ManChine AI Technology LLC

GOVERNANCE • INTEGRITY • HUMANITY

REA-01

RUNTIME EXECUTION AUTHORITY

PUBLISHED ARCHITECTURE SPECIFICATION — VERSION 1.6

STATUS

PUBLISHED — FROZEN ARCHITECTURE BASELINE FOR STANDARDS DEVELOPMENT

AUTHOR

Richard R. Colimon

NORMATIVE FOUNDATION

RGF-01 — Runtime Governance Foundations
RGV-01 v2.3 — Runtime Governance Vocabulary

SEQUENCING POSITION

REA-01 stabilizes the authority contract before RGE-01 — Runtime Governance Evaluation — is finalized.

RiCo

Runtime Integrity Control

PUBLICATION DATE: 08/19/2026

BUILDING TRUST IN CONSEQUENTIAL AI

Review Note

Version 1.6 applies a targeted architectural correction pass following adversarial review of Version 1.5. This version is published as the frozen architecture baseline against which RGE-01 may proceed; publication does not expand REA-01 into full normative prose, and conversion to a mature normative specification remains future work under Section 24. It establishes that the governance basis applicable to a given authority-relevant determination — governing policy, criterion, threshold, authority mapping, evidence requirement, or precedence rule — remains traceably attributable to what was actually in force at the time of that determination and is not retroactively redefined by a later governance change; requires that a change to an authority-relevant governance mechanism itself receive authority-impact assessment where it could alter the legitimacy, scope, admissibility, continuation, reassessment obligation, or execution treatment of an existing or in-flight authority relationship; and adds the minimum traceability requirement necessary to reconstruct authority-relevant temporal ordering where ambiguity among event occurrence, observation, determination, effective transition, and execution could change the governance result. Evaluation mechanics, consequence enforcement, domain-specific thresholds, and implementation mechanisms remain assigned to RGE-01, REB-01, applicable governing or behavioral specifications, and implementation guidance as appropriate. No prior architectural decision is silently reversed; the focused changes are recorded at the end of this document.

1. Purpose and Normative Role

REA-01 specifies the lifecycle and validity conditions of Runtime Execution Authority: the bounded authority under which execution may legitimately begin, continue, change, be constrained, be suspended, be restored, be revoked, or cease under an orderly withdrawal or replacement.

REA-01 defines the authority contract. It does not prescribe a specific runtime product, implementation mechanism, measurement system, policy engine, evidence engine, or execution interceptor.

REA-01 is intended to provide a stable normative object against which RGE-01 can later evaluate governance conditions. RGE-01 therefore evaluates whether relevant governance conditions satisfy the authority contract; it does not create authority merely by evaluating it.

Relationship to RGV-01's Authority and Legitimacy.

REA-01 does not redefine, rename, or replace RGV-01's Authority or Legitimacy. “Runtime Execution Authority” is REA-01's lifecycle-tracked representation of the Authority relevant to consequential execution: its source, scope, limits, dependencies, transitions, and continuing availability as part of the governance basis. REA-01 records authority-relevant conditions that may contribute to later evaluation of Legitimacy, but REA-01 does not determine, own, or represent the complete Legitimacy condition. Under RGV-01, Legitimacy depends on currently valid Authority together with applicable Authorization, Evidence, Policy, and Context. Evaluation of that complete governance basis remains outside REA-01's authority-layer responsibility.

Where a REA-01 lifecycle condition changes what was granted — for example, Establishment, Constraint, Revocation, Expiry, Withdrawal, or Replacement — it operates on Authority itself. Where a REA-01 lifecycle condition changes whether currently-granted Authority may presently be relied upon without altering the grant — for example, Suspension and Restoration — it tracks Legitimacy as RGV-01 defines it. Section 4 preserves this distinction explicitly and is the normative resolution of the Authority/Legitimacy ontology question raised in external architecture review of Version 1.2.

2. Scope

- Establishment and provenance of Runtime Execution Authority.
- Scope, limits, duration, identity, delegation, and transfer of authority.
- Maintenance and continuity of authority while execution and surrounding conditions change.
- Authority-relevant evidence requirements without absorbing general evidence evaluation.
- Constraint, intervention, suspension, restoration, revocation, expiry, withdrawal, replacement, and decommissioning.
- Authority behavior during in-flight execution, partial failure, concurrency, uncertainty, and delayed evidence.
- Required authority-state and transition records for traceability and later evaluation.

3. Architectural Boundaries

Component	Primary responsibility	REA-01 boundary
RGV-01	Canonical vocabulary	REA-01 SHALL use published vocabulary consistently and SHALL NOT silently redefine canonical terms.
RGF-01	Foundational runtime-governance principles	REA-01 specializes the authority lifecycle introduced by the foundations.
REA-01	Authority contract and authority-state transitions	Defines when authority exists, remains valid, narrows, pauses, resumes, ends, or is transferred.
RGE-01	Runtime Governance Evaluation	Evaluates governance conditions relevant to authority and other governance objects; it does not originate authority.

REB-01	Execution-boundary behavior	Applies or enforces execution-boundary consequences defined by the architecture; it does not define the source of authority.
RiCo	Runtime Integrity Control implementation/reference architecture	Performs Runtime Integrity Control and may consume or interact with authority, evaluation, and execution-boundary state governed by REA-01, RGE-01, and REB-01. RiCo does not absorb those specifications' normative responsibilities merely because a RiCo implementation is deployed.

Connective relationship among REA-01, RGE-01, RGV-01 Admissibility, and REB-01.

These responsibilities are functionally connected, but they do not constitute a single universal normative pipeline and must not collapse into a single undifferentiated evaluation or control step. REA-01 defines the authority contract — the conditions under which Runtime Execution Authority exists and remains valid. RGE-01 evaluates whether those conditions, and other applicable governance conditions, are presently satisfied. RGV-01 defines Admissibility as a governance determination, made at a defined decision point, as to whether execution is presently permissible. REB-01 enforces an Admissibility determination at the execution boundary, permitting or denying consequential execution from proceeding. Whether, when, and under what procedure a subsequent Admissibility determination occurs remains the responsibility of the applicable governing or behavioral specification.

REA-01 defines conditions; RGE-01 evaluates them; the evaluation output supports an Admissibility determination; REB-01 enforces the consequence of that determination. Precisely which component or process is responsible for formally making or representing the Admissibility determination itself is a question for RGE-01 to resolve — REA-01 does not assign that responsibility here, and RGE-01 SHALL NOT be treated as originating authority merely because it performs this evaluation, consistent with the boundary table above.

