotent append, queue, retries, DLQ, acknowledgment receipt.	No provisional receipt before durable append. Evidence: queue config, loss and idempotency tests.
7. Exception Oracle	Quarantine and govern malformed, drifted, or policy-conflicting records.	Original digest, proposed repair, rule version, reviewer, replay result, resolution code.	Oracle cannot silently rewrite or approve its own exception. Evidence: manifest, repair diff, reviewer signature.
8. Epoch and settlement	Build append-only tenant roots and anchor the epoch.	Tenant accumulator, previous-root chain, fixed epoch ID, leaf count, Base anchor.	Conflicting or non-monotonic epochs rejected. Evidence: proofs, manifest, event, receipt, verifier.
9. Evidence and assurance	Produce legally useful and reproducible evidence.	Signed archive, PDF index, proofs, policies, certificates, retention and legal-hold metadata, verifier.	Incomplete packages are marked INCOMPLETE, never compliant. Evidence: schema, audit, custodian declaration, reproducibility record.

IV.2 Two-Sided Enforcement Boundary

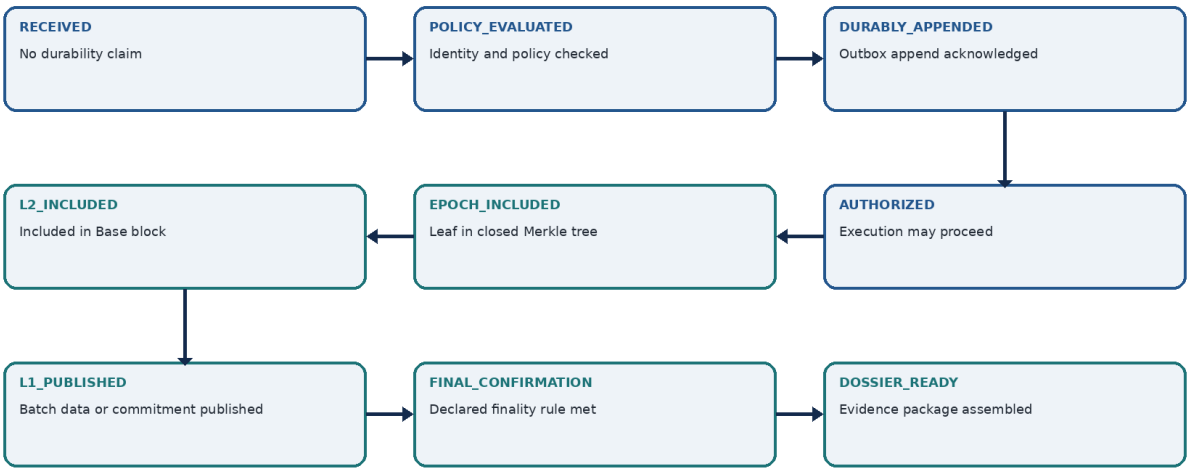
1. Block all covered destinations except through approved gateways.
2. Require workload identity and an approved policy version at the gateway.
3. Issue a signed authorization receipt only after durable append succeeds.
4. Require every covered downstream tool to reject requests without a valid receipt.
5. Detect and alert on alternate ledger history, unsigned calls, policy substitution, and uncovered routes.

Bounded non-bypassability

For covered workloads and destinations inside the declared trust boundary, no execution is accepted without a valid authorization receipt under an approved policy. Any alternate history or bypass is rejected or produces independently detectable evidence. This is bounded, not absolute.

IV.3 Receipt State Machine

Receipt and Settlement State Machine



No API response may state final anchoring while the event is only pending epoch inclusion.

State	Meaning	Permitted claim
RECEIVED	Gateway received request.	No durability, authorization, or anchoring claim.
POLICY_EVALUATED	Identity and policy checks completed.	Decision computed under identified policy version.
DURABLY_APPENDED	Canonical record entered durable outbox.	Provisional evidence durability inside declared outbox SLO.
AUTHORIZED	Execution may proceed.	Valid provisional authorization receipt exists.
QUARANTINED	Execution held for exception review.	No approval or repair unless governance closes the exception.
EPOCH_INCLUDED	Leaf is in a closed Merkle tree.	Merkle inclusion proof exists. No chain-inclusion claim yet.
L2_INCLUDED	Epoch commitment is in a Base block.	L2 inclusion under stated confirmation count.
L1_PUBLISHED	Relevant batch data or commitment has been published to Ethereum.	Publication evidence under Base assumptions.
FINAL_CONFIRMATION	Declared finality rule is met.	Anchored settlement receipt may be issued.
DOSSIER_READY	All required evidence artifacts assembled.	Dossier may be released if completeness and signature checks pass.

