CEDAR AUTHORIZATION PRIMER

Preserving Authorization

During AI-Assisted Code Modernization

How modernization teams change code without silently changing authority

A neutral architecture primer on evidence extraction, Cedar modeling, behavioral comparison, shadow decisions, and bounded cutover.

FIRST-PARTY SOURCES / INDEPENDENT LUMINITY SYNTHESIS



Luminity Digital
INTELLIGENCE, ENGINEERED. DELIVERED.

Modernization Must Preserve Who May Do What

AI can accelerate discovery and drafting. Evidence, comparison, and governed cutover determine whether authority remains intact.

AT A GLANCE

228
repositories
in the Reparo study

53
Cedar repositories
in the evaluated set

2
distinct checks
validation and behavior

1
governed cutover
route at a time

Evidence Before Policy 01

Legacy code is an evidence source. It may contain conflicts, gaps, and accidental behavior.

Comparison Before Cutover 02

Validator success and generated test agreement do not prove production equivalence.

IN THIS PRIMER

Key Points

01 Authorization Logic Hides Across Legacy Applications

The effective access model may be spread across routes, middleware, services, data filters, comments, and operating procedures.

02 AI Can Accelerate Authorization Evidence Extraction

Models can organize code and documentation into candidate rules, but reviewers still own intent, conflicts, and missing evidence.

03 Cedar Provides a Typed Target Authorization Model

A schema and explicit policies turn recovered evidence into a reviewable model of principals, actions, resources, context, and relationships.

04 Validation and Behavioral Comparison Answer Different Questions

Validation checks policy structure. Behavioral comparison tests whether candidate decisions agree with approved allow and deny cases.

05 Shadow Decisions Expose Migration Gaps

Parallel legacy and Cedar decisions reveal mismatches before the new policy becomes the enforcement source.

06 Progressive Cutover Preserves Authority

Move bounded routes only after coverage, comparison evidence, rollback, monitoring, and exception ownership meet the acceptance gate.

Generated policy remains a candidate until evidence and shadow decisions support cutover.

© 2026 Luminity Digital, Inc. | Independent synthesis of first-party sources.

Cedar first-party sources, Reparo, and AWS migration guidance · verified Nov 14, 2026

Authorization Logic Hides Across Legacy Applications

The effective access model may be spread across routes, middleware, services, data filters, comments, and operating procedures.

CONTROL EVIDENCE

- ✓ Route checks — CODE PATH
- ✓ Role and group logic — MIDDLEWARE
- ✓ Resource filters — DATA LAYER
- ✓ Operational exceptions — DOCUMENTATION
- ! Single policy source — OFTEN ABSENT

Requested Action → Governed Execution

AUTHORIZATION PATH

Legacy checks | Observed behavior | Candidate model

1 **Inventory** — Protected actions

2 **Trace** — Checks and data

3 **Classify** — Rule or exception

4 **Record** — Evidence source

FOUR INTERPRETATIONS

Distributed Logic — CODE

Authorization can appear in controllers, services, middleware, and queries.

Implicit Relationships — DATA

Data ownership and hierarchy may encode authority without a named policy.

Operational Exceptions — OPS

Runbooks and support procedures may contain material access exceptions.

Evidence Gaps — GAP

Missing tests and conflicting checks remain unknowns, not inferred truth.

BOUNDARY TEST — Inventory protected actions | Trace every decision input | Record conflicting evidence | Keep unknowns visible

© 2026 Luminity Digital, Inc. | Independent synthesis of first-party sources.

AI Can Accelerate Authorization Evidence Extraction

Models can organize code and documentation into candidate rules, but reviewers still own intent, conflicts, and missing evidence.

CONTROL EVIDENCE

- ✓ Source snippets — TRACEABLE
- ✓ Structured claims — CANDIDATE
- ✓ Conflicts and unknowns — PRESERVED
- ✓ Human review — REQUIRED
- ! Automatic intent recovery — NOT PROVEN

Requested Action → Governed Execution

AUTHORIZATION PATH

Repository evidence | AI extraction | Reviewed claims

1. **Collect** — Code and docs
2. **Extract** — Actors and rules
3. **Challenge** — Conflicts and gaps
4. **Approve** — Bounded claim set

FOUR INTERPRETATIONS

Source Traceability — TRACE

Every candidate rule links back to code, comments, documentation, or observed behavior.

Structured Extraction — P-A-R-C

Normalize principal, action, resource, context, relationships, and exceptions.

Conflict Register — REVIEW

Keep contradictory checks and unclear precedence visible for review.

Human Authority — OWNER

Application owners approve intent and unresolved exceptions before policy generation.

BOUNDARY TEST

Keep the source citation | Separate fact from inference | Escalate contradictions | Require accountable review

© 2026 Luminity Digital, Inc. | Independent synthesis of first-party sources.

Reparo paper · verified Nov 14, 2026

Cedar Provides a Typed Target Authorization Model

A schema and explicit policies turn recovered evidence into a reviewable model of principals, actions, resources, context, and relationships.