4. Authority Lifecycle Model

The lifecycle model is a conceptual bridge, not a claim that every implementation must expose identical internal states. Normative conformance is based on externally meaningful authority conditions and transitions. Version 1.3 separates durable states and properties from the transitions and events that produce them, and distinguishes conditions that operate on the Authority grant itself from conditions that track the continuing Legitimacy of an existing grant's exercise, consistent with Section 1.

4.1 Grant-Level Conditions (operate on Authority itself)

Durable states and properties:

- **Granted:** Authority exists, for a bounded subject, scope, purpose, duration, and context, from an identifiable and valid source. Entered via the Establishment transition.
- **Constrained:** a property that may apply to a Granted authority whose permissible scope or action set has been narrowed. Constrained is not a state exclusive of Granted/Active status but a modifier on it — an authority may be simultaneously Active and Constrained. See 4.3.
- **Revoked (terminal):** Authority is permanently withdrawn.
- **Expired (terminal):** Authority ceases because a defined temporal or event-bound limit is reached.
- **Withdrawn / Replaced (terminal for the retiring arrangement):** A governing component or authority arrangement is intentionally removed or superseded without erasing the historical record.

Transitions and events that produce these states: Establishment, imposition of a Constraint, Revocation, occurrence of Expiry, Withdrawal, and Replacement.

4.2 Authority-Reliance Conditions (track present availability of an existing grant for reliance)

Durable states:

- **Active: currently-granted Authority is presently available for reliance under REA-01's authority-side conditions. Active status does not by itself establish the complete RGV-01 Legitimacy condition.**
- **Suspended:** currently-granted Authority is temporarily not relied upon; continued execution cannot be justified by the suspended authority alone.
- **Indeterminate: whether the authority-side conditions required for currently-granted Authority to remain available for reliance cannot presently be confirmed. Indeterminate is distinct from Suspended: Suspended is an affirmative act; Indeterminate is an epistemic gap. Indeterminate authority must not silently resolve into Active status. See Section 15 and Section 16 for the governed handling of indeterminate conditions.**

Transitions and events: Suspension (imposition) and Restoration — an affirmative transition returning suspended authority to Active status only after required conditions are affirmatively confirmed current. Restoration is a transition, not a durable state.

4.3 Note on Terminology

This structure resolves two issues identified in external architecture review of Version 1.2. First, “Restored” was previously listed as though it were a durable state coextensive with Active and Suspended; it is a transition into Active status, not a state an authority remains in. Second, whether “Constrained” is a state or a modifier was previously undefined; Version 1.3 treats it as an orthogonal modifier on Granted/Active status rather than a mutually exclusive peer state. Both corrections are non-normative clarifications of the conceptual model; they do not change any Version 1.2 architectural decision.

5. Establishing Authority

- The source of authority must be identifiable and attributable.
- The source must itself possess sufficient standing to grant the claimed authority.
- The authorized subject or execution actor must be identifiable at the level required by the governed action.
- Scope, purpose, permitted action class, relevant resource or system boundary, and applicable temporal conditions must be bounded.
- Authority must not be inferred solely from technical capability, possession of credentials, system access, prior execution, or absence of objection.
- Where establishment depends on external conditions, the dependency and its validity horizon must be represented.
- **Accountable root.** The chain of authority SHALL terminate at an identifiable, accountable source external to the technical governance architecture itself — for example, a natural person, legal entity, contractual arrangement, or applicable regulatory or organizational body, depending on the governing context. A technical or governance component SHALL NOT be its own source of standing. REA-01 does not require that every authority system share the same legal or organizational root structure; it requires only that the chain terminate outside the technical architecture rather than regress indefinitely within it.

6. Delegation and Authority Chains

- Delegated authority cannot exceed the delegator's valid authority.
- Delegation must preserve provenance from the originating authority through each delegation edge.
- Sub-delegation must be explicitly permitted or prohibited; silence must not automatically imply permission to sub-delegate.
- Expiry, revocation, suspension, or material constraint of an upstream authority must propagate to dependent delegated authority as required by the dependency.
- Conflicting delegations, overlapping scopes, and multiple concurrent authorities require deterministic resolution or escalation rules.
- Delegation must distinguish transfer, sharing, representation, and technical execution on behalf of another authority holder.
- **Agentic and tool-mediated delegation.** Where a tool invocation, sub-agent spawning, or automated delegation step meets the definition of delegation set out above — a transfer or extension of authority to act to another actor or component — the requirements of this section apply to it. This does not assert that every tool call or agent action necessarily constitutes a new legal or governance delegation; whether a given automated step meets that definition is determined by the applicable governing or behavioral specification and the specific architecture, not settled generically by REA-01.
- **Aggregate delegation.** The aggregate scope of authority delegated from a given authority, considered across all concurrent delegations, is a review item requiring resolution before normative drafting (Section 22). REA-01 does not yet establish a normative bound on aggregate delegated scope.

7. Maintaining Authority

Authority is not a one-time permission token. Maintenance concerns whether the authority-side conditions necessary for continued reliance on the established Authority remain sufficiently intact during execution. REA-01 does not treat satisfaction of these authority-side conditions as establishing the complete RGV-01 Legitimacy condition.

- **Technical identity continuity:** the credentials, service identity, or technical principal exercising authority remain attributable to the authorized actor, or to a validly delegated successor.
- **Accountable-principal continuity:** the human, organization, or other accountable party ultimately responsible for the exercise of authority has not changed in a way that breaks the basis on which authority was established, independent of whether technical identity markers changed. Technical identity continuity and accountable-principal continuity are distinct conditions; satisfying one does not establish the other.
- **Scope continuity:** the action remains inside the authorized boundary.
- **Purpose continuity:** the execution has not materially changed into a different governed purpose.
- **Temporal continuity:** the authority has not expired and required review intervals have not lapsed.
- **Context continuity:** material environmental or organizational conditions have not invalidated the basis of authority.
- **Dependency continuity:** upstream authority, required evidence, and required governance services remain available or have an explicitly governed degraded mode.

8. Runtime Evidence and Authority

REA-01 addresses evidence only to the extent necessary to support authority establishment, maintenance, transition, and cessation. General evidence qualification, admissibility analysis, weighting, contradiction resolution, and broader governance evaluation remain responsibilities of the appropriate evaluation/evidence specifications.