IV.4 Durable Outbox and Cloudflare Boundary

- ctx.waitUntil() may trigger optional analytics or export work. It shall not be the sole durability mechanism for compliance evidence.
- Required sequence: canonicalize; evaluate policy; append to durable outbox; receive idempotent acknowledgment; return provisional receipt; queue batching, proof generation, settlement, and dossier work.
- Queue consumers shall be idempotent because delivery can repeat. Dead-letter recovery, ordering assumptions, retries, and data-loss tests shall be documented.

IV.5 Exception Oracle Governance

```
X_i = (d_original, d_proposed, rule_version, reason, reviewer, decision, t_opened, t_resolved, replay_result)
repaired_event.prev_event = original_event.event_id
```

Governance rule	Mandatory control
Original preservation	No database update overwrites the original record, digest, receipt, or proof state.
Repair as new record	Every repaired record is a new linked event with its own identity, policy, signature, toll, and settlement state.
Segregation of duties	Oracle proposer, reviewer, approver, and production rule publisher are separated for high-risk mutations.
No self-approval	The Oracle service cannot approve its own exception or silently mutate an approved rule.
Appeal and dispute	Tenant dispute, review status, evidence hash, hold, and final resolution remain visible.
Replay validation	A repaired record must replay deterministically and document whether execution was prevented, repeated, reversed, or compensated.
Exception economics	Incremental surcharge, support cost, proof cost, refund, and dispute treatment are reconcilable.

IV.6 FIDO2 / WebAuthn Multi-Signature Rule Mutations

Status

[DESIGN TARGET] The source blueprint requires hardware-backed signing and segregation of duties. This framework specifies FIDO2/WebAuthn as the preferred human-authentication mechanism for high-risk rule mutations. It is not asserted as deployed.

Mutation class	Approval threshold	Authentication and evidence
Routine low-risk policy metadata	One policy owner plus automated validation.	WebAuthn user-presence assertion; signed change request; tests; policy hash.
High-risk allow/deny or approval rule	2-of-3: policy owner, security owner, business-risk owner.	Phishing-resistant WebAuthn; independent sessions; signed diff; test evidence; effective time; rollback plan.
Cryptographic parameter or circuit change	3-of-5: chief cryptographer, CISO delegate, protocol owner, external reviewer, release manager.	Hardware-backed WebAuthn or HSM-backed signatures; parameter hashes; audit; verifier compatibility; timelock.
Treasury cap, signer, or withdrawal change	3-of-5 with CFO and security participation.	WebAuthn plus treasury multisig; transaction simulation; limits; legal and accounting review; timelock.
Emergency pause	2-of-3 emergency quorum, with after-action review.	Hardware-backed approval; reason code; scope; expiry; immutable event; board notification threshold.
Unpause or emergency override	Higher threshold than pause.	Root-cause closure; independent test; legal and security approvals; tenant notice where required.

IV.7 Failure Semantics and Disaster Recovery

Failure	High-risk action	Low-risk action	Required evidence
Identity or policy unavailable	Fail closed.	Signed degraded mode only if pre-approved and time-bounded.	Outage receipt, scope, expiry, reconciliation.
Durable outbox unavailable	Fail closed.	Do not issue authorization receipt.	Loss test and recovery event.
Proof service backlog	Block proof-mandatory execution or reduce admission.	Provisional state only within approved SLO.	Backlog metrics, scaling action, degraded-mode record.
Base or RPC outage	Continue provisional receipts only within approved maximum delay.	Batch locally and anchor when service returns.	Outage chronology, root continuity, re-anchor verification.
HSM or signer failure	Block affected tenant or role.	Use approved redundant signer only within declared boundary.	Failover test, signer provenance, revocation.
Region loss	Fail over to isolated region with preserved sequence and keys.	No split-brain epoch closure.	DR test, root continuity, data restoration, RTO/RPO.
Evidence store unavailable	Execution policy determines fail-closed or degraded behavior.	No dossier claim until artifacts are complete.	Completeness status and recovery evidence.

