



Start the release review from the same code

A frozen source snapshot gives reviewers a common basis even after the branch changes. Scope, coverage and unsupported analysis stay visible.

Source

Repository, branch, commit and cited lines.

Coverage

What ran, skipped, failed or was unsupported.

Question

The release or remediation decision the review must inform.

What changes for management

Reviewers stop debating screenshots and start from the same immutable source and coverage record.

Proof to ask for

Repository, branch, commit, scan identity, supported analysis and visible failures or skips.

Boundary to retain

A fixed snapshot makes source review reproducible; it does not prove runtime behavior.

Outcome: The release discussion begins from one reproducible source and a visible analysis boundary.



Make the finding prove its case

Open the exact source, reproduce or challenge the proposed route and keep missing relationships visible. A source pattern is evidence for review, not proof of runtime exploitability.

Confirmed

The checked evidence supports the claim within scope.

Refuted

Counter-evidence rejects the claim.

Unresolved

The missing check could still change the decision.

What changes for management

The queue becomes a set of claims that can be confirmed, refuted or left explicitly unresolved.

Proof to ask for

Cited lines, validation or replay result, missing relationships and counter-evidence.

Boundary to retain

A source pattern or candidate route does not establish runtime exploitability.

Outcome: The reviewer can explain what the evidence supports and name the check that could change the conclusion.



Turn review into owned engineering work

Connect the evidence, conclusion, uncertainty and next check to the engineer who can act. Bulk assignment organizes work without changing truth or severity.

Reason

Decision, evidence and unresolved assumption.

Owner

Responsible engineer and due condition.

Verify

Fresh evidence required after the change.

What changes for management

The finding reaches engineering with the reason, owner and verification condition attached.

Proof to ask for

Decision rationale, unresolved assumption, due condition and the fresh evidence required after change.

Boundary to retain

Assignment and categorization organize work; they do not change the truth of a finding.

Outcome: Engineering receives a bounded task with a reason, owner and proof condition instead of an isolated alert.



Keep the reason when the code changes

Compare scans of the same repository, distinguish new, persistent and no-longer-matched findings, and review changed identity or coverage before carrying a decision forward.

Compare

Show what changed in source and analysis.

Retain

Keep rationale and audit context.

Decide

Expand, narrow, pause or stop from reproducibility and handoff quality.

What changes for management

A repeat scan begins with what changed while preserving why the earlier decision was made.

Proof to ask for

Source and coverage differences, finding identity, prior rationale and current verification evidence.

Boundary to retain

A no-longer-matched result is not by itself proof that a fix worked.

Outcome: The team can distinguish a verified fix from a moved finding, changed coverage or stale assumption.