- An authority state must not be represented as current when the evidence required to support that state is known to be stale beyond an allowed validity horizon.
- Evidence latency must not be silently treated as affirmative evidence of continuity.
- Evidence failure must be distinguishable from evidence of failure.
- Where contradictory authority-relevant evidence exists, the architecture must define whether authority is constrained, suspended, escalated, or held pending evaluation.
- Historical authority evidence must remain attributable to the state and time at which it supported a determination. Preservation or historical verifiability of that evidence does not, by itself, establish its current applicability, continuing Authority, or continuing Legitimacy after material conditions have changed.
- **Late and corrected evidence.** Consistent with RGV-01's treatment of Admissibility as non-retroactive, evidence that arrives after an authority-relevant determination, or evidence later shown to have been incorrect, does not retroactively alter that determination. It may bear on subsequent authority state and may trigger a required review, but it does not rewrite the historical record of what was determined at the time.

9. Authority Continuity and Material Change

Operational continuity does not by itself establish authority continuity. A system may remain technically capable of acting after the conditions supporting legitimate authority have changed.

- Material changes in identity, scope, purpose, environment, policy, dependency, resource, target, risk, or governing context require authority-impact assessment.
- Governed materiality. The architecture must not depend on an implementation making an ad hoc judgment that a change is "material." The applicable governing or behavioral specification must establish the criteria, decision rule, or accountable procedure by which a change becomes authority-relevant enough to require assessment, revalidation, constraint, suspension, or another defined response. REA-01 does not prescribe a universal quantitative threshold.
- Cumulative and trajectory-based change. A sequence of individually non-material changes must be assessable for cumulative effect where their combined trajectory could alter the conditions on which authority was established or is presently relied upon. Repeated sub-threshold change must not provide a path for authority drift that would have been treated as material if introduced as a single change.
- Governance-basis continuity. The governing policy, specification, criterion, threshold, authority mapping, evidence requirement, precedence rule, or other governance basis applicable to a given authority-relevant determination is the basis actually in force at the time that determination is made or is required to be made. A subsequent change to that governance basis does not retroactively redefine, reclassify, or rewrite the basis of a determination already made, consistent with the non-retroactivity principle in Section 8. This does not freeze governance bases or prevent a legitimately governed change from applying to determinations made after its effective time; it requires only that the basis applicable to a given determination remain traceably attributable to what was actually in force when that determination occurred.
- Governance of governance changes. A change to an authority-relevant governance mechanism — including a change to materiality criteria, authority mappings, thresholds, evidence requirements, precedence rules, or another governance basis addressed by this section — is itself subject to authority-impact assessment under this section where the change could alter the legitimacy, scope, admissibility, continuation, reassessment obligation, or execution treatment of an existing or in-flight authority relationship. Governance must not be bypassed merely by changing the rules that determine when governance is required.
- A material change must not inherit prior authority automatically unless the authority contract explicitly permits that class of change.
- In-flight execution must be treated separately from future execution: a loss or narrowing of authority may require completion, containment, rollback, safe-stop, handoff, or prohibition depending on the governed action.
- Irreversible actions require explicit treatment because revocation after consequence formation cannot retroactively undo the consequence.
- Scope drift must be detectable as a potential authority-continuity failure rather than merely as an operational deviation.
- **Material behavioral and system change.** Material change includes change to the executing system itself — including model updates, fine-tuning, changed tools, changed retrieval sources, changed memory, or changed configuration — that could plausibly affect the conditions supporting authority, regardless of whether a formal identity or version marker changed. Technical identity continuity (Section 7) is necessary but not sufficient to establish authority continuity where such material behavioral change has occurred.

10. Constraint and Intervention

Constraint narrows authority without necessarily eliminating it. Intervention is an authority-governed action taken in response to a condition that may affect execution or authority state.

- A constraint must identify what remains authorized and what no longer is.
- Intervention authority must itself be attributable and bounded; the ability to intervene does not arise merely because a governance component detects a problem.

- Emergency or protective intervention must identify its legal/organizational source, scope, duration, and post-event review requirement.
- An intervention must not silently convert into permanent authority.
- Authority-relevant refusal or withdrawal. Where a valid refusal, withdrawal of consent, veto, or equivalent governed input changes the authority basis, the resulting authority condition must have a defined effect on what execution remains authorized. Recording the refusal without representing its authority-side effect is insufficient where the refusal is itself authority-relevant. Whether and how that effect is enforced at the execution boundary belongs to REB-01 and the applicable governing or behavioral specification.
- Temporary protective or emergency authority — including the case where continuing execution lacks ordinary authority but stopping execution would itself cause unacceptable harm — is addressed further in Section 17.

11. Suspension

- Suspension is temporary withholding of authority, not deletion of its history. Suspension is the imposition transition into the Suspended exercise-validity state (Section 4.2).
- The suspension trigger, effective time, affected scope, responsible authority, and treatment of in-flight actions must be recorded.
- Execution that continues during suspension must rely on some other valid authority or a separately defined safe-state obligation; the suspended authority cannot be cited as its basis.
- Suspension may be total or scoped, but ambiguity must not default to the broader permission.

12. Restoration

- Restoration is an affirmative transition into Active status (Section 4.2), not the automatic disappearance of a suspension condition.
- The restoring authority must have standing to restore the affected authority.
- Restoration must confirm that relevant conditions are current at restoration time rather than merely reusing pre-suspension evidence.
- Where execution context changed during suspension, restoration may require a new establishment or re-authorization rather than simple reinstatement.

13. Revocation, Expiry, and Cessation

- Revocation permanently withdraws authority under the affected authority record.
- Expiry ends authority when a predefined temporal or event-bound condition is reached.
- Cessation must identify the effective boundary after which new execution cannot rely on the ended authority.
- Historical execution performed while authority was valid remains part of the record; later revocation must not rewrite history.
- Downstream delegated authority must be evaluated for propagation effects when upstream authority ends.
- **Revocation during in-flight execution.** Revocation during in-flight execution requires distinguishing what has actually been withdrawn: new authority-dependent determinations after the effective revocation time are always precluded; consequences already formed by execution that has already occurred are not retroactively undone; the historical authority record showing that authority was valid when relied upon is not rewritten; and whether the remaining, not-yet-executed steps of an in-flight action may complete, must halt, require containment, or require safe-stop depends on the governed action's own treatment under Section 9 and the applicable behavioral specification, not on revocation alone.
- **Rollback and compensation.** Operational reversal, rollback, or compensation of an action's effects does not erase or rewrite the historical authority or governance record, and does not retroactively change whether the action was authorized when it was performed.