Section V - Economic Tolling Matrix and Automated Treasury Operations

V.1 Toll Definitions

Item	Framework value	Status / limitation
Standard attestation	0.0015 USDC per accepted standard control event.	[ASSUMPTION] Public price. Contract and accounting enforcement require proof.
Exception surcharge	0.0075 USDC incremental surcharge in addition to the standard toll.	[DESIGN DECISION] This framework adopts the stronger incremental interpretation. Change requires synchronized contract, API, invoice, and white paper.
Enterprise vault fee	4,800 per month or per epoch is unresolved in the source.	[BLOCKER] Final paper must choose one unit and state included services.
On-chain settlement	One aggregate debit per tenant epoch.	No per-event on-chain charge. Internal accounting remains signed and reconcilable.
Gas submission target	<= 0.00015 USDC per event at the target batch and data profile.	[DESIGN TARGET] Gas cap alone does not guarantee margin. Remaining all-in COGS must fit inside the residual cost budget.

V.2 Revenue and Margin Formulas

```
R = N_s * p_s + N_x * (p_s + p_x)
R = N * (p_s + q * p_x)
For N = 10,000, p_s = 0.0015, p_x = 0.0075: R = 15 + 75q
C_epoch = F_epoch + G_epoch + N * (c_edge + c_queue + c_storage + c_hsm + c_proof + c_rpc + c_monitor + c_support + c_loss)
Gross margin = 1 - C_epoch / R_epoch
For an 85% floor: C_epoch <= 0.15 * R_epoch
At 10,000 all-standard events: R = 15; total all-in C_epoch <= 2.25; all-in cost/event <= 0.000225 USDC
```

Cost allocation consequence

If Base submission cost is capped at 0.00015 USDC per event, only 0.000075 USDC per event remains for edge processing, queue, storage, HSM, proof generation, RPC, monitoring, support, and reserves in an all-standard 10,000-event epoch. Therefore, the gas target is necessary but not sufficient for an 85% all-in margin floor.

V.3 Tolling Matrix

Exception rate	Epoch revenue at 10,000 events	Maximum all-in cost at 85% margin	Control consequence
0%	15.00 USDC	2.25 USDC	Lowest cost budget. Batch efficiency and low support load are critical.
1%	15.75 USDC	2.3625 USDC	Minor additional proof and review capacity.
5%	18.75 USDC	2.8125 USDC	Exception operations, support, and prover capacity require explicit allocation.
10%	22.50 USDC	3.3750 USDC	Surcharge must cover incremental exception cost and reserve.
25%	33.75 USDC	5.0625 USDC	Potential exception storm. Admission and pricing circuit breakers likely activate.
100%	90.00 USDC	13.50 USDC	Not a normal operating state. Treat as failure or incident scenario, not ordinary margin upside.

V.4 Economic Circuit Breakers

Condition	Required action	Authority and evidence
Projected margin below 85%	Increase batch size; delay non-critical anchor within disclosed limits; use approved reserve; apply disclosed price adjustment; or stop accepting work.	CFO-approved policy, cost inputs, decision log, tenant notice if pricing changes.
Gas exceeds epoch cap	Hold routine settlement within maximum delay. Use an accelerated premium path for critical events.	Gas oracle sources, cap calculation, settlement class, exception approval.
Proof backlog exceeds SLO	Reduce admission, scale prover capacity, or enter declared degraded mode.	Queue depth, SLO, capacity action, risk owner.
Tenant balance below reserve	Notify tenant, restrict costly exceptions, invoke approved auto-funding or settlement-cap rules.	Balance proof, notice, spending cap, authorization.
USDC depeg or restriction	Pause new deposits and settlement movement; preserve accounting; use documented contingency rail.	Price and transfer trigger, legal review, reconciliation, resumption gate.
Base outage	Continue signed provisional receipts only within approved delay; anchor when service returns.	Outage record, local roots, continuity test, final receipt.
Cost data unavailable	Use conservative assumptions and do not claim the margin floor.	Data-quality flag and CFO acceptance.

