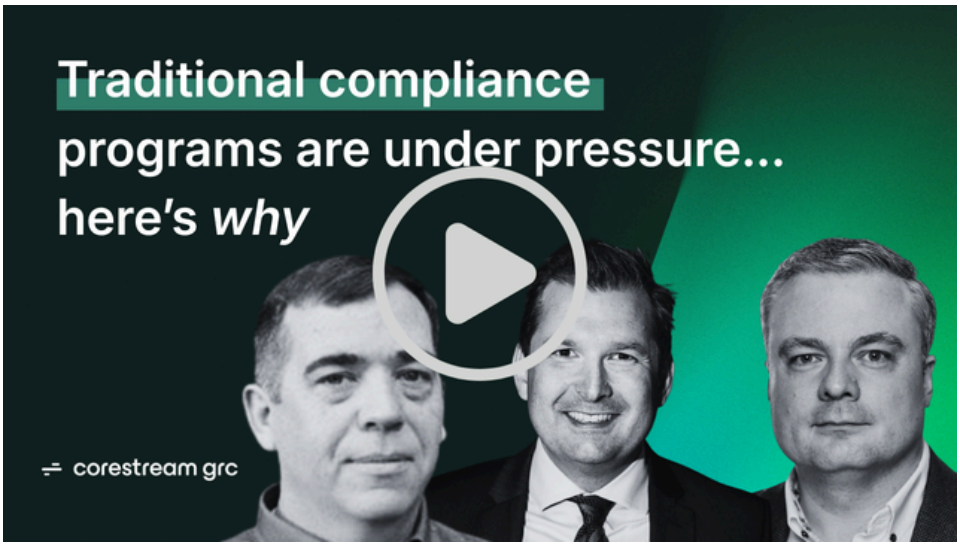
axiom
corestream grc

Beyond the RAG chart: effective GRC reporting at board-level

Introduction: from static snapshot to compliance story

Picture a typical quarterly board pack. The compliance slide shows 98% green, no red flags and no open questions, so the board moves on within a few minutes. Then, months later, a control failure that had in fact been recurring quietly for a year surfaces as a genuine incident, and the first question anyone asks is: how did the board not know? The uncomfortable answer is usually that the board did know, in a narrow sense. It had seen the green tile every quarter. I**t had simply never seen the story behind it.**

On the recent CoreStream GRC webinar, The Modern CISO's Compliance Stack, host Lucy Montague (CoreStream GRC's Head of Marketing) summarized the issue: **compliance reporting needs to move away from a static snapshot, toward "narrative and story and trends over time, and lessons learned.**" Because boards don't just want a number, they want to understand what it means.



Most compliance and risk reporting still doesn't work that way. It's built to reassure, not to inform, filled with the kind of "100 green, amber, red tiles" that CoreStream GRC's GRC Strategy Director Paul Cadwallader has warned looks tidy but says almost nothing about whether risk is actually being reduced. As CoreStream GRC's own guide to building a value-based compliance culture says: **"Reporting becomes theater. Dashboards look perfect. Risks look green. Everyone knows it is not real."**

This guide explores what changes when reporting stops being theater made up of vanity metrics: what to measure, why this is a global shift, and how AI-powered platforms are starting to make that story easier to tell.

Why most compliance reporting fails the board

The most common failure isn't a lack of data. It's the wrong data, measured for the wrong reason. Speaking on CoreStream GRC's webinar about the early warning signs of a checkbox compliance program, Paul Cadwallader pointed to **"metrics focused on activity, and not outcomes"**: tracking the percentage of policies reviewed or training completion rates, rather than risk incidