

Authorization Decision Matrix v1

RBAC, Default Deny and Least Privilege

Outcome. Design one bounded authorization matrix with explicit subjects, resources, actions and deny-by-default behavior, then prove allowed and forbidden requests at the enforcement boundary.
Evidence gate. Accept only when every critical dimension has inspectable evidence, the negative probe behaves as predicted, and changed-context transfer preserves a residual limitation.

RBAC, Default Deny and Least Privilege Evidence Path

01 AUTHZ DECISION Authority: Authorization answers whether a specific subject may perform a specific action on a specific resource under the policy context. Boundary: Authentication identity alone does not authorize the requested action.	02 DEFAULT DENY Authority: Requests that do not match an explicit allow rule should be denied at the authoritative enforcement point. Boundary: A framework default is not treated as durable evidence unless it is explicitly configured and tested.	03 LEAST PRIVILEGE Authority: Roles should receive only the permissions required for their owned tasks, including both horizontal and vertical boundaries. Boundary: Least privilege does not require one universal role hierarchy.
04 EVERY REQUEST Authority: Authorization checks must apply to each protected request/resource at the enforcement boundary, not only during navigation or login. Boundary: Client-side hiding is not a substitute for server-side authorization.	05 MODEL FIT Authority: RBAC is one authorization model; when resource relationships or attributes dominate, a different or combined model may be more appropriate. Boundary: This lesson does not teach full ABAC/ReBAC design.	06 EVIDENCE BOUNDARY Authority: Separate source facts, local observations, bounded inferences, and human decisions. Boundary: Unavailable production behavior remains NOT_OBSERVED or NEEDS_VERIFICATION.

Identity, decision, and claim boundary

Learner		Reviewer	
Case / attempt		Capture date	
Scenario / concern		Decision	ACCEPT / REPAIR / DEFER

Claim boundary. This is a bounded executable lab. Retain implementation, applicable runtime, browser, DOM, or tool observations, mutation, repair, transfer, and residual-limit evidence; one passing checker is not whole-system proof. Runtime claims require retained output from the supplied bounded fixture. Source facts and static readiness are not promoted into production observations.

Required record fields and evidence tests

A field is complete only when its value is bounded, traceable, and classified. Use UNKNOWN when the required observation is unavailable or contradictory.

Field	Question to close	Minimum evidence	Invalid promotion
Subject/Role	What does Subject/Role mean in this case?	Bounded scenario fact, source, or observable	Inference can be relabeled as observation
Resource Scope	What does Resource Scope mean in this case?	Bounded scenario fact, source, or observable	Inference can be relabeled as observation
Action	What does Action mean in this case?	Bounded scenario fact, source, or observable	Inference can be relabeled as observation
Explicit Allow Rule	What does Explicit Allow Rule mean in this case?	Bounded scenario fact, source, or observable	Inference can be relabeled as observation
Default Decision	What does Default Decision mean in this case?	Bounded scenario fact, source, or observable	Inference can be relabeled as observation
Enforcement Point	What does Enforcement Point mean in this case?	Bounded scenario fact, source, or observable	Inference can be relabeled as observation
Positive Probe	What does Positive Probe mean in this case?	Bounded scenario fact, source, or observable	Inference can be relabeled as observation
Negative Probe	What does Negative Probe mean in this case?	Bounded scenario fact, source, or observable	Inference can be relabeled as observation
Evidence	What does Evidence mean in this case?	Bounded scenario fact, source, or observable	Inference can be relabeled as observation
Residual Policy Question	What does Residual Policy Question mean in this case?	Bounded scenario fact, source, or observable	Inference can be relabeled as observation

Evidence and failure states

Evidence: OBSERVED / INFERRED / NOT_OBSERVED / NEEDS_VERIFICATION. Decisions: ACCEPT / REPAIR / DEFER. Failure layers: AUTHZ DECISION / DEFAULT DENY / LEAST PRIVILEGE / EVERY REQUEST / MODEL FIT.

Decision and evidence table

English support projection from derived_text/tables/SEC-002-TBL1.example.en-US.json. This example demonstrates field relationships; it does not supply the learner's transfer or final decision evidence.

Field	Governed example value	Evidence question	Boundary check
Subject/Role	bob / Editor	What observation supports Subject/Role?	Is the conclusion no stronger than this value?
Resource Scope	workspace w1 / file f1	What observation supports Resource Scope?	Is the conclusion no stronger than this value?
Action	file.write	What observation supports Action?	Is the conclusion no stronger than this value?
Explicit Allow Rule	Editor includes file.write AND subject.workspace_id == resource.workspace_id	What observation supports Explicit Allow Rule?	Is the conclusion no stronger than this value?
Default Decision	DENY	What observation supports Default Decision?	Is the conclusion no stronger than this value?
Enforcement Point	synthetic server policy evaluator	What observation supports Enforcement Point?	Is the conclusion no stronger than this value?
Positive Probe	bob writes file f1 in w1 -> ALLOW	What observation supports Positive Probe?	Is the conclusion no stronger than this value?
Negative Probe	bob member.manage in w1 -> DEFAULT_DENY	What observation supports Negative Probe?	Is the conclusion no stronger than this value?
Evidence	local fixture outputs stored as observations	What observation supports Evidence?	Is the conclusion no stronger than this value?
Residual Policy Question	Production identity, tenant membership and policy deployment are not proven here	What observation supports Residual Policy Question?	Is the conclusion no stronger than this value?
Source-package validation	ACCEPTED_IMPORTABLE; 0 blockers; 0 warnings · QA_ACCEPTED_ELIGIBLE		

Complete Authorization Decision Matrix v1

Enter one bounded value per required field. Every material entry needs an evidence locator and a state. Use additional workbook rows when the artifact needs multiple concerns, responsibilities, resources, or path steps.

