CONTINUITY AXIOMS

Continuity is an audited property.

A hardened specification of continuity: attribution, boundaries, reversals, verification, tolerances, access, and audit—written to reduce drift under real load.

What this enforces

- Attribution that survives authority change.
- Bounded exposure through defined limits and access.
- Reversible decisions with recorded preconditions.
- Verification that reduces error in high-cost environments.
- Audits grounded in facts: artifacts, logs, and controls.

Operating premise

If a property cannot be enforced, logged, reviewed, and audited, it is treated as non-existent. This brief is designed for board-level circulation: concise, legible, and implementation-oriented.

Axioms 01–17

01 — Authority Transition Preserves Attribution
Attribution continuity is invariant under authority change.

02 — Boundary Degradation Increases Exposure
Exposure increases as boundary definition decreases.

03 — Decision Reversal Requires Record
A reversal implies recorded preconditions.

04 — Claims Require Addressable Reference
Every claim requires an addressable reference.

05 — State Transition Requires Logging
If the state changes, the transition must be logged.

06 — Load Implies Control Tightening
Control increases monotonically with load.

07 — Context Decay Requires Structural Preservation
Structure preserves intent independent of context.

08 — Undefined Ownership Elevates Risk
No owner implies elevated risk.

09 — Ambiguity Generates Interpretive Drift
Ambiguity produces drift.

10 — Definition Drift Implies Execution Drift
If definitions drift, execution drifts.

11 — Constraints Exist Only Under Enforcement
Unenforced constraints are non-constraints.

12 — Exceptions Require Logged Rationale
Every exception needs a recorded rationale.

13 — Permission Requires Defined Scope
Permission without scope is undefined permission.

14 — Scope Requires Defined Inputs
Scope must specify inputs.

15 — Inputs Require Verification
Inputs must be verified before reliance.

16 — Verification Reduces Error
More verification yields less error.

17 — Unknown Values Must Be Marked
Unknowns must be explicitly labeled.

Axioms 18–33

18 — Marked Unknowns Prevent Assumption
Marked unknowns block implicit assumptions.

19 — Decisions Must Be Attributable
Every decision has an accountable actor.

20 — Attribution Enables Review
Attribution makes actions reviewable.

21 — Specific Review Improves Control
Precision review strengthens control.

22 — Control Reduces Variance
Control reduces variability.

23 — Variance Requires Tolerance Definition
Variance must be measured against defined tolerance.

24 — Tolerance Requires Threshold
Tolerance requires explicit thresholds.

25 — Threshold Requires Stop Condition
Thresholds require stop conditions.

26 — Stop Preserves Optionality
Stop conditions preserve options.

27 — Optionality Requires Restraint
Optionality is created by restraint.

28 — Exposure Remains Controllable Under Limitation
Limits bound exposure.

29 — Limits Require Access Definition
Limits must specify access.

30 — Access Grants Must Be Recorded
Access grants must be recorded.

31 — Recorded Grants Enable Audit
Recorded grants make audit possible.

32 — Factual Audit Preserves Continuity
Factual audit preserves continuity.

33 — Continuity Requires Restraint and Action
Continuity requires restraint and action.

Minimum enforcement primitives

- **Append-only transition logging** for state changes and reversals.
- **Attribution ledger** that persists across authority handoffs.
- **Scope registry** binding permissions to defined inputs and boundaries.
- **Verification gates** for provenance, integrity, and freshness.
- **Access grant ledger** with scope, duration, rationale, and approver.
- **Factual audit map** connecting claims to artifacts (tickets, logs, controls).

Continuity audit checklist

- Is every decision attributable to an actor?
- Do authority transitions preserve attribution without reset?
- Are boundaries defined where exposure matters?
- Are reversals logged with preconditions and rationale?
- Are constraints enforced (or removed)?
- Are unknowns explicitly marked (and respected downstream)?
- Are tolerances and thresholds defined for variance?
- Do thresholds include stop conditions?
- Are access grants recorded with scope and duration?
- Is audit factual—grounded in artifacts, logs, and controls?

Note: This brief is a governance artifact. Its value is realized only when the underlying primitives are implemented and enforced.