V.5 Epoch Closure and Settlement Classes

```
CloseEpoch iff N >= 10,000 OR elapsed_time >= 24 hours OR critical_event OR legal_hold_trigger
```

Class	Use	Maximum anchor delay	Required handling
Routine	Normal low-risk attestations.	24 hours.	Batch for efficiency; disclose provisional state.
Elevated	High-risk action, exception approval, or financial side effect.	1 hour or lower approved target.	Smaller batch or priority settlement; stronger approval.
Critical	Security incident, materiality escalation, policy override, legal hold, or high-value financial action.	Immediate dedicated epoch, subject to chain availability.	Independent alert, priority verification, incident and legal workflow.

V.6 Automated Treasury Operations

> **Approved wording**
>
> Use "scheduled treasury sweeper job" or "automated treasury settlement service." Do not use "stealth sweeper." Every movement shall be visible in signed logs, contract events, wallet records, reconciliation, and approval evidence.

Control	Requirement
Scheduler	24-hour maximum sweep cadence for routine balances, plus event-driven critical settlement where approved.
Signer boundary	Dedicated HSM or multisig key. No application worker key may withdraw or sweep unrestricted funds.
Limits	Per-tenant spending cap; global daily cap; destination allowlist; expiry; minimum balance; maximum sweep; emergency pause.
Separation of duties	Code deployer, scheduler operator, signer approver, reconciler, and dispute approver shall be separated.
Observability	Every attempt records job ID, source, destination, amount, rate, tenant allocation, epoch, signer, policy hash, transaction, success, failure, and retry.
Reconciliation	Daily wallet-to-contract-to-internal-ledger reconciliation. Differences force freeze and investigation.
Failure handling	Idempotent transaction construction, nonce policy, replacement policy, duplicate protection, rollback prohibition, and alerting.
Source artifact	scripts/sweep_treasury.js requires a published source hash, dependency lock, security review, signer interface, runbook, and test evidence before it is cited as deployed.
Custody position	Preferred initial design is non-custodial: customer retains ownership and grants capped, expiring settlement permission; unused funds remain withdrawable.

V.7 LexicaVault.sol Minimum Contract Design

```
depositUSDC(amount)
authorizeSettlement(tenantId, spendingCap, validUntil)
settleEpoch(tenantId, epochId, root, previousRoot, standardCount, exceptionCount, grossTollUSDC,
policySetHash, circuitSetHash, manifestHash)
withdrawUSDC(amount, recipient)
disputeEpoch(tenantId, epochId, evidenceHash)
pauseTenant(tenantId)
```

- Contract invariants: monotonic epochs; previous-root continuity; exact toll arithmetic; spending caps; expiry; sufficient balance; role separation; pause; withdrawal delay for disputed funds; replay prevention; reentrancy protection; explicit upgrade governance; event emission for every state change.
- Publication package: Base chain ID 8453; actual contract address; deployment transaction; compiler and optimization settings; verified source; ABI; bytecode hash; proxy and admin; multisig signers; timelock; emergency powers; audit; known findings; property tests; verification instructions.

V.8 Stress Model and Reserve Allocation

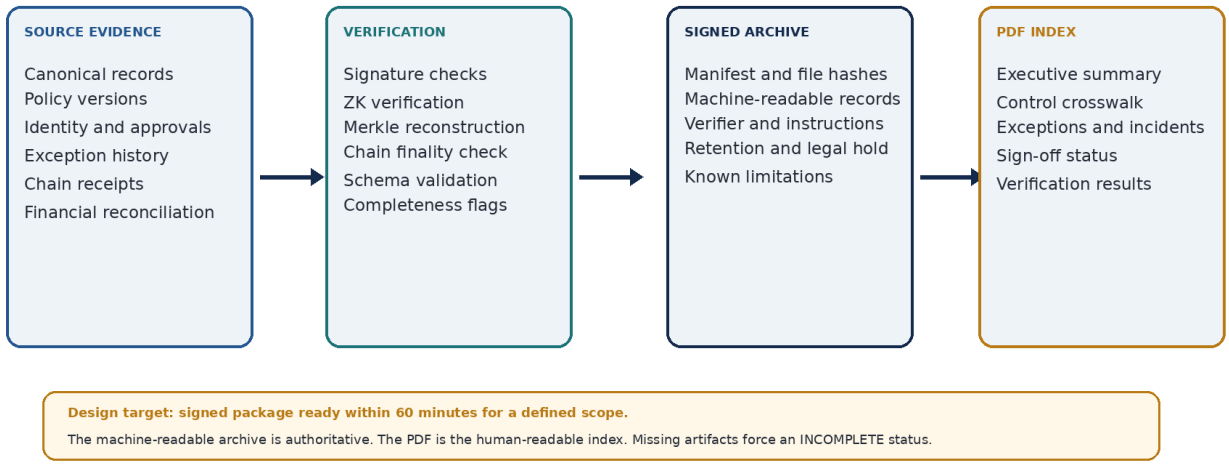
Scenario	Required analysis	Reserve consequence
Low volume	Cost when epoch closes after 24 hours with far fewer than 10,000 events.	Fixed-cost and gas reserve; pricing or minimum commitment.
Gas spike	Margin and delay under extreme L1 and L2 fees.	Settlement reserve and accelerated-path budget.
Exception storm	Prover, support, review, and surcharge economics.	Incident staffing and proof-capacity reserve.
Customer concentration	Impact if largest tenant leaves, defaults, disputes, or pauses.	Liquidity and credit reserve; concentration limits.
USDC or custody event	Depeg, blacklist, wallet compromise, chain, or counterparty contingency.	Treasury, legal, and customer-restitution reserve.
Security incident	Key compromise, evidence loss, fraud, or settlement error.	Security-incident and legal reserve; forensic and notification budget.

```
Expected Loss = sum over scenarios (probability_j * financial_loss_j)
```

