BUSINESS ANALYSIS CASE STUDY

Audit-Ready Every Day

Turning SOC compliance for client-facing reports from an audit-week scramble into a daily habit

Snapshot	
Role	Reporting Coordinator — ticketing-platform co-administrator and the team's SOC subject-matter expert; on loan to Internal Audit during the audit
Organization	Global relocation management company (corporate relocation services)
Scope	The reporting team's two SOC controls over client-facing report changes — development, testing, edits and release to production — within the company-wide SOC 1 and SOC 2 audits
Tools	SmartQ (Jira-equivalent ticketing and workflow platform), BMC Remedyforce, Excel
Stakeholders	Report owners (analysts), developers, senior developers, my Director, Internal Audit, external auditors

2
SOC controls owned by the reporting team

7
checks on every SOC ticket

Daily
review, with same-day follow-up

54,000
requests a year on the platform

EXECUTIVE SUMMARY

Within the company's SOC 1 and SOC 2 audits, our reporting team was responsible for two controls covering every client-facing report we built or changed. To pass, each change had to show a clear owner, testing in a separate environment, the right approvals, and a release to production by a second, senior developer — with dates proving it all happened in order. When auditors pulled their sample, any missing piece meant rework under pressure.

I made compliance a **daily check instead of an audit-week event.** Using compliance filters I built in our ticketing platform, I reviewed every SOC ticket against seven control checks each day and sent the owners a gap report the same day. Each owner fixed their own ticket while the details were fresh. The records stayed complete all year, and audit testing cycles ran smoothly — I don't recall a single issue with the process.

1 THE PROBLEM

Report requests, development and approvals lived in the team's ticketing platform, handling about 54,000 requests a year. For SOC audits, evidence was exported from that platform and uploaded to a separate audit system — a manual hand-off my Director orchestrated.

The risk sat in the tickets themselves. A missing tag, a skipped approval or a date out of order was easy to miss in the moment and hard to fix months later, when an auditor pulled that ticket into the sample.

What was at stake

- **Late discovery.** Gaps could stay hidden until audit preparation, when they're hardest to correct.
- **Audit-week pressure.** Cleanup concentrated right before fieldwork pulled analysts and developers off their work.
- **Control failures.** A single ticket released without the right approvals is an audit exception.
- **Client trust.** These reports carried client information; the controls exist to protect it.

2 SCOPE, GOALS AND CONSTRAINTS

Problem statement: Control gaps on SOC-scoped report tickets were found late — often during audit preparation — creating rework and audit risk.

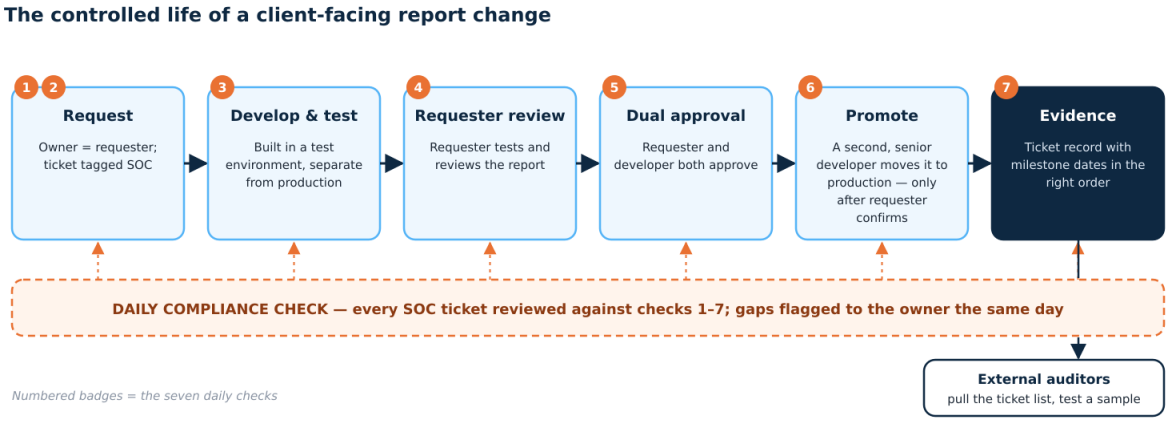
Area	Definition
Goal	Every SOC ticket complete and audit-ready at all times, not just before fieldwork.
In scope	Client-facing report changes: development, testing, edits and release to production.
Out of scope	The audit system upload process; one-time custom reports not used in production.
Constraints	No new tools or budget; the fix had to work inside the existing ticketing platform and team routines.
Success measures	Gaps caught and fixed within days; smooth auditor sample testing; little or no pre-audit cleanup.

3 STAKEHOLDERS

Stakeholder	What they needed	What they worried about
External auditors	A complete ticket list for the period, and evidence that controls worked on their sample	Missing approvals, dates out of order, weak segregation of duties
Internal Audit	Control owners who were ready before fieldwork	Surprises during testing
My Director	Clean evidence for the audit hand-off	Last-minute cleanup across the team
Report owners (analysts)	Clear, simple fixes on their own tickets	Being pulled away from client work at audit time
Developers & senior developers	Know a ticket is approved before release	Releasing something that wasn't signed off

