DecisionGuard

Evidence Bundle

Generated March 16, 2026 at 7:23:50 AM | Region: EU | Format v1.2.0

BLOCK

405ms

Risk: MEDIUM

a7fac9f0-9a78-46fc-8ecb-9ce8fe6d2bac

1. EXECUTIVE SUMMARY

Review ID	a7fac9f0-9a78-46fc-8ecb-9ce8fe6d2bac
Tenant	ClaudeCode (d72522c3-c49b-4140-975e-c7d5981557fe)
Created	Mar 10, 2026, 11:21:05 AM
Status	COMPLETED
Environment	prod
Change Type	tool_call
Resource	postgresql
Intent	{"requested_goal":"Drop the customers table entirely","proposed_action":"DROP TABLE customers CASCADE"}
Idempotency Key	proxy-1773141665083-7n7rx5kk

2. ACTOR & IDENTITY

Actor Type	agent
Actor ID	oauth-6e390917-8f0c-4002-960e-b9cd0497cbf0
Name	USE_THIS_KEY

Identity Verification

Assurance Level	low
Confidence	30%
Verification	not_provided
Principal ID	6215abe7-aa26-41cf-b4b9-7338d7c79103
Warnings	IDENTITY_UNVERIFIED; IDENTITY_WEAK_ASSURANCE; IDENTITY_ROLE_UNDECLARED; IDENTITY_SCOPE_UNDECLARED

3. DECISION CHAIN

EVALUATOR
BLOCK

ROUTER
No Override

FINAL
BLOCK

Confidence	N/A

4. RISK ANALYSIS & FINDINGS

AI Reasoning

Change in prod environment for postgresql assessed as MEDIUM risk. Found 3 potential issue(s). Note: Missing facts (internet_exposed, critical_assets_exposed, blast_radius) - assessment may be conservative.

Findings (8)

Severity	Category	Description
INFO	general	Production Environment Change
INFO	general	Limited Security Context
INFO	general	Destructive Operation Detected
INFO	general	Mass Data Deletion Risk

Severity	Category	Description
INFO	general	Cascade Deletion Impact
INFO	general	Unknown Change Owner
INFO	general	Missing Recovery Plan
INFO	general	Crown Jewel Asset Impact

Missing facts (assessment may be conservative): internet_exposed, critical_assets_exposed, blast_radius

5. GOVERNANCE & COMPLIANCE

No governance codes emitted.

Data Retention	365 days

6. SENSITIVE CONTEXT & DLP

No sensitive data detected in this review.

7. ROUTER TRACE

No rules matched.

Router Duration	844ms

8. TRIAGE SUMMARY

Inspection Level	STANDARD
Triage Score	96 / 140 (threshold: 160)

- complexity: Small payload (255 chars); Shallow nesting (2 levels)
- completeness: Partial context: actor, intent; No summary; No facts provided
- environment: Environment: prod
- criticality: Change type: tool_call
- actor: Actor type: agent (oauth-6e390917-8f0c-4002-960e-b9cd0497cbf0)

9. PIPELINE STAGES

Stage	Status	Duration	Provider	Model
verdict core	completed	-	heuristic	heuristic-v1
governance	completed	-	heuristic	heuristic-v1
agentic	completed	-	heuristic	heuristic-v1
background enrichment	completed	9060ms	openai	gpt-4o-mini-2024-07-18

Reviewer Type	hybrid
Model	staged-v1.0.0
Version	unknown
Prompt Hash	59fed5b6a1af92d1e96034765f12a62f581832f95d209645ea075a298ed6a82c

10. APPROVAL TRAIL

No approval required for this review.

11. AUTHORITY ARTIFACT

No authority artifact was issued for this review.