- Report expected loss, uninsured expected loss, stress loss, liquidity requirement, legal reserve, security-incident reserve, treasury reserve, and customer-credit reserve.

Section VI - Statutory Evidence Support and Compliance Dossier Generation

Compliance Dossier Generation Model



VI.1 Dossier Positioning

Core rule

The dossier is an evidence package, not only a generated PDF. The authoritative output is a signed machine-readable archive. The PDF is a human-readable index. An incomplete package is marked INCOMPLETE and shall not be labeled compliant.

Sub-60-minute design target

[DESIGN TARGET] For a defined tenant, system scope, and reporting period whose required evidence is already available, the signed archive and PDF index should be generated within 60 minutes. The SLO excludes missing customer evidence, legal review, external provider delays, chain outages, and remediation of failed verification.

VI.2 Required Dossier Components

Component	Contents
Manifest	Dossier ID; tenant; period; protocol and schema versions; file list; file hashes; signer; generation time; completeness status.
Executive summary	Scope; systems; event counts; exceptions; incidents; unresolved items; limitations; sign-off status.
System inventory	Models; providers; deployments; agents; tools; owners; risk classes; jurisdictions.
Role analysis	Provider; deployer; importer; distributor; product manufacturer; controller; processor; service-provider roles as applicable.
Policy inventory	Policy versions; approvals; effective periods; test results; policy hashes; override history.
Event evidence	Canonical records or authorized redacted records; signatures; commitments; continuity links.
ZK evidence	Proofs; public inputs; circuit IDs; proving-key and verifier-key hashes; verification results.
Merkle evidence	Leaves; paths; tenant roots; global root; prior root; root reconstruction.

Component	Contents
Chain evidence	Chain ID; actual Lexica contract; transaction; block; event log; finality status; independent RPC verification.
Identity evidence	Workload certificates; SCIM mapping; OAuth scopes; HSM references; revocations; WebAuthn or human approvals.
Exception evidence	Original digest; repair proposal; rule version; reviewer; approval; replay; surcharge; dispute.
Financial evidence	Event counts; rates; gross toll; refunds; disputes; vault debit; sweeps; reconciliation.
Incident evidence	Detection; classification; materiality process; notifications; remediation; closure.
Retention evidence	Retention class; legal hold; deletion status; jurisdiction; evidence custodian.
Assurance evidence	Audits; penetration tests; control tests; availability; DR; known findings.
Limitations	Missing records; unsupported routes; degraded periods; third-party failures; assumptions.
Verifier	Open-source or escrowed tool, version, source hash, deterministic instructions, expected outputs.