14. Replacement, Withdrawal, and Decommissioning

Removal of a governance service, RiCo implementation, or other component is not equivalent to erasing prior governance. REA-01 must define the authority-side requirements for an orderly cessation or transfer of governance responsibility while leaving product-specific uninstall procedures to implementation documentation. Component replacement — where a successor component or arrangement assumes the same responsibility without interruption — is distinguished below from withdrawal of the underlying governance responsibility, where no successor assumes it; the authority-continuity consequences of these two cases differ, per Section 4 and Section 15.

- Architectural requirement: establish a defined cessation point after which the retiring component no longer performs its assigned governance or verification responsibility.
- Implementation examples may include revoking or transferring credentials, API permissions, keys, service identities, delegated roles, and other technical capabilities. These are deployment mechanisms, not REA-01's normative authority architecture.
- Disconnect or reassign authority-relevant measurement and evidence inputs without falsely representing the loss of observation as proof of continued validity.
- Remove or bypass execution hooks/interceptors introduced for the retiring component only after responsibility for the affected execution paths has been explicitly confirmed or transferred. This requirement does not presume the retiring component itself held execution-boundary control: under RGV-01, execution-boundary control is REB's responsibility, not RiCo's, and

decommissioning of a RiCo implementation SHALL NOT be treated as “returning” control it never legitimately held. Where the retiring component did legitimately implement REB or another control-bearing responsibility, this step confirms transfer of that responsibility to its successor or to the organization's designated architecture.

- Architectural requirement: preserve access to governance records and evidence that applicable retention, accountability, or organizational requirements require to survive the transition. Export mechanics belong to implementation guidance.
- Preserve historical records and provenance with integrity, accurate attribution, and retention consistent with applicable requirements; decommissioning must not create the appearance that the prior governance state never existed.
- Verify that no hidden dependency on the retired component remains in authority chains, execution paths, credentials, evidence collection, or restoration logic.
- Record the exact time, scope, and responsible authority at which the retiring component's governance responsibility ceased.
- Distinguish withdrawal without replacement from transfer to a successor, because the authority-continuity consequences are different: withdrawal without replacement leaves the governance responsibility unfulfilled and must be assessed against Section 9 and any applicable governance requirement; transfer to a successor requires continuity of the evidence and authority record across the handoff.
- Where decommissioning affects in-flight execution, the treatment in Section 15 applies; decommissioning SHALL NOT proceed in a manner that silently leaves in-flight, authority-dependent execution without a defined authority basis.

15. Concurrency, Conflict, and In-Flight Execution

- Multiple authorities may exist concurrently only where their scopes and precedence are determinable.
- Conflicting authority claims must not be resolved by whichever component acts first.
- A transition occurring during an in-flight action must have a defined effect on that action and on subsequent actions. Loss, suspension, expiry, revocation, or material narrowing of an authority basis must not be bypassed merely by routing unfinished or subsequent authority-dependent execution through a queue, retry, recovery path, alternate route, delegated actor, replica, failover mechanism, or functionally equivalent execution path. The enforcement mechanism for this invariant belongs to REB-01, applicable behavioral specifications, and implementation.
- Atomic, reversible, long-running, distributed, and irreversible actions may require different authority-transition behavior.
- Authority-relevant temporal ordering. Where ambiguity among event occurrence time, observation time, determination time, effective transition time, or execution time could change the governance result — including which authority condition applied, whether a determination preceded or followed a material change, or whether an in-flight action crossed a consequence boundary before or after a transition took effect — the applicable architecture must be able to reconstruct the ordering actually relied upon. This does not require every authority-relevant event to carry every such timestamp; it requires that ordering-sensitive determinations remain traceable to the ordering that was actually used to make them.
- Consequence boundary and intervention window. For an in-flight action that can become practically irreversible, the applicable architecture must identify the authority-relevant point or condition after which a pending consequence can no longer be meaningfully altered by an authorized intervention. Preserving authority does not require every formed consequence to remain reversible; it requires that any authority-dependent right or standing to intervene be evaluated while intervention can still affect what remains changeable.
- Closure of an intervention window must not be used to manufacture authority by inertia. Once the remaining consequence is no longer changeable, the historical record must preserve which authority condition applied while intervention was still possible and when the relevant consequence boundary was crossed.
- A system must not claim authority continuity merely because stopping would be operationally inconvenient.
- **Distributed disagreement.** Distributed components may hold differing views of current authority state due to stale caches, propagation delay, network partition, or asynchronous evidence delivery. REA-01 requires that this class of disagreement be addressed architecturally; it does not prescribe a specific consensus, replication, or synchronization mechanism.
- **Indeterminacy from disagreement.** Where a component cannot presently confirm current authority state with the confidence the applicable governance requirement demands — including due to delayed revocation propagation or partition — that condition is Indeterminate (Section 4.2), not a silent continuation of ordinary Active authority.
- **Resolving indeterminacy.** Indeterminate authority must be resolved through an explicitly governed failure/degraded-mode rule (Section 16), which may legitimately result in safe-stop, constrained continuation, protective action, or another established behavior appropriate to the governed action. REA-01 does not mandate a single universal resolution and does not treat the more restrictive available option as automatically required.

16. Failure and Degraded Modes

- Loss of a governance component, evidence source, identity provider, policy source, or communication path must have a defined authority effect.
- Fail-open behavior must never be assumed as a default authority rule.
- Fail-closed behavior may also create unacceptable consequences; where a safe degraded mode exists, its authority basis must be explicit.
- Recovery from a degraded mode must include authority-state reconciliation before normal operation resumes.

- The governed handling of Indeterminate authority (Section 4.2, Section 15) is an instance of this section's requirement that loss of a governance component, evidence source, identity provider, policy source, or communication path have a defined authority effect; it must be resolved by an explicit rule, not left to default behavior.

17. Temporary Protective / Emergency Action — Open Architectural Question

Some conditions require action, or require withholding action, before an ordinary authority determination can be completed — including cases where continuing execution lacks ordinary authority but stopping execution would itself cause unacceptable harm. REA-01 addresses the authority basis for this case at the architecture level. How such action is technically executed, and the engineering of safe states, fail-open/fail-closed behavior, and containment mechanisms, is a matter for REB-01, applicable behavioral specifications, and safety engineering practice, not REA-01.

