AI TEMPLATE | RISK MANAGEMENT

Root Cause Analysis Template

A structured investigation framework for operations teams. Move from symptoms to true root causes using the 5-Why chain, evidence grading, contributing factor mapping, and corrective action tracking.

Category:	Risk Management / Operations
Audience:	Managers, analysts, investigators, quality leads
Use When:	Incidents, repeated failures, near-misses, process breakdowns
Sections:	12 structured sections with investigation tables
Principle:	Separate facts from assumptions. Fix systems, not people.

SECTION 1

Incident Summary

Capture the basic facts before investigating. Do not interpret yet. Just record what happened, when, where, and who was involved.

FIELD	DETAILS

FIELD	DETAILS
Incident Title	
Date & Time Detected	
Date & Time Started (if different)	
Location / System / Process	
Reported By	
Severity	Critical / High / Medium / Low
Impact Summary	
Immediate Action Taken	

> **Rule:** Write what happened, not why. The "why" comes later. Premature conclusions poison the investigation.

SECTION 2

Timeline of Events

Reconstruct the sequence. Include what was observed, by whom, and what action was taken at each point. Gaps in the timeline are clues.

TIME	EVENT	OBSERVED BY	ACTION TAKEN	EVIDENCE

If you cannot fill a row with evidence, mark it as "assumed" or "unknown". Gaps matter as much as facts.

SECTION 3

The 5-Why Chain

Start with the problem statement. Ask "why" repeatedly until you reach a systemic cause. Most teams stop too early. Push past the comfortable answer.

Problem Statement

WHAT HAPPENED (FACTUAL, SPECIFIC, MEASURABLE)

LEVEL	WHY?	ANSWER	EVIDENCE TYPE
Why 1	Why did this happen?		Data / Observation / Testimony
Why 2	Why did that cause occur?		Data / Observation / Testimony
Why 3	Why was that possible?		Data / Observation / Testimony
Why 4	Why did the system allow it?		Data / Observation / Testimony
Why 5	Why was there no safeguard?		Data / Observation / Testimony

Depth test: If your root cause is a person ("John made a mistake"), you stopped too early. Ask: why was the system designed so that one person could cause this?

SECTION 4

Evidence Grading

Not all evidence is equal. Grade each piece to understand how confident you are in your conclusions.

GRADE	MEANING	EXAMPLE	CONFIDENCE
A - Hard Data	System logs, metrics, timestam	Server log shows timeout at 14:03	High
B - Direct Observation	Witnessed by a person present	Operator saw the alert fire	Medium-High
C - Testimony	Reported after the fact	"I think I clicked approve"	Medium
D - Inference	Logical deduction, no direct pro	Must have been X because Y	Low-Medium
E - Assumption	No evidence, just belief	"It always works that way"	Low

If your root cause relies only on Grade C-E evidence, you need more investigation before declaring it solved.

SECTION 5

Contributing Factor Map

Root causes rarely act alone. Map the contributing factors across these categories to see the full picture.

CATEGORY	CONTRIBUTING FACTOR	EVIDENCE	GRADE	FIXABLE?
Process				Yes / No / Partial
People / Training				Yes / No / Partial
Technology / Tools				Yes / No / Partial
Communication				Yes / No / Partial
Oversight / Controls				Yes / No / Partial
External / Environment				Yes / No / Partial
Incentives / Pressure				Yes / No / Partial

Key insight: If you find 3+ contributing factors in the same category, that category is your systemic weakness, not the individual incident.

SECTION 6

Barrier Analysis

What defenses should have prevented this? Why did they fail? This reveals where your safety net has holes.

BARRIER (CONTROL)	EXPECTED BEHAVIOR	ACTUAL BEHAVIOR	WHY IT FAILED	FIX PRIORITY

Barrier Types to Check

- Prevention barriers: Should have stopped the event from starting
- Detection barriers: Should have caught it early
- Mitigation barriers: Should have limited the damage
- Recovery barriers: Should have restored normal state quickly

SECTION 7

Root Cause Statement

Write the root cause as a clear, testable statement. It must be systemic (not a person), supported by evidence, and actionable.