VI.3 Compliance Control Map

Legal or control area	Lexica evidence contribution	Residual customer duty
EU AI Act Article 9	Risk decision, policy version, test result, exception, mitigation, approval, and monitoring evidence.	Design, operate, review, and update the full risk-management system.
EU AI Act Article 12	Automatic event record, identity, time, decision, action, context reference, and continuity.	Determine required logging scope and preserve sufficient underlying context.
EU AI Act Article 17	Policy and QMS linkage, approvals, monitoring, exception handling, incident and accountability evidence.	Maintain the broader documented quality management system.
SEC incident disclosure	Detection chronology, system scope, action trail, investigation evidence, and materiality inputs.	Make and document materiality determinations and required filings.
Canadian evidence rules	Authentication, system integrity, business-process evidence, and reproducible verification.	Establish admissibility and foundation in the proceeding.
eIDAS electronic ledgers	Integrity and chronology evidence.	Determine whether qualified status is needed and engage qualified services if required.
Privacy and data protection	Minimization, encryption, access history, purpose and retention metadata.	Legal basis, notices, rights, transfers, processor governance, and impact assessment.
Financial controls	Signed counts, rate application, vault debit, sweep, and reconciliation.	Accounting treatment, tax, reserves, approvals, and financial-statement controls.

VI.4 Retention and Legal Hold

- Do not use one universal 6-24 month retention statement. Retention depends on role, data class, jurisdiction, contract, incident, legal hold, and specific statutory duties.
- Article 19 provider logs for certain high-risk systems may require at least six months unless other law provides otherwise. Article 18 documentation duties may extend longer. The final paper shall map the applicable role and record type.
- Commitments may remain on a public chain while underlying evidence stays tenant-controlled, encrypted, region-scoped, and subject to legal hold and deletion policy.
- Every deletion shall preserve a signed deletion record, policy basis, custodian, time, key-destruction evidence where applicable, and unresolved-hold check.

VI.5 Evidentiary Positioning

Approved statement

Lexica records are designed to support authentication, integrity, chronological reconstruction, and independent verification. Their legal effect and admissibility remain subject to applicable law, procedural rules, evidence foundations, and judicial or regulatory determination.

- Preserve evidence about how the record was created, how the clock was maintained, how keys were controlled, how data was stored, how outages were handled, how integrity was tested, and who can explain the system under oath.
- A Base anchor does not automatically become a qualified electronic ledger under eIDAS.

VI.6 Dossier SLO and Completeness Rules

Stage	Target	Stop condition
Evidence collection	All indexed artifacts located and hash-checked.	Missing required source, unsupported route, unresolved legal hold, or failed access.
Cryptographic verification	Signatures, proofs, Merkle paths, roots, and chain states verified.	Any mismatch, unknown parameter, revoked key, or inconsistent root.
Control crosswalk	Each required control mapped to evidence, limitation, and owner.	Unmapped obligation or unsupported legal statement.
Archive signing	Manifest and archive signed by authorized dossier key.	Signer unavailable, key revoked, or manifest mismatch.
PDF rendering	Human-readable index generated from verified manifest.	PDF differs from manifest or omits limitations.
Release	Dossier status COMPLETE or INCOMPLETE with reasons.	No release under a false compliant label.

Appendix A - Master Drafting Matrix

Section	Exact required subsections	Mandatory content	Proof / artifact	Approval outcome
I	Abstract; purpose; liability squeeze; duty map; evidence gap; outcome; limits; residual risk.	Separate exposure categories. State Lexica supports controls and evidence but grants no immunity.	EU AI Act role map; SEC disclosure map; contract-risk example; residual-risk table; legal memorandum.	GC accepts framing; CFO accepts exposure; CISO accepts objective.
II	Genesis; prototype; testnet; pilot; adversarial test; cryptographic readiness; controlled mainnet; sovereign deployment; federation roadmap.	Use dates only with evidence. Define entry and exit criteria. Explain migration.	Commits; tags; deployments; audits; incidents; benchmarks; ceremony; migration plan.	Reviewers can distinguish deployed facts from targets.
III	Threat model; record; suite; commitment; encryption; signature; ZK; setup; Merkle; tenant separation; key lifecycle; PQC; proof obligations.	Define every primitive and parameter. State public/private data, trusted components, leakage, setup risk, key compromise.	Definitions; proof sketches; vectors; circuit and verifier; setup transcript; certificates; rotation and tenant tests.	Chief Cryptographer and CISO approve security model.
IV	Enforcement; identity; canonicalization; policy; proof; outbox; Oracle; epoch; evidence; receipts; failure; DR.	Fail closed for high risk. Signed degraded mode for approved low risk. No silent repair. Define approvals and replay.	Diagrams; bypass; Oracle matrix; queue test; DR test; SLO report.	CISO accepts bounded non-bypassability and recovery; auditor accepts traceability.
V	Tolls; revenue; cost; margin; epoch; gas; contract; balances; treasury; reconciliation; depeg; dispute; tax and accounting.	Resolve exception pricing and enterprise fee. Include all COGS. Explain custody and licensing assumptions.	Model; scenarios; contract invariants; gas simulations; reconciliation; legal memo; reserve policy.	CFO accepts economics and treasury exposure.
VI	EU AI Act; SEC; evidence law; privacy; retention; hold; exports; verification; limits; customer duty; counsel review.	Replace safe harbor with statutory and evidentiary support. Map control, duty, limitation, and role.	Article matrix; evidence; retention; privacy; Canada evidence; eIDAS; sample dossier.	GC and external auditor approve claims and reproducibility.

