EACG
Enterprise Architecture Consulting Group

SECURITY DIALOGUES
No. 9 · 2 October 2026
Marcus Hale (PSIRT) · Tess Calder (red team) · Jessy Lang

Compliant vs. Secure

Seven ways a clean audit misleads, and what to do about each

A company passes its SOC 2 renewal with zero findings and is breached ten weeks later, through a control the report had just certified. The report was accurate: it was a photograph of one Tuesday. Keep the certificate, and stop treating the photograph as a live feed.

SNAPSHOT ASSURANCE
A dated photograph of a control, read as a live fact.

1. Which Tuesday is it?

2. What is out of scope?

3. Who keeps it true?

WHERE THE GAP OPENS AND HOW TO CLOSE IT

1	**True on the day** The control was real at the audit and false by the time it mattered.	A contractor account came in through a new onboarding tool nobody had connected to the access review. Systems change constantly, audits do not. Give somebody the job of keeping the certified control true after the audit ends. In this story that job belonged to nobody.
2	**The scope line nobody reads** What was never inside the boundary stays unprotected.	Read the scope statement first: it is usually the most important sentence in the report. An ISO 27001 scope around corporate IT left the factory floor outside, and a vendor remote-access box was the way in. Attackers read your scope for what it excludes. So should you.
3	**Stitched compliance** Plausible documents, never reconciled with each other.	Check the seams. Were the measures derived from the objectives, or approved two hours after them? Is every role mapped to a named person, team or system access? Ask who that is, today. A tender office confirms documents arrived, not that they describe an operated system.
4	**Controls that work on paper** The policy is real, the practice may not be.	A thirty-day patch policy can sit next to a box unpatched for over a year, because the auditor sampled tickets, not the fleet. Sampling stops being representative as the company grows. Measure the real fleet, not the five tickets someone pulled.
5	**The certificate as alibi** "We were compliant at the time" closes the conversation.	The certificate is good evidence for a lawyer and terrible evidence for a postmortem. In a retro, answer the engineering question, not only the liability question.
6	**A certified PSIRT** Certified and actually staffed are two different claims.	Handling vulnerabilities is easy to certify and hard to keep true, because it reacts to things nobody can schedule. Run it as a standing, always-on function. The honest test is what happened the last time a report landed at two in the morning.
7	**One word for three things** ISO 27001, SOC 2 and the CRA go wrong in different ways.	ISO 27001 is a snapshot of your management system, SOC 2 a snapshot of specific controls running. The Cyber Resilience Act is a standing legal obligation across a product's support life: staffed in March and unstaffed by August is no longer a stale audit, it may be a live requirement unmet.

THREE PRACTICES THAT CLOSE THE GAP

Monitor continuously
Decouple verification from the audit calendar: automated daily or weekly checks that the access review ran and the patch SLA is met across the real fleet. For a mid-size client, roughly two extra headcount and a platform, a few hundred thousand a year.

Review scope on a trigger
Whenever a new system, vendor connection or onboarding tool is added, someone asks whether it falls inside or outside the certified boundary, before it becomes the exception nobody scoped.

Keep an owned inventory
An inventory kept current, with an owner, instead of a document produced once and framed in a lobby. Check more often than the thing you trust was built to update.

Listen to the episode
Compliant vs. Secure and the rest of the series.
eacg.de
/en/podcast/s09-snapshot-assurance

Digital Product Design
From the first idea to a viable first release.
eacg.de
/en/consulting/digital-products

PSIRT Services
Intake, assess and disclose vulnerabilities, built or run as a service.
eacg.de
/en/consulting/psirt

© 2026 EACG GmbH