- The mature architecture must determine whether protective or emergency action relies on pre-established contingency Authority, special Authorization, a domain-defined degraded-mode rule, another already-defined governance basis, or a genuinely distinct authority construct. REA-01 does not yet establish a new canonical Authority category for this scenario.
- Any governance basis used to justify protective or emergency action must be attributable to an identifiable source with standing; the ability to detect a problem does not by itself confer authority to act on it (Section 10).
- Any protective or emergency basis that permits exceptional action must be bounded in scope and duration according to the applicable governing specification.
- Exceptional protective or emergency treatment must not silently become an ordinary or permanent authority basis; continuation beyond its defined bound requires the governance basis applicable to ordinary execution.
- Whether protective or emergency invocation requires mandatory post-event accountability review, and which specification establishes that requirement, remains open for normative resolution; any resulting record requirement should align with Section 19.
- REA-01 does not define specific safety mechanisms, fail-open/fail-closed defaults, or containment engineering; it defines the authority basis and accountability boundary within which such mechanisms, wherever defined, must operate.

18. Trust Assumptions and Governance-System Integrity Boundaries

REA-01 does not provide security guarantees and does not attempt to solve cybersecurity. Its authority model presupposes the integrity of the authority record, the identity sources it relies upon, and the evidence sources it references; compromise of any of these is a security failure outside REA-01's scope, addressed by applicable security specifications and organizational practice, not by REA-01.

- REA-01 requires that the authority record (Section 19) be traceable and attributable in a manner sufficient to make unauthorized alteration, forgery, or compromise of authority-relevant records detectable upon review, even though REA-01 cannot prevent such compromise.
- REA-01 does not require, and does not itself define, specific cryptographic, access-control, or infrastructure-security mechanisms. Where such mechanisms are needed to satisfy this section's traceability requirement, they are a matter for implementation and applicable security specifications.

19. Authority Record and Traceability Requirements

At minimum, an authority record or equivalent traceable representation should be capable of preserving:

- Authority identifier and version/state.
- Source and provenance.
- Authorized subject/actor.
- Scope, purpose, target/resource, and relevant action class.
- Temporal validity and review horizon.
- Delegation chain and dependency references.
- Authority-relevant evidence references.
- Current state and state-transition history.
- Constraint, suspension, restoration, revocation, expiry, replacement, or withdrawal events.
- Responsible authority for each transition.
- Effective time of each transition and treatment of in-flight execution.
- Material-change assessment reference, including the governing criterion or accountable procedure used when a change required authority-side reassessment.
- Where applicable, cumulative-change or authority-drift assessment sufficient to show why a sequence of changes did or did not cross a governed materiality boundary.
- Where applicable, the authority-relevant intervention window or consequence-boundary event and the authority condition in effect when that boundary was crossed.
- Governance-basis reference sufficient to identify the governing policy, criterion, threshold, mapping, or other governance basis actually applicable to each authority-relevant determination, including its state at the time of that determination.
- Where ordering among event occurrence, observation, determination, effective transition, or execution could affect the governance result, sufficient timing information to reconstruct that ordering.

- Successor or handoff reference where governance responsibility is transferred.
- **Execution linkage.** Where the applicable architecture generates them, a reference sufficient to link the authority record to the corresponding Governance Event(s) or Governance Receipt (RGV-01 Section 4.4) associated with the execution the authority record governed.

20. Conformance Structure

The mature specification should separate normative requirements from explanatory rationale and examples. Conformance should test externally meaningful authority behavior, not mandate a specific internal software design.

- Establishment conformance.
- Delegation-chain conformance.
- Continuity/material-change conformance.
- Governed-materiality and cumulative-change conformance.
- Authority-relevant refusal/withdrawal effect conformance.
- Intervention-window/consequence-boundary conformance for in-flight irreversible actions.
- Governance-basis continuity and reflexive governance-change conformance.
- Authority-relevant temporal-ordering reconstruction conformance.
- Constraint/suspension/restoration/revocation conformance.
- Evidence-staleness and evidence-loss behavior.
- In-flight transition behavior.
- Decommissioning/handoff conformance.
- Traceability and historical-record preservation.

21. Terminology Notes (Non-Normative)

The following terms are used by REA-01 in a specific architectural sense that may differ from usage in adjacent fields. These notes exist to prevent accidental semantic import from other domains; they do not redefine or attempt to govern the meaning of these terms outside REA-01.

- **Authority.** Used here as defined by RGV-01 (a legitimate basis under which execution is permitted), not as used in identity and access management or public-key infrastructure (for example, “Certificate Authority”).
- **Revocation / Suspension.** Used here as authority-lifecycle conditions (Section 4), not as references to certificate-revocation mechanisms such as CRLs or OCSP, which are implementation techniques that may or may not be used to realize these conditions.
- **Delegation.** Used here as a governance-authority concept (Section 6), related to but not necessarily coextensive with OAuth-style delegated authorization or IAM delegated administration.
- **Material Change.** Used here as an authority-continuity concept (Section 9), not as a term of art from contract or transactional law (for example, “material adverse change”).
- **Protective / Emergency Action. Section 17 uses this phrase for an unresolved architectural scenario requiring a valid governance basis for exceptional protective or emergency action. REA-01 does not establish “Emergency Authority” as a canonical Authority category. The phrase must not be read as a term from safety engineering (for example, emergency stop or safety interlock) or legal emergency-powers doctrine.**

22. Additional Authority Conditions Identified for Future Resolution

The following conditions were identified during external architecture review as requiring resolution before normative drafting. They are recorded here as review-surface items rather than resolved, and remain open for resolution during subsequent normative drafting.

- **Succession.** Authority-holder succession (for example, organizational restructuring, merger, or contractual novation), distinct from component replacement (Section 14) and from delegation (Section 6).
- **Renewal / Extension.** Whether renewal of temporal authority is a distinct transition preserving provenance, or a new Establishment; not yet resolved.
- **Expansion.** The inverse of Constraint (Section 4.1): whether and how authority scope may legitimately grow without a full new Establishment.
- **Joint / Shared Authority.** Authority genuinely held jointly by multiple parties (for example, dual-control requirements), distinct from the concurrent-but-independent authorities addressed in Section 15.
- **Orphaned Authority.** Delegated authority whose upstream source has become unreachable or ceased to exist, distinct from ordinary expiry or revocation.
- **Aggregate Delegation.** Whether and how the aggregate scope of concurrent delegations from a single authority should be bounded (Section 6).