COMPONENT	YOUR ANSWER

COMPONENT	YOUR ANSWER
Root Cause (1 sentence)	
Category	Process / People / Technology / Controls / External
Evidence Grade	A / B / C / D / E
Confidence Level	High / Medium / Low
Could this cause other incidents?	Yes / No / Unknown
Has this happened before?	Yes (when?) / No / Unknown

Quality check: A good root cause statement passes this test: "If we fix X, this specific failure mode cannot recur." If it can still recur, dig deeper.

SECTION 8

Corrective Actions

Define actions that fix the root cause, not just the symptom. Each action must have an owner, deadline, and success measure.

ACTION	TYPE	OWNER	DUE DATE	SUCCESS MEASURE	STATUS

Action Types

- Immediate containment: Stop the bleeding now (hours)
- Short-term fix: Prevent recurrence this week (days)
- Systemic fix: Redesign the process or control (weeks)
- Verification: Confirm the fix actually works (ongoing)

SECTION 9

Verification Plan

How will you prove the fix works? Define what you will measure, when you will check, and what "fixed" looks like.

CORRECTIVE ACTION	VERIFICATION METHOD	CHECK DATE	EXPECTED RESULT	ACTUAL RESULT	CLOSED?

Discipline: An RCA is not complete until verification confirms the fix works. Schedule the check date now, not later.

SECTION 10

Lessons Learned

What did this investigation teach the team? Capture insights that apply beyond this single incident.

LESSON	APPLIES TO	ACTION TO EMBED	OWNER

SECTION 11

Recurrence Risk Assessment

Before closing, assess whether this could happen again elsewhere.

QUESTION	ANSWER
Could this happen in another team/location?	
Are similar processes at risk?	
Do other systems share the same weakness?	
Is the fix scalable or local only?	
Who else needs to know about this?	

SECTION 12

AI Prompt - Copy and Paste

Use this prompt with any AI assistant. Paste your incident data where indicated.

```
Act as a senior operations investigator.

Conduct a Root Cause Analysis using the incident data below.
Be rigorous. Separate facts from assumptions.

Structure:
1. Incident Summary (what, when, where, severity)
2. Timeline of Events (sequence with evidence)
3. 5-Why Chain (push past the obvious)
4. Evidence Grading (rate each piece A through E)
5. Contributing Factor Map (process, people, tech, controls)
6. Barrier Analysis (what should have prevented this)
7. Root Cause Statement (systemic, testable, actionable)
8. Corrective Actions (immediate, short-term, systemic)
9. Verification Plan (how to prove the fix works)
10. Lessons Learned (what applies beyond this incident)
11. Recurrence Risk (could this happen elsewhere)

Rules:
- Never blame a person. Find the system failure.
- Grade every piece of evidence.
- If evidence is weak, say so explicitly.
- Every action must have an owner and deadline.
- The root cause must be fixable and testable.

Incident data: [PASTE HERE]
Timeline: [PASTE HERE]
Known facts: [PASTE HERE]
Assumptions: [PASTE HERE]
Previous similar incidents: [PASTE HERE]
```

Investigation Principles

- Fix systems, not people. If a person could cause it, the system allowed it.
- Evidence over opinion. Grade everything.
- Depth over speed. A shallow RCA is worse than none.
- Verify before closing. An unverified fix is a hope, not a solution.

SECTION

Common Mistakes in Root Cause Analysis

- Stopping at the first "why" - the obvious answer is rarely the root cause.
- Blaming individuals instead of finding systemic failures.
- Confusing correlation with causation.
- Accepting testimony as fact without corroboration.
- Declaring a root cause with only Grade D-E evidence.
- Defining corrective actions that only fix the symptom.
- Closing the RCA before verifying the fix works.
- Ignoring contributing factors outside your team.
- Treating every incident as unique when patterns exist.
- Writing the RCA to satisfy compliance, not to learn.

Best Practices

- Start with the timeline. Facts first, interpretation second.
- Use the 5-Why chain but branch when multiple causes exist.
- Grade every piece of evidence before drawing conclusions.
- Map contributing factors across all categories, not just the obvious one.
- Check all four barrier types: prevention, detection, mitigation, recovery.
- Write the root cause as a testable hypothesis.
- Define verification criteria before implementing the fix.
- Share lessons learned with teams who face similar risks.
- Track recurrence. If it happens again, your RCA failed.
- Time-box the investigation. 80% of value comes in the first 48 hours.

Final principle: The purpose of RCA is not to explain the past. It is to prevent the future. If your analysis does not change a system, it was documentation, not investigation.