Required field	Learner value	Evidence locator	State / review note
Subject/Role			OBSERVED / INFERRED / UNKNOWN
Resource Scope			OBSERVED / INFERRED / UNKNOWN
Action			OBSERVED / INFERRED / UNKNOWN
Explicit Allow Rule			OBSERVED / INFERRED / UNKNOWN
Default Decision			OBSERVED / INFERRED / UNKNOWN
Enforcement Point			OBSERVED / INFERRED / UNKNOWN
Positive Probe			OBSERVED / INFERRED / UNKNOWN
Negative Probe			OBSERVED / INFERRED / UNKNOWN
Evidence			OBSERVED / INFERRED / UNKNOWN
Residual Policy Question			OBSERVED / INFERRED / UNKNOWN

Human closure

Decision	ACCEPT / REPAIR / DEFER	Reviewer	
Residual uncertainty		Consequence	
Smallest next evidence		Evidence owner / date	

Run → observe → mutate → repair → transfer

Run the bounded fixture and retain observable results. Predict each deliberate mutation before executing it, then prove the repair and changed-context transfer.

Case	Bounded concern or change	Provisional decision	Deciding evidence	Learner observation	Stable / unresolved boundary
SIMPLE	A synthetic project workspace has Viewer, Editor and WorkspaceAdmin roles over projects, files and member-management actions. The learner builds the smallest role/action matrix and verifies both horizontal and vertical denials through a local policy evaluator.	Every authorization result needs subject, action, resource scope, and an authoritative enforcement point.	Creates the first valid rows of Authorization Decision Matrix v1.	<div></div> <div></div>	<div></div> <div></div>
REALISTIC	Remove the explicit rule for a newly introduced action and verify the decision remains deny.	A newly introduced action without an allow rule must remain denied.	Shows why happy-path success is insufficient.	<div></div> <div></div>	<div></div> <div></div>
EDGE OR FAILURE	Give Editor a member-management permission and show the least-privilege review flags the vertical expansion.	Adding member-management to Editor should be flagged as a vertical privilege expansion.	Connects defensive repair to evidence rather than intuition.	<div></div> <div></div>	<div></div> <div></div>
TRANSFER NEAR	A synthetic support system has Agent, Supervisor and Billing roles with tenant-scoped tickets. Build a new minimal matrix and identify one case where role alone may be insufficient context.	Tenant-scoped support access may require context beyond a role name alone.	Tests independent transfer.	<div></div> <div></div>	<div></div> <div></div>

Reasoning sequence

Phase	Action	Required capture	Truth rule
Boundary	Enumerate roles, resources, and actions	Scenario fact, evidence locator, or explicit UNKNOWN	Runtime claims require retained output from the supplied bounded fixture. Source facts and static readiness are not promoted into production observations.
Boundary	Declare default deny	Scenario fact, evidence locator, or explicit UNKNOWN	Runtime claims require retained output from the supplied bounded fixture. Source facts and static readiness are not promoted into production observations.
Boundary	Locate enforcement	Scenario fact, evidence locator, or explicit UNKNOWN	Runtime claims require retained output from the supplied bounded fixture. Source facts and static readiness are not promoted into production observations.
Stress test	Probe an unknown action	Prediction, changed assumption, stable boundary, next evidence	A plausible counterexample does not become an observed implementation fact
Stress test	Expand Editor privilege	Prediction, changed assumption, stable boundary, next evidence	A plausible counterexample does not become an observed implementation fact
Stress test	Test a direct request	Prediction, changed assumption, stable boundary, next evidence	A plausible counterexample does not become an observed implementation fact

Guardrail. A local deterministic fixture does not prove production timing, delivery, ordering, durability, recovery, enforcement, or system-wide correctness.

Changed-context transfer

Transfer the matrix to a tenant-scoped support system.

Transfer item	Changed-context requirement	Learner evidence	Review check
Scenario	State the changed concern, resource, or responsibility boundary.	_____	Worked scenario not copied
Observed facts	Record only facts supplied or directly observed.	_____	Inference stays separate
Concern split	Create separate rows for independent responsibilities or paths.	_____	No page-wide shortcut
Classification	Choose only ACCEPT / REPAIR / DEFER or preserve UNKNOWN.	_____	Placement is justified
Failure probe	Apply one counterexample that tests an over-broad claim.	_____	No invented mechanism
Non-claims	State at least two limits plus the smallest next evidence.	_____	Residual and next evidence stated

Non-compensatory review

Critical dimension	PASS / REPAIR	Evidence locator	Repair or rationale
Scenario and responsibility boundary correctness	_____ _____	_____	_____
Observation, inference, and source traceability	_____ _____	_____	_____
Decision rationale and next-evidence quality	_____ _____	_____	_____
Failure diagnosis and overclaim resistance	_____ _____	_____	_____
Transfer, residual uncertainty, and non-goals	_____ _____	_____	_____

Canonical QA gate

Validation	ACCEPTED_IMPORTABLE; 0 blockers; 0 warnings	Disposition	QA_ACCEPTED_ELIGIBLE
Blocker / note	No canonical-source blocker recorded.	Clearance receipt	_____

Media decision. Deck and video are NOT_APPLICABLE_WITH_RATIONALE; the embedded visuals, editable record, worksheet, and learner-authored reasoning are the assessed support.