These items are carried forward into Section 23.

23. Open Questions for External Technical Review

1. Does REA-01 correctly sit before RGE-01 as the specification that defines the authority contract RGE later evaluates, and does Section 3's connective-relationship statement correctly allocate responsibility for formally making the Admissibility determination to RGE-01 rather than presuming it?
2. Where, if anywhere, does REA-01 still allow itself to absorb responsibilities that properly belong to RGE-01, REB-01, evidence specifications, security specifications, or implementation documentation?
3. Does the Section 1 / Section 4 treatment of Runtime Execution Authority as a lifecycle/record-keeping layer over RGV-01's Authority and Legitimacy — rather than a new primitive — correctly avoid silently redefining canonical RGV-01 terms?
4. Is the Section 4.1 / 4.2 split between grant-level conditions and exercise-validity conditions the correct division, or does it require further refinement before becoming normative?
5. What is the correct authority behavior when required evidence becomes unavailable but there is no affirmative evidence that authority has failed — that is, what specifically resolves an Indeterminate condition (Section 4.2, Section 15, Section 16)?
6. How should REA-01 distinguish authority loss affecting new actions from authority loss occurring during an irreversible or safety-critical in-flight action, beyond the general treatment in Section 9 and Section 13?
7. What propagation rules are required for nested delegation when upstream authority is constrained, suspended, expired, or revoked?
8. Should decommissioning be normative in REA-01, or should REA-01 define only cessation/handoff requirements while implementation standards define uninstall mechanics?
9. What minimum record is necessary to prove when governance responsibility transferred or ceased, and is the Section 19 Governance Event/Receipt linkage sufficient?
10. How should each item in Section 22 (succession, renewal/extension, expansion, joint/shared authority, orphaned authority, aggregate delegation) be resolved, and does resolving them require new lifecycle states, or can they be expressed using the Section 4 model as structured?
11. Does the Section 17 Temporary Protective / Emergency Authority treatment remain correctly bounded to authority and accountability, without drifting into safety-engineering normative territory?
12. What minimum architectural requirement should govern materiality criteria so that two conforming implementations observing the same relevant state cannot silently apply incompatible authority-continuity assumptions, while still allowing domain-specific thresholds?
13. How should cumulative sub-threshold changes be represented and evaluated so that authority drift cannot occur through a sequence of individually non-material changes?
14. When refusal, withdrawal, or another human/governing input is authority-relevant, what minimum authority-side effect must be represented before REB-01 enforcement is considered, and which details properly belong outside REA-01?
15. For irreversible or progressively irreversible execution, what minimum information must define the intervention window or consequence boundary without turning REA-01 into a safety-engineering or execution-control specification?
16. Which additional adversarial cases should be resolved before normative prose is finalized?

24. Proposed Development Sequence

1. Reconcile all REA-01 terminology against published RGV-01 v2.3.
2. Review RGF-01 foundations for any authority assumptions that REA-01 must specialize or preserve.
3. Resolve, with RGE-01, which component or process formally makes or represents the Admissibility determination described in Section 3.
4. Resolve each item in Section 22 before Section 4 is finalized as normative.
5. Build an issue/decision register for every unresolved authority transition and boundary question.
6. Pressure-test establishment, delegation, continuity, constraint, suspension, restoration, revocation, expiry, replacement, and decommissioning.
7. Run targeted adversarial tests for governed materiality, cumulative authority drift, authority-relevant refusal effect, and intervention-window closure before irreversible consequence formation.
8. Resolve cross-specification boundaries with RGE-01 and REB-01 before final normative drafting.
9. Convert accepted decisions into numbered normative requirements using SHALL/SHALL NOT/SHOULD/MAY discipline.
10. Add non-normative examples, state-transition tables, diagrams, and adversarial scenarios only after the normative model is stable.
11. Run independent technical review, reconcile findings, then determine publication readiness.

Architectural Position

REA-01 is the normative authority-layer specification of the Runtime Governance Standards Family. It defines the conditions and transitions by which Runtime Execution Authority is established, bounded, maintained, changed, suspended, restored, ended, transferred, or withdrawn. Runtime Execution Authority is REA-01's lifecycle-tracked representation of the Authority relevant to consequential execution, including its source, scope, limits, dependencies, transitions, and continuing availability for reliance. It is not a new governance primitive and does not own, determine, or represent the complete RGV-01 Legitimacy condition. RGV-01 supplies canonical vocabulary; RGF-01 supplies foundational principles; RGE-01 evaluates governance conditions against the authority contract and supports the Admissibility determination that REB-01 enforces; REB-01 addresses execution-boundary behavior; and RiCo performs Runtime Integrity Control while interacting with outputs and state governed by those specifications without absorbing their

normative responsibilities or becoming their normative source. This document is published as the frozen architecture-level specification: Version 1.6 incorporates the focused architecture corrections and stress-test hardening identified through successive external and adversarial review passes, and establishes the stable architecture baseline against which RGE-01 and subsequent behavioral specifications may proceed, prior to eventual conversion into mature normative prose.