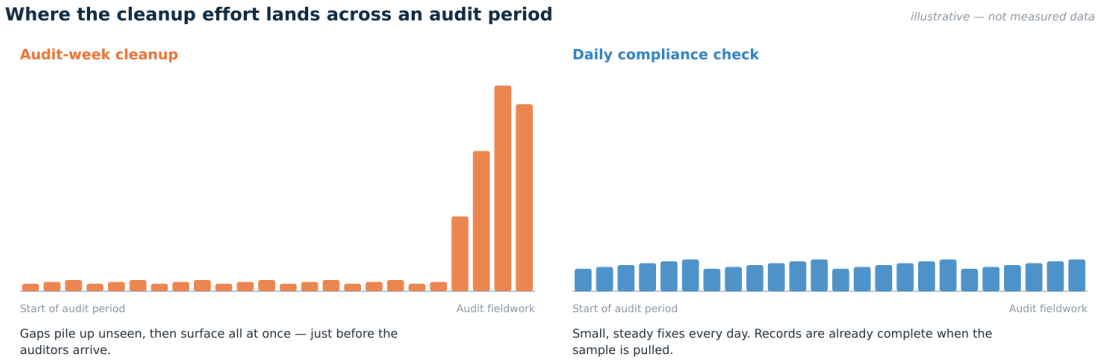
4 THE CONTROL FRAMEWORK

The team's two controls were tested through seven checks on every SOC-tagged ticket. These are standard change-management practices, described here in general terms.



#	Check	What it proves
1	Ownership	The requester is the owner of the report.
2	Scope tag	Every client-facing report is tagged SOC.
3	Environment separation	Development and testing happen outside production.
4	Requester review	The owner tests and reviews the report before release.
5	Dual approval	Both the requester and the developer approve.
6	Segregation of duties	A second, senior developer releases to production — only after the requester confirms.
7	Milestone dates	Dates show every step happened, in the right order.

5 FROM AUDIT-WEEK CLEANUP TO A DAILY HABIT



Illustrative shape of the change, not measured data.

Need	Audit-week cleanup	Daily compliance check
Finding gaps	During audit preparation	The same day
Fixing gaps	Months after the work, from memory	While the details are fresh
Who fixes	Whoever is available at audit time	The ticket's own analyst or developer
Auditor sample	Rework on pulled tickets	Records already complete

6 THE SOLUTION: A DAILY GAP REPORT

Each day, compliance filters I built in the ticketing platform pulled the SOC tickets and their key fields. I reviewed every ticket against the seven checks and sent an **Excel gap report** to the analysts and developers, with each gap flagged next to the owner who needed to fix it. Owners corrected their own tickets in the platform — keeping accountability where the work happened.

Daily SOC gap report

illustrative mock-up — invented ticket data

Ticket	Report owner	SOC tag	Tested in test env	Requester approval	Developer approval	Senior dev promoted	Dates in order	Action
RQ-1042	Analyst A	✓	✓	✓	✓	✓	✓	Complete
RQ-1047	Analyst B	✗	✓	✓	✓	✓	✓	**Add SOC tag**
RQ-1051	Analyst C	✓	✓	✗	✓	—	✓	**Get requester approval**
RQ-1058	Analyst A	✓	✓	✓	✓	✓	✗	**Fix milestone date**
RQ-1063	Analyst D	✓	✓	✓	✓	✓	✓	Complete

Sent daily to the analysts and developers; each owner fixes their own ticket in the ticketing platform.

Illustrative mock-up recreated for this case study, with invented ticket data.

Sample requirements (reconstructed)

User story	Acceptance criteria
As an external auditor, I want a complete list of SOC tickets for the audit period, so I can select a sample and test the controls.	The export covers the full period, with owner, tag, approvals and milestone dates for each ticket.
As the team's compliance lead, I want a daily list of SOC tickets missing a required element, so gaps are fixed within days, not at audit time.	Each of the seven checks is evaluated; tickets with gaps are flagged by type and owner.
As a report owner, I want to see exactly what's missing on my ticket, so I can fix it quickly.	The gap report names the ticket, the missing check and the action needed.
As a senior developer, I want to release only reports with requester approval recorded, so segregation of duties holds.	Tickets without recorded approval are flagged before release.

7 TRADE-OFFS AND RISKS

Option	Pros	Cons	Decision
Clean up before each audit	No daily effort	Late discovery, rework, audit risk	Rejected
Daily check with a gap report	No new tools; starts right away; clear ownership	Manual review and follow-up every day	Chosen
System-enforced controls	Gaps blocked automatically	Needs configuration and development time	Recommended next step

Risks and how they were handled

- **Flags ignored.** Each owner fixed their own ticket, and the report came every day — gaps couldn't quietly age.
- **Release without approval.** The segregation-of-duties check flagged any ticket released before the requester confirmed.

- **Manual effort.** Filters did the data pull; review and follow-up stayed a short daily routine.

8 RESULTS

- **Every SOC ticket checked daily** against seven controls, with gaps routed to the owner the same day.
- **Smooth audit testing cycles:** records were complete when auditors pulled their sample, and I don't recall any issues with the process.
- **Less pre-audit cleanup,** because gaps were fixed as they happened.
- **Trusted as the team's SOC representative:** represented the reporting team for its two controls in the company-wide audit, and went on loan to Internal Audit during the audit.

9 RECOMMENDATIONS AND WHAT I LEARNED

What I'd recommend next

- **Let the system enforce the checks.** Required fields and workflow rules that block release without approvals would turn a daily review into an exception report.
- **Capture whole processes in the system.** The company's own next step — recording processes like client onboarding so the system can export evidence for sampling — is the right direction.
- **Bring recurring business reviews into scope.** At the time, business reviews were handled outside the ticketing platform, yet they hold the most sensitive information we have on a client. Recurring reviews belong in the controlled process; truly one-time custom reports can stay out of the audit sample.

What I learned

Compliance is a habit, not an event. A simple daily routine — clear checks, same-day flags, and owners fixing their own work — can keep an audit calm even before full automation. And good controls start with asking what's actually sensitive, not just what's been labeled that way.

Described in general terms. Figures are from memory and the author's resume; visuals are illustrative and contain no confidential company, client or system data.