StackGen

ROOT CAUSE TAXONOMY

SRE ROOT CAUSE TAXONOMY 16 ACTIVE ROOT CAUSE CODES • 5 CATEGORIES

You fixed it. Do you know why it broke?

Go beyond "human error" — classify the actual root cause of every incident and start seeing the patterns that repeat.

DERIVED FROM THE STATE OF RELIABILITY 2026 ANALYSIS OF:

27K+	178K+	392	2018-26
classified incidents	status-page entries	companies	date range

A practical reference for SRE, platform and reliability teams.

Root Cause Taxonomy

SSOR 2026 QUICK REFERENCE • TAXONOMY V0.9 • 16 ACTIVE ROOT CAUSE CODES • RC-14 RETIRED • SOFTWARE & ONLINE SERVICES

HOW TO USE

1. Identify the proximate cause
Why did the system behave this way?

2. Match to the most specific RC
Prefer RC-08 over RC-15 if vendor is named.

3. Check FM partners
For the most common failure-mode pairings.

4. Disclosure badge
High = abundant signal · Med = needs confirmation · Low = infer cautiously

Code & Config Changes — 3 RCs

RC-01 Code Defect / Regression — HIGH

A code change introduced a defect causing incident-level impact.

Deploy timing correlation | Rollback resolves | "regression in X"

FM → FM-09 • FM-04 • FM-06 • FM-08

RC-02 Config Change — MED

Non-code change — config value, feature flag, IAM policy, DNS record.

No code deploy | Specific config push | Undocumented change

FM → FM-10 • FM-30 • FM-01

RC-03 Schema / Index Change — MED

DDL change — column, index, partition, stored procedure causes impact.

DB errors after DDL | Query plan regression | Specific endpoints affected

FM → FM-06 • FM-11

Resources & Limits — 2 RCs

RC-04 Capacity Exhaustion — HIGH

Finite resource consumed faster than replenished — CPU, memory, connections, disk.

Resource at ceiling | OOM kills | Queue growing | "scaling up"

FM → FM-13 • FM-14 • FM-08

RC-05 Quota / Rate Limit — MED

A quota or rate limit was hit — internal threshold or externally imposed.

HTTP 429s | "rate limit exceeded" | Throttling; specific clients

FM → FM-03 • FM-13

Infrastructure — 3 RCs

RC-06 Network / DNS — MED

Networking or DNS infrastructure — BGP routing, DNS resolution, network partition

"DNS resolution issue" | BGP; packet loss | Geo-based intermittent failures

FM → FM-30 • FM-01 • FM-29

RC-07 Authentication / Authorization — MED

Auth, identity, or token failure — login, token validation, OAuth, SSO broken

"Login issues" | "token validation failed" | OAuth / SSO / IAM

FM → FM-02 • FM-30 • FM-01

RC-11 Hardware Failure — LOW

Physical infrastructure failure — disk, NIC, host, rack, data-center thermal event

"Hardware fault" | "host failure" | "disk failure"; "thermal event"

FM → FM-13 • FM-01

External & Security — 3 RCs

RC-08 Third-Party / Vendor — HIGH

Upstream vendor caused failure — cloud provider, CDN, identity, payment processor

Vendor named verbatim | Upstream status degraded | Resolution tracks upstream

FM → FM-01 • FM-12

RC-10 External Attack — MED

External actors — DDoS, abuse, scraping, credential stuffing, adversarial traffic

"Attack" / "abuse" | "WAF triggered" | Unusual traffic spike

FM → FM-15 • FM-01

RC-12 Security Incident / Breach — MED

Compromise, vulnerability exploitation, or supply-chain breach forcing operational impact

"Security advisory" | Token rotation; CVE | "service taken offline"

FM → FM-16 • FM-12

Data & AI — 2 RCs

RC-09 Data Processing / Pipeline — MED

Ingestion, ETL, replication, queue processing, or backfill failure

"Data delays" | "processing backlog" | "replication lag"; queue-drain

FM → FM-21 • FM-31 • FM-26

RC-13 Model / AI Component — HIGH*

Specific to AI inference, model serving, embedding service, or AI pipeline

Model-version errors | Inference latency after deploy | Specific AI endpoint affected

FM → FM-17 • FM-19 • FM-33

Human & Operational — 3 RCs

RC-15 Other — VAR

Identifiable cause not fitting RC-01–RC-13. Reasoning field MUST specify.

Use sparingly | Cause clearly determinable | Explicitly not RC-01–RC-13

FM → (VARIES)

RC-16 Operational Coordination — LOW

Cross-team handoff failure or process breakdown — explicit disclosure required (narrow scope)

"Teams weren't in sync" | Missed runbook step | Vendor handoff failure

FM → FM-12 • FM-21

RC-17 Operational Action / Operator Error — LOW

Wrong target, scope, or moment — the action itself was the proximate cause

(v0.9)

Operator to wrong env | Emergency change on wrong target | Delete vs. list confusion

FM → FM-09 • FM-26 • RC-16 CO-OCCURS

RETIRED

RC-14

Undetermined — retired in Taxonomy v0.6 → Migrate existing rows to Unclassified · Do not assign to new rows

* RC-13 disclosure: High within AI providers · Low elsewhere

Turn root cause analysis into systemic insight



Pair every FM code with an RC code

At post-incident review, don't stop at what failed — assign the root cause too.

EXAMPLES:

FM-09 (Deploy Regression) + RC-01 (Code Defect) – a defect introduced at deploy time

FM-01 (Cross-Org Cascade) + RC-08 (Third-Party / Vendor) – the upstream vendor caused it

FM-10 (Config Failure) + RC-02 (Config Change) – an undocumented config change triggered the outage

One FM + one RC gives you a complete incident fingerprint.



Check your disclosure confidence

Each RC code carries a confidence badge — High, Med, or Low — based on how explicitly companies disclose this cause type on status pages.

High (RC-01, RC-08) – strong signal, trust the pattern

Med (RC-02, RC-06) – needs confirmation before acting on trends

Low (RC-11) – infer cautiously; under-represented in public data

If your RC distribution is heavily Low-confidence, your postmortems may lack enough detail to surface real patterns.



Spot whether you're fixing symptoms or causes

RC-08 (Third-Party / Vendor) appearing repeatedly alongside RM-42 (Wait for upstream fix) means you're absorbing vendor risk with no structural response.

RC-01 (Code Defect) at high frequency without a matching PREVENT remediation means your review process isn't catching defects before deploy.

The RC + RM pairing is where the action insight lives.



PRACTICAL PROMPT

“What is your most frequent root cause over the last 6 months? Does your team have a PREVENT remediation in place for it?”

From the State of Reliability 2026

The Root Cause Taxonomy is one part of a connected incident-learning framework developed through the analysis of public reliability data.

Failure Mode	What failed?
Root Cause	Why did it fail?
Remediation	What was done about it?
Context Atlas	What information was required to diagnose and act?

Use the framework to create a more consistent language for postmortems, incident trends, and reliability investment.

DOWNLOAD THE FULL FRAMEWORK

FM Cheat Sheet
Failure Mode Taxonomy

RM Cheat Sheet
Remediation Taxonomy

Context Atlas
Diagnostic Context Reference

Download The State of Reliability 2026 full report.

Follow StackGen for the report release and additional reliability research.

stackgen.com/state-of-reliability-2026