Appendix B - Independent Assurance Gates

Gate	Required result	Blocking evidence
Threat-model review	All boundaries, attackers, dependencies, failure paths, and out-of-scope routes documented.	Signed review and unresolved finding register.
Cryptographic review	Commitment, ZK circuit, setup, signatures, parameters, key lifecycle, and verifier assessed.	Independent report, parameter hashes, test vectors.
Smart-contract audit	Settlement, access, upgrades, disputes, arithmetic, pause, and emergency paths tested.	Audit, findings, remediation, property tests.
Penetration test	Tenant isolation, gateway bypass, identity abuse, API abuse, and evidence access tested.	Report, scope, retest, exceptions.
Queue and loss test	Termination, duplicate delivery, reordering, retry exhaustion, DLQ recovery, and idempotency tested.	Test data, measured loss, recovery proof.
Disaster-recovery test	HSM failure, region loss, Base outage, RPC outage, and evidence-store restoration tested.	RTO/RPO results, key and root continuity.
Privacy assessment	Inventory, legal basis, retention, deletion, access, and transfers reviewed.	PIA/DPIA, data maps, processor terms.
Financial-control review	Balances, caps, counts, refunds, sweeps, disputes, and reconciliations tested.	Control report, reconciliation samples, reserve policy.
Regulatory-claims review	Every legal statement tied to authority and counsel interpretation.	Citations, role analysis, jurisdiction matrix.
Dossier reproducibility	Independent party verifies package without Lexica interface.	Verifier run log, expected and actual output, exception record.

Appendix C - Publication Execution Sequence

6. Remove the false Lexica contract reference to the Circle USDC address.
7. Deploy and verify the real LexicaVault.sol or remove all claims that it exists.
8. Freeze the Authorization Chain Record schema and canonical encoding.
9. Define the exact zero-knowledge relation and trusted components.
10. Publish cryptographic parameters, domain tags, field conversion, and test vectors.
11. Complete the Groth16 ceremony or select a proof system with an approved lifecycle.
12. Replace waitUntil durability claims with a durable outbox and queue.
13. Implement the formal receipt and settlement state machine.
14. Decide whether the exception charge is total or incremental.
15. Resolve whether the enterprise fee is monthly or per epoch.
16. Build the complete all-in cost model and automatic margin circuit breakers.
17. Implement an observable, access-controlled scheduled treasury sweeper.
18. Design the non-custodial vault structure and obtain Canadian and EU payment-regulatory opinions.
19. Replace safe-harbor language across website, contracts, sales materials, and API responses.
20. Correct the EU AI Act penalty and role-classification model.
21. Rewrite the SolarWinds discussion and separate it from individual-criminal-exposure examples.
22. Add tenant-controlled encrypted evidence retention, legal hold, deletion, and restore controls.
23. Publish named FIPS certificates and exact operational boundaries before making FIPS claims.
24. Commission cryptographic, contract, penetration, privacy, financial-control, and legal reviews.
25. Generate one complete sample dossier and require independent reproduction without the dashboard.
26. Publish v5.4 only after every failed verification step is closed or expressly disclosed as residual risk.