Change Log — Version 1.2 to Version 1.3

What changed

- Added an explicit statement of the relationship between RGV-01's Authority/Legitimacy and REA-01's Runtime Execution Authority (Section 1), using the narrowest formulation supported by published RGV-01 v2.3 text: Runtime Execution Authority is a lifecycle-tracked representation of execution-relevant Authority, not a new primitive and not a renaming of Authority or Legitimacy.
- Restructured Section 4 into grant-level conditions (4.1: Granted, Constrained, Revoked, Expired, Withdrawn/Replaced — operating on Authority itself) and exercise-validity conditions (4.2: Active, Suspended, Indeterminate — tracking Legitimacy of an existing grant), separating durable states from transitions/events. Restored is now explicitly a transition into Active status, not a peer state. Constrained is now explicitly an orthogonal modifier, not a mutually exclusive state.
- Added an explicit connective-relationship statement in Section 3 linking REA-01's authority contract, RGE-01's evaluation, RGV-01's Admissibility determination, and REB-01's enforcement, while explicitly leaving which component formally makes the Admissibility determination to RGE-01 to resolve.
- Added an Indeterminate exercise-validity condition (Section 4.2), distinct from Suspended, addressing uncertainty (including distributed disagreement, stale state, propagation delay, and partition, Section 15) without automatically equating it with Suspension and without adopting a universal "more restrictive state" default — resolution is deferred to an explicitly governed failure/degraded-mode rule (Section 16), preserving safe-stop, constrained continuation, protective action, or other legitimately established behavior.
- Added an accountable-root/authority-chain termination principle (Section 5) preventing a technical component from being its own source of standing, without prescribing a single universal root structure.
- Added Temporary Protective / Emergency Authority as a new, bounded architectural category (Section 17), with standing, scope/duration bounds, non-conversion into permanent authority, and mandatory post-event review, while explicitly excluding safety-engineering mechanism design from REA-01's scope.
- Added Trust Assumptions and Governance-System Integrity Boundaries (Section 18), stating REA-01's reliance on the integrity of the authority record, identity sources, and evidence sources, and requiring traceability sufficient to make compromise detectable, without claiming to prevent it.
- Split technical identity continuity from accountable-principal continuity (Section 7), and connected material behavioral/system change — model updates, fine-tuning, changed tools, retrieval, memory, or configuration — to the existing material-change trigger (Section 9) regardless of formal version markers.
- Added a late/corrected-evidence non-retroactivity principle (Section 8), mirroring RGV-01's Admissibility non-retroactivity without implying evidence can rewrite a historical determination.
- Added an explicit enumeration of what is and is not withdrawn by revocation during in-flight execution, and a rollback/compensation non-retroactivity principle (Section 13).
- Corrected Section 14 decommissioning language: replaced "immutable historical records" with preservation centered on integrity, attribution, and applicable retention; removed the assumption that a retiring RiCo implementation necessarily held execution-boundary control (explicitly reserved to REB under RGV-01); replaced "making new authority-dependent runtime determinations" with function-neutral language; and cross-referenced in-flight execution treatment (Section 15).
- Added agentic/tool/sub-agent delegation binding to the existing delegation model (Section 6), explicitly without asserting every tool call constitutes a new legal or governance delegation, and flagged aggregate delegation scope as an unresolved review item rather than adding a normative bound.
- Added Terminology Notes (Section 21, non-normative) flagging Authority, Revocation/Suspension, Delegation, Material Change, and Emergency Authority as terms with distinct meanings in IAM, PKI, OAuth, contract law, and safety engineering.
- Added Additional Authority Conditions Identified for Future Resolution (Section 22): succession, renewal/extension, expansion, joint/shared authority, and orphaned authority, carried into the updated Open Questions (Section 23).
- Extended the authority record (Section 19) to permit linkage to the corresponding Governance Event(s) or Governance Receipt where RGV-01 Section 4.4 records exist for the governed execution.
- Updated Section 23 Open Questions and Section 24 Proposed Development Sequence to reflect the above and to keep unresolved items visible rather than silently deciding them.
- Updated version references, Review Note, and Architectural Position to Version 1.3; document status remains Architecture Review Draft.

Findings deliberately not incorporated, and why

- The adversarial review's proposed universal "default to the more restrictive state" fallback for distributed disagreement was not adopted. Per explicit instruction, Version 1.3 instead requires that indeterminacy not silently resolve into continued authority

and that resolution follow an explicitly governed failure/degraded-mode rule, preserving safe-stop, constrained continuation, or protective action as legitimate outcomes rather than mandating one universal answer.

- A specific consensus, replication, or synchronization protocol for distributed authority-state agreement was not specified. This is an implementation-layer concern; REA-01 states the architectural requirement (Section 15) and leaves the mechanism to implementation and, where relevant, REB-01/RGE-01.
- A normative numeric or structural bound on aggregate delegated scope was not added. This remains an open review-surface item (Section 6, Section 22) rather than a drafted rule, consistent with the instruction not to introduce large amounts of new normative language in this pass.
- Succession, renewal/extension, expansion, joint/shared authority, and orphaned authority were added to the review surface (Section 22) but not resolved into new lifecycle states. Resolving them may or maynot require new states in Section 4; that determination is deferred to normative drafting per Section 24.
- Specific safety mechanisms, fail-open/fail-closed defaults, and containment engineering were not defined in Section 17. These belong to REB-01, applicable behavioral specifications, and safety engineering practice; REA-01 defines only the authority and accountability basis for emergency/protective action.
- Specific cryptographic, access-control, or infrastructure-security mechanisms were not defined in Section 18. REA-01 states the traceability requirement that such mechanisms must ultimately satisfy; the mechanisms themselves belong to applicable security specifications and implementation.
- Which component or process formally makes or represents the RGV-01 Admissibility determination was not settled in Section 3. RGV-01 assigns REB-01 the role of enforcing an Admissibility determination but does not assign responsibility for making one; assigning that responsibility to RGE-01 by assertion here would risk exceeding what RGV-01 supports. This is recorded as an open question (Section 23, item 1) and a development-sequence item (Section 24, item 3) for resolution with RGE-01.
- Conformance testability concerns raised for “material change,” “purpose continuity,” and “scope drift detection” (Section 20) were not resolved in this pass, since the corrections requested for Version 1.3 did not include conformance-structure changes and resolving them would edge toward normative drafting. This remains available for a future pass; RGV-01's own qualitative treatment of “Consequential” (deferring a universal quantitative threshold to governing specifications) is a possible precedent worth considering at that time.

Remaining conflict with RGV-01

None identified. The Section 1 and Section 4 restatement of Runtime Execution Authority was checked against RGV-01 v2.3's published definitions of Authority, Legitimacy, Legitimacy Continuity, and Admissibility; it uses only relationships those definitions already establish and introduces no new canonical term. Section 3's connective-tissue statement uses RGV-01's Admissibility and REB definitions as published and does not assign RGE-01 or REB-01 a responsibility RGV-01 does not support. Section 14's corrected decommissioning language is consistent with RGV-01's allocation of execution-boundary control to REB rather than RiCo.

Readiness for another architecture review

Version 1.3 is ready for another architecture review. It resolves the foundational ontology, lifecycle-modeling, and cross-specification-connective issues identified in the prior adversarial review at the architecture level requested, without expanding into full normative prose. The open questions in Section 23 and the review-surface items in Section 22 are the recommended focus of the next review pass before normative SHALL/SHALL NOT drafting begins.