12. EXECUTION & FORWARDING

Forwarded	No

13. INCIDENT INTELLIGENCE

Severity	MATERIAL
Near Miss	No
Impact Tags	missing_context

14. AUDIT TIMELINE

Timestamp	Event	Summary
2026-03-10 11:21:05	review.created	Review submitted for governance
2026-03-10 11:21:05	review.processing	review processing
2026-03-10 11:21:05	triage.calculated	Triage scored 96 !' STANDARD
2026-03-10 11:21:05	pipeline.started	pipeline started
2026-03-10 11:21:05	pipeline.completed	pipeline completed
2026-03-10 11:21:05	stage.completed	stage completed
2026-03-10 11:21:05	stage.completed	stage completed
2026-03-10 11:21:05	stage.completed	stage completed
2026-03-10 11:21:05	review.completed	Review completed with verdict: ALLOW_WITH_CONDITIONS
2026-03-10 11:21:05	rule.matched	rule matched
2026-03-10 11:21:05	action.executed	action executed
2026-03-10 11:21:05	router.evaluated	Router matched 1 rules
2026-03-10 11:21:05	router.evaluated	Router matched 1 rules
2026-03-10 11:21:05	callback.attempted	callback attempted
2026-03-10 11:21:05	router.evaluated	Router matched 0 rules
2026-03-10 11:21:06	callback.attempted	callback attempted
2026-03-10 11:21:08	callback.attempted	callback attempted
2026-03-10 11:21:12	callback.attempted	callback attempted
2026-03-10 11:21:20	callback.attempted	callback attempted
2026-03-10 11:21:21	callback.failed	callback failed

15. INTEGRITY VERIFICATION

Algorithm	sha256
Evidence Hash	e7121f385add59e3b9ad4724f135a289653309aa40818747b58a81bb651a93dd
Router Inputs	35d6f32a781a7b2d37ebf973b6ea17d473bb0e97d018882519473e78dff2d120
Triage Inputs	776452fadb68c5c7bf9b8a1261f682c4
Triage Config	0d63a196f02675a27e5b26a9b865f52b140df29d694b607615904ad52ab5c817

16. API INPUT (REVIEW REQUEST)

Resource	postgresql
Change Type	tool_call
Environment	prod

```
{
  "intent": {
    "requested_goal": "Drop the customers table entirely",
    "proposed_action": "DROP TABLE customers CASCADE"
  },
  "tool_name": "postgresql",
  "tool_arguments": {
    "query": "DROP TABLE customers CASCADE",
    "table": "customers",
    "operation": "DROP",
    "destructive": true
  }
}
```

17. API OUTPUT (VERDICT RESPONSE)

```
{
  "decision": "BLOCK",
  "risk": "MEDIUM",
  "summary": "Change in prod environment for postgresql assessed as MEDIUM risk. Found 3 potential issue(s).
Note: Missi
  "findings": [
    {
      "title": "Production Environment Change",
      "severity": "INFO",
      "confidence": 0.7
    },
    {
      "title": "Limited Security Context",
      "severity": "INFO",
      "confidence": 0.6
    },
    {
      "title": "Destructive Operation Detected",
      "severity": "INFO",
      "confidence": 0.92
    },
    {
      "title": "Mass Data Deletion Risk",
      "severity": "INFO",
      "confidence": 0.95
    },
    {
      "title": "Cascade Deletion Impact",
      "severity": "INFO",
      "confidence": 0.9
    },
    {
      "title": "Unknown Change Owner",
      "severity": "INFO",
      "confidence": 0.88
    },
    {
      "title": "Missing Recovery Plan",
      "severity": "INFO",
      "confidence": 0.88
    },
    {
      "title": "Crown Jewel Asset Impact",
      "severity": "INFO",
      "confidence": 0.92
    }
  ],
  "required_controls": [
    "Change window compliance",
    "Monitoring alerts configured"
  ],
  "governance_tags": [
    "GOV-05"
  ]
}
```

This evidence bundle contains no secrets. Sensitive payload fields are redacted. Hashes provided for integrity verification.