



FOR GRC OPERATIONS MANAGERS & COMPLIANCE LEADS

POWERED BY GRACIE AI AGENTS

The Quarterly Control Review Toolkit.

The master checklist, evidence standard and decision framework for running a control review an auditor won't push back on.

23-task checklist

Evidence standard

Status decision matrix

Executive summary template

23 tasks. 4 statuses. One decision log. Six weeks, start to close.

surecloud.com

WHY THE MECHANICS MATTER

A control can pass and still be wrong.

A control that failed on day one and ran uncorrected for 89 days still rates Effective if your review only checks day 90. That's not a testing gap. That's a testing design flaw.

Most quarterly reviews fail quietly, not because the framework is wrong, but because the mechanics underneath it are loose: no named evidence owner, no fixed definition of "sufficient," no gate stopping a team from reviewing before testing is actually done.

This toolkit is the mechanics. Everything here maps to the 4-phase process: Prepare, Test, Review and Decide, Report and Close. Work through it once and you have a repeatable cycle. Work through it every quarter and you have an audit trail that holds up when someone outside your team reads it.

What's inside

1	The cycle at a glance	Four phases, four gates, and the owner accountable for each. Page 3.
2	The 23-task checklist	Every task, grouped by phase, in the order you run them. Page 4.
3	The evidence standard	Three tests evidence must pass, and the method to match each control. Page 5.
4	The status decision matrix	Four statuses, the criteria for each, and the action each forces. Page 6.
5	Executive summary template	Three paragraphs the board can read in three minutes. Page 7.
6	Failure patterns and cadence	Where reviews break, and which controls can't wait 90 days. Pages 8–9.

THE CYCLE AT A GLANCE

Four phases. Four gates. No skipping ahead.

PHASE	WEEKS	OWNER	YOU CAN'T MOVE ON UNTIL...
Prepare	1–2	GRC Operations Manager	Every in-scope control has a named owner and defined evidence requirements
Test	2–4	Control owners & GRC reviewers	Every control has a draft status backed by filed evidence
Review and Decide	5	Compliance Lead	The decision log is signed with final statuses and escalations logged
Report and Close	6	GRC Operations Manager	The executive summary is out and next quarter's calendar is set



SIZING RULE

100–300 controls fits this six-week cycle. Under 100, you can likely close in four weeks. Over 500, build in extra testing weeks rather than compress the standard.

The four gates, in order

1 Prepare Scope, owners, evidence requirements and deadlines fixed before anyone tests.	2 Test Design and operating effectiveness assessed against filed evidence.	3 Review and Decide Statuses confirmed, remediation owned, escalations logged, log signed.	4 Report and Close Reports issued, workpapers filed, next quarter scheduled.
---	--	--	--

2

WORK IT TOP TO BOTTOM

The 23-task checklist.

Phase 1 — Prepare

WEEKS 1–2 · GRC OPERATIONS MANAGER

- ☐ Retire inactive controls from the library
- ☐ Assign named owners with current contact details to every in-scope control
- ☐ Confirm framework mappings are current
- ☐ Set testing frequency per control (quarterly / annual / continuous)
- ☐ Log regulatory deadlines and audit windows falling within 90 days
- ☐ Note every control change since last quarter
- ☐ Issue evidence templates with collection deadlines
- ☐ Brief owners on what counts as acceptable evidence

Phase 2 — Test

WEEKS 2–4 · CONTROL OWNERS & GRC REVIEWERS

- ☐ Collect evidence against the issued templates
- ☐ Evaluate design effectiveness: can this control, as written, mitigate the risk?
- ☐ Evaluate operating effectiveness: did it run as designed for the full period?
- ☐ Apply the correct testing method for each control (see page 5)
- ☐ Document the sampling methodology used
- ☐ Assign a draft status to every control

Phase 3 — Review and Decide

WEEK 5 · COMPLIANCE LEAD

- ☐ Confirm or adjust every draft status
- ☐ Agree remediation owner and deadline for each Partially Effective control
- ☐ Escalate every Ineffective control to the risk register within 5 business days
- ☐ Scan results for systemic patterns across owners or business units
- ☐ Sign the decision log

Phase 4 — Report and Close

WEEK 6 · GRC OPERATIONS MANAGER

- ☐ Produce the operational report (full detail, by status)
- ☐ Produce the 3-paragraph executive summary
- ☐ File testing workpapers in the evidence repository, labelled by quarter
- ☐ Log remediation actions with owners in the risk/action system
- ☐ Confirm next quarter's calendar: start date, deadline, review meeting

SCOPE RULE

Any control changed since the last review, or mapped to a regulatory obligation due inside 90 days, is in scope every quarter. No exceptions, no carry-forward.

3

THE EVIDENCE STANDARD

Evidence that survives an audit six months later.

Before you file anything as evidence, it has to answer three questions. If it doesn't, the status can't be Effective, whatever the control owner says.

01 · PERIOD COVERAGE**Does it span the full quarter, first working day to last?**

Not a screenshot from collection day.