Focused Change Note — Version 1.3 to Version 1.4

• REA-01 now records authority-side lifecycle conditions that contribute to governance evaluation but does not claim to own, determine, or represent the complete RGV-01 Legitimacy condition.
• RiCo is bounded to Runtime Integrity Control and does not absorb REA-01, RGE-01, or REB-01 normative responsibilities.
• Temporary Protective / Emergency Authority is no longer asserted as a new Authority category; the scenario remains an open architectural question pending normative resolution.
• Decommissioning architecture is separated more clearly from deployment mechanics such as credential/key transfer and record-export procedures.
• Document remains an Architecture Review Draft; full normative expansion has not begun.

Focused Change Note — Version 1.4 to Version 1.5

• Refined Runtime Execution Authority as REA-01’s lifecycle-tracked representation of execution-relevant Authority, removing residual language that described it as a layer over Legitimacy.
• Recast Section 4.2 as Authority-Reliance Conditions so Active, Suspended, and Indeterminate describe the present availability of an Authority grant for reliance without claiming to represent the complete RGV-01 Legitimacy condition.
• Corrected Section 7 so authority maintenance concerns authority-side conditions for continued reliance rather than whether Authority itself is “legitimate.”
• Made explicit the T0→T1 continuity invariant: historically attributable or verifiable authority evidence does not by itself establish current applicability, continuing Authority, or continuing Legitimacy after material change.
• Added an execution-path invariant preventing authority loss, suspension, expiry, revocation, or material narrowing from being bypassed through queues, retries, recovery paths, alternate routes, delegated actors, replicas, failover, or functionally equivalent execution paths; enforcement mechanics remain outside REA-01.

• Revised Section 3 to describe REA-01, RGE-01, Admissibility, and REB-01 as functionally connected responsibilities rather than a single universal normative sequence, consistent with RGV-01 v2.3.
• Removed the residual implication that “Emergency Authority” is an established canonical Authority category; Section 17 remains an unresolved protective/emergency-action scenario pending cross-standard resolution.
• Added a governed-materiality requirement so material change cannot depend on ad hoc implementation judgment; domain-specific thresholds remain outside REA-01.
• Added cumulative/trajectory-based change treatment to prevent authority drift through sequences of individually sub-threshold changes.
• Added authority-side treatment for authority-relevant refusal or withdrawal: the record must represent its effect on remaining authorized execution space, while enforcement remains with REB-01 and applicable specifications.
• Added an intervention-window/consequence-boundary distinction for progressively irreversible execution, preserving meaningful authority-dependent intervention while change remains possible without requiring perpetual reversibility.
• Extended authority-record and conformance review surfaces to cover materiality decisions, cumulative change, authority-relevant refusal effect, and consequence-boundary timing.
• Added focused external-review questions and a targeted adversarial-test step for these stress-test findings before normative drafting.

Focused Change Note — Version 1.5 to Version 1.6

• Added a Governance-basis continuity requirement (Section 9): the governance basis applicable to an authority-relevant determination is the basis in force at the time of that determination, and a later governance change does not retroactively redefine the basis of a determination already made, mirroring the Section 8 evidence non-retroactivity principle without freezing legitimately governed policy change.
• Added a Governance of governance changes requirement (Section 9): a change to an authority-relevant governance mechanism itself — materiality criteria, authority mappings, thresholds, evidence requirements, precedence rules — is subject to authority-impact assessment where it could alter an existing or in-flight authority relationship, closing the path by which governance could be bypassed by changing the rules that trigger governance.
• Added an Authority-relevant temporal ordering requirement (Section 15): where ambiguity among event occurrence, observation, determination, effective transition, or execution ordering could change the governance result, the ordering actually relied upon must be reconstructable. This does not mandate a universal timestamp set; it is scoped to ordering-sensitive determinations.
• Extended the authority record (Section 19) with a governance-basis reference field and an ordering-reconstruction field, and extended Section 20 conformance with corresponding governance-basis-continuity and temporal-ordering categories.
• No change was made to Section 5, 9's governed-materiality threshold delegation, Section 10's refusal/withdrawal effect provision, Section 15's execution-path invariant, Section 16, or Section 18: these were reviewed against the adversarial findings and found to be correctly scoped architectural layering rather than unresolved REA-01-layer gaps. See the accompanying change report for the finding-by-finding disposition.
• Section 17 (Temporary Protective / Emergency Action) is unchanged and remains an open architectural question; the corrections in this pass did not identify a logical dependency requiring its resolution.
• Document remains an Architecture Review Draft; full normative expansion has not begun.

Publication Conversion Note — Version 1.6 (Architecture Review Draft → Published)

Effective 08/19/2026, Version 1.6 is converted from Architecture Review Draft to Published following completion of the final REA-01 architecture gate review and its confirmation that RGE-01 may safely proceed. This conversion is a publication-status and editorial action only; it makes no architectural, normative, or boundary change to REA-01 as approved at the gate review.
• Cover, header/footer, and Review Note updated to reflect Published status in place of Architecture Review Draft, and a publication date of 08/19/2026 was added to the cover.
• Architectural Position corrected: it referenced "Version 1.5" though the document was already at Version 1.6, and described itself as an architecture-review draft. It now correctly refers to Version 1.6 and to the document's Published status. No substantive content of this paragraph was altered beyond this correction.
• Section 22 and Section 23 self-references to "this document's status as an architecture review draft" and "this draft" were corrected to remove the contradiction with Published status. The substance of every review-surface item and open question in Sections 17, 22, and 23 is unchanged and remains open, consistent with this document's status as a pre-normative architecture specification.
• Section 6's aggregate-delegation provision was corrected from a stale "Version 1.3" reference to a version-neutral reference, consistent with Section 22 still listing aggregate delegation as unresolved.
• Prior change-log entries (Version 1.2 through Version 1.6) are left unmodified as an accurate historical record of this document's status at each point in time; they are not restated as though the document had always been published.
• Sections 17, 22, 23, and 24 remain in the published document as bounded, explicitly labeled review-surface and future-development content. Publication freezes REA-01's architecture as the stable baseline for RGE-01; it does not assert that these items have been resolved, and does not convert REA-01 into a mature normative (SHALL/SHALL NOT) specification.
• No change was made to the REA-01/RGV-01/RGE-01/REB-01 boundary allocations, to Section 3's connective-relationship statement, or to the meanings of Authority, Legitimacy, Admissibility, Runtime Execution Authority, Runtime Integrity Control, or RiCo.