CONTROL EVIDENCE

- ✓ Principal types — MODELED
- ✓ Actions and resources — EXPLICIT
- ✓ Context attributes — TYPED
- ✓ Policy source links — RETAINED
- ! Unmapped legacy behavior — MIGRATION GAP

Requested Action → Governed Execution

AUTHORIZATION PATH

Recovered evidence | Cedar schema | Candidate policies

1. **Model** — Entity types
2. **Map** — Actions and resources
3. **Author** — Permit and forbid
4. **Trace** — Policy to source

FOUR INTERPRETATIONS

Typed Vocabulary — SCHEMA

The schema names entity types, actions, attributes, and relationships.

Explicit Decisions — POLICY

Policies state which principal may perform an action on a resource under conditions.

Forbid Boundary — DENY

Explicit forbids preserve hard ceilings that broad permits cannot override.

Traceability — LINEAGE

Each candidate statement remains linked to the evidence and reviewer decision that produced it.

BOUNDARY TEST

Model before translation | Preserve hard prohibitions | Track every policy source | Leave unmapped checks open

© 2026 Luminity Digital, Inc. | Independent synthesis of first-party sources.

Cedar authorization and Cedar policy validation · verified Nov 14, 2026

Validation and Behavioral Comparison Answer Different Questions

Validation checks policy structure. Behavioral comparison tests whether candidate decisions agree with approved allow and deny cases.

CONTROL EVIDENCE

- ✓ Validator-clean policy — STRUCTURAL
- ✓ Allow and deny cases — BEHAVIORAL
- ✓ Independent review — SAMPLED
- ✓ Decision agreement — MEASURED
- ! Production equivalence — NOT ESTABLISHED

Requested Action → Governed Execution

AUTHORIZATION PATH

Candidate policy | Validation and tests | Comparison evidence

1. **Validate** — Schema and types
2. **Generate** — Allow and deny cases
3. **Execute** — Candidate policy
4. **Compare** — Decision agreement

FOUR INTERPRETATIONS

Reparo Corpus — RESEARCH

The paper evaluated 228 repositories, including 53 Cedar repositories.

Validator Result — STRUCTURE

It reported 99 to 100 percent validator-clean output after repair.

Cedar Agreement — BEHAVIOR

It reported 82.0 to 86.5 percent agreement with the generated oracle.

Evidence Limit — LIMIT

The same repository evidence can shape both policy and oracle, so agreement is not proof.

BOUNDARY TEST

Validate structure | Test approved behavior | Review disagreement samples | Do not claim equivalence

© 2026 Luminity Digital, Inc. | Independent synthesis of first-party sources.

Reparo paper and Cedar policy validation · verified Nov 14, 2026

Shadow Decisions Expose Migration Gaps

Parallel legacy and Cedar decisions reveal mismatches before the new policy becomes the enforcement source.

CONTROL EVIDENCE

✓ Same request facts	COMPARABLE
✓ Legacy decision	RECORDED
✓ Cedar decision	SHADOW
✓ Mismatch classification	REVIEWED
! Automatic cutover	BLOCKED

Requested Action → Governed Execution

AUTHORIZATION PATH

Legacy decision | Parallel comparison | Cedar shadow

1 **Capture** — Same request

2 **Decide** — Legacy and Cedar

3 **Classify** — Mismatch cause

4 **Resolve** — Policy or evidence

FOUR INTERPRETATIONS

Comparable Inputs — INPUT

Both paths need the same identity, action, resource, and context facts.

Mismatch Classes — DIFF

Separate translation errors, stale data, legacy defects, and approved behavior changes.

No Silent Repair — HOLD

A model should not choose the winner when evidence conflicts or intent remains unclear.

Decision Evidence — AUDIT

Retain request facts, both decisions, policy version, and reviewer disposition.

BOUNDARY TEST — Run both paths | Classify every material mismatch | Approve intended changes | Retain the evidence

© 2026 Luminity Digital, Inc. | Independent synthesis of first-party sources.

AWS OPA-to-Cedar migration and Cedar security · verified Nov 14, 2026

Progressive Cutover Preserves Authority

Move bounded routes only after coverage, comparison evidence, rollback, monitoring, and exception ownership meet the acceptance gate.

CONTROL EVIDENCE

- ✓ Bounded route — SELECTED
- ✓ Shadow threshold — MET
- ✓ Rollback path — TESTED
- ✓ Exception owner — NAMED
- ! Unresolved high-risk gap — HOLD

Requested Action → Governed Execution

AUTHORIZATION PATH

Shadow evidence | Acceptance gate | Enforced Cedar route

1. **Select** — Low-breadth route
2. **Approve** — Evidence and owners
3. **Cut Over** — Bounded enforcement
4. **Observe** — Rollback if needed

FOUR INTERPRETATIONS

Route-by-Route — SCOPE

Cut over a bounded operation or service boundary instead of the entire application.

Rollback Ready — BACKOUT

Keep the prior enforcement path available until the new route proves stable.

Exception Register — EXCEPT

Assign owners and expiry dates to retained legacy exceptions and uncovered behavior.

Acceptance Record — PROOF

Retain coverage, comparisons, approvals, deployment version, monitoring, and residual risk.

BOUNDARY TEST | Cut over bounded routes | Keep rollback available | Own every exception | Accept residual risk explicitly

© 2026 Luminity Digital, Inc. | Independent synthesis of first-party sources.

AWS OPA-to-Cedar migration and Cedar security · verified Nov 14, 2026