02 · OPERATIONAL PROOF**Does it show the control actually executed?**

Not that it exists, or that someone attests to it.

03 · INDEPENDENT VERIFICATION**Is it system-generated?**

Owner-attested evidence alone is **not sufficient** for anything above Partially Effective.

Match the method to the control

METHOD	BEST FOR	WHAT YOU FILE
Inspection	Policy & configuration controls	Documents, screenshots, config exports
Observation	Process-based workflows	Meeting records, approval logs
Enquiry	Judgment-dependent controls	Interview notes, attestations
Re-performance	High-risk automated controls	Independent re-runs, comparisons
Automated testing	Continuous technical controls	System logs, API outputs, alerts



The higher the control risk, the more independent the evidence needs to be. **Enquiry alone never clears a high-risk control.**

4

THE STATUS DECISION MATRIX

Four statuses. Four required actions. No fifth option.

Effective

CRITERIA

Full-period evidence. Operated as designed. No exceptions.

ACTION

Document the rationale. Close.

Partially Effective

CRITERIA

Evidence incomplete, exceptions unresolved, or operation inconsistent.

ACTION

Named remediation owner. Fixed deadline.

Ineffective

CRITERIA

Control departed from design, or failed to mitigate the risk it exists for.

ACTION

Escalate to the risk register within 5 business days.
Agree a remediation plan. Re-test before next quarter.

Not Tested

CRITERIA

Evidence never submitted, or insufficient to evaluate.

ACTION

Identify the cause — ownership gap, evidence gap, or scoping error — then prioritise for next quarter if a regulatory obligation is affected.

DECISION RULE — PUT THIS ON THE WALL

"If an external auditor reading the evidence would question whether the control operated as designed throughout the period, the status is Partially Effective. Not Effective."

5

EXECUTIVE SUMMARY TEMPLATE

What the board needs in three minutes.

Three paragraphs. Nothing more. If your board can't tell whether the control environment is improving and what needs fixing, cut it back.

1

Paragraph 1 — Current state

"This quarter, [X]% of controls tested Effective, versus [X]% last quarter. [Trending up / down / flat]. [One sentence on what's driving the change, if anything is]."

2

Paragraph 2 — Material risks

Bullet every Ineffective control linked to a regulatory obligation with a live deadline. One line each: control, obligation, deadline, remediation status.

3

Paragraph 3 — Decisions needed

State explicitly what you're asking for. Budget. An escalation. A resourcing call. Don't bury the ask in narrative.

**KEEP THE DETAIL SOMEWHERE ELSE**

This is the operational report's translation layer, not a shorter version of it. Keep the full detail — by status, by owner, by re-test requirement — in the operational report for the working team.



WHERE REVIEWS ACTUALLY BREAK

Four failure patterns, and the fix for each.

01**Evidence collection delays**

Cause: Vague requests, no enforced deadline, owners who were never briefed.

Fix: Standard template per control type. A tracking log everyone can see.

02**Internal-to-external misalignment**

Cause: Testing quietly turns into "is the paperwork good" instead of "did the control work."

Fix: Define operating effectiveness per control up front. Re-perform a sample every quarter, not just when something looks wrong.

03**Incomplete remediation**

Cause: Actions get logged with no owner, no escalation path, no consequence.

Fix: Move actions into a system with reminders. Check progress mid-quarter, not just at the next review.

04**Risk register disconnection**

Cause: A control fails in the review record and never reaches the risk register.

Fix: A formal handoff from decision log to risk register, with a 5-day SLA for anything Ineffective.



WHEN QUARTERLY ISN'T ENOUGH

Some controls can't wait 90 days to be checked.

A quarterly cycle is right for controls that involve human judgement and change slowly: policy reviews, access certifications, vendor assessments, management attestations.

It's the wrong cadence for controls that drift between snapshots: log monitoring, vulnerability scanning, encryption status, backup integrity. Those need to be watched continuously, not sampled four times a year.

What changes with continuous controls monitoring

DIMENSION	MANUAL QUARTERLY ONLY	WITH CONTINUOUS MONITORING
Evidence collection	Manual, owners chased for screenshots	Automated, built throughout the quarter
Review meeting focus	Evaluating whether evidence is even complete	Reviewing flagged exceptions only
Regulatory evidencing	A point-in-time snapshot, with gaps	A continuous record spanning the full period

75%

Organisations pairing continuous controls monitoring with a quarterly review cycle report a **75% reduction in audit preparation time.**

 GRACIE AI AGENTS

Start next quarter with a complete testing record, not a scramble.

Gracie AI Agents run evidence collection and control performance analysis continuously, so the quarterly review starts with evidence already filed, not a chase for screenshots in week three.

23

tasks, from scoping to close

6

weeks, start to signed decision log

75%

less audit preparation time with continuous monitoring

Book a demo.

See Gracie collect evidence against your own control library, then get pricing for your GRC estate.

[Book a demo →](#)

Get pricing for your GRC estate — surecloud.com



SureCloud. Founded London, 2006. Your Business Assured.

surecloud.com