Appendix D - Required Artifact Register

Artifact class	Required artifacts
Protocol source	Repository URL or escrow location; release tag; source commit; dependency lock; build instructions; source hashes.
Deployment	Environment; date; region; Cloudflare configuration; endpoint; worker version; queue; outbox; evidence store; release manifest.
Contracts	Real address; chain ID; deployment transaction; source verification; ABI; bytecode; proxy; admin; multisig; timelock; audit; findings.
Cryptography	Suite registry; parameters; curves and fields; domain tags; circuit; compiler; setup transcript; proving and verifier keys; test vectors.
Keys and identity	HSM or KMS product; certificate; firmware; approved mode; key generation; backup; rotation; revocation; WebAuthn policy; break glass.
Security	Threat model; pen test; bypass test; cross-tenant test; parser fuzzing; log leakage scan; queue loss; DR; incident runbooks.
Economics	Rate policy; cost spreadsheet; gas simulation; batch model; reserve policy; stress scenarios; reconciliation; dispute and refund samples.
Legal and privacy	Role map; authority crosswalk; legal claim memo; retention schedule; legal-hold procedure; privacy assessment; processor terms; licensing opinions.
Dossier	Manifest schema; sample archive; PDF index; verifier; verification log; custodian declaration; completeness and limitation register.

Appendix E - Authority and Source Register

The attached blueprint identifies the following primary authorities and technical sources. Final publication shall verify current text, applicability, and citation format before release.

EU AI Act, Regulation (EU) 2024/1689: https://eur-lex.europa.eu/eli/reg/2024/1689/oj/eng

SEC cybersecurity disclosure rules and related release: https://www.sec.gov/newsroom/press-releases/2023-139

US DOJ - former Uber security chief case summary: https://www.justice.gov/usao-ndca/pr/former-chief-security-officer-uber-sentenced-three-years-probation-covering-data

Base transaction finality: https://docs.base.org/base-chain/network-information/transaction-finality

Cloudflare Workers context.waitUntil: https://developers.cloudflare.com/workers/runtime-apis/context/

Cloudflare Queues: https://developers.cloudflare.com/queues/

Base chain connection and chain ID: https://docs.base.org/base-chain/quickstart/connecting-to-base

Poseidon technical paper: https://www.usenix.org/system/files/sec21-grassi.pdf

Groth16 paper: https://eprint.iacr.org/2016/260

NIST CMVP: https://csrc.nist.gov/projects/cryptographic-module-validation-program

NIST post-quantum FIPS announcement: https://csrc.nist.gov/news/2024/postquantum-cryptography-fips-approved

Base network fees: https://docs.base.org/base-chain/network-information/network-fees

FINTRAC money services business guidance: https://fintrac-canafe.canada.ca/msb-esm/msb-eng

MiCA, Regulation (EU) 2023/1114: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX%3A32023R1114

Canada Evidence Act: https://laws-lois.justice.gc.ca/eng/acts/c-5/page-3.html

eIDAS consolidated text: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX%3A02014R0910-20241018

Appendix F - Final CISO, CFO, and General Counsel Questions

Role	Non-negotiable questions
CISO	Can covered actions bypass the gateway? Can keys be exported? Can one tenant access another? Can Lexica rewrite history? What fails closed? What remains available during Base, HSM, queue, region, and evidence-store failures?
CFO	Is every cost included? What happens below 10,000 events? Is 0.00015 gas compatible with total 0.000225 cost? Who owns USDC? Can Lexica move excess funds? What reserves support disputes, outages, depegging, incidents, and customer concentration?
General Counsel	Are provider and deployer roles correct? Are penalty statements precise? Are safe-harbor claims removed? Is evidence preserved for holds? Are retention periods role-specific? Does the payment model create registration or licensing duties?
Auditor	Can counts, roots, signatures, policy versions, proof results, receipts, and settlement amounts be independently reproduced from the archive?
Board	Which risks are reduced? Which remain? Who owns each residual risk? What threshold requires escalation, funding, pause, disclosure analysis, or customer notice?

Controlled Closing Statement

Final permitted promise

Lexica Ledger Protocol does not eliminate enterprise responsibility. It is designed to make covered decisions attributable, policy-bound, tamper-evident, economically reconcilable, and independently verifiable within a declared technical and legal scope.

Approval condition

This framework is ready for architecture drafting and budget planning. It is not ready for an external claim of v5.4 deployment, full compliance, safe harbor, formal verification, zero leakage, or guaranteed margin until the artifact and assurance gates in this document are closed.

Own the evidence standard. Require every enterprise, vendor, insurer, auditor, and regulator to verify the record without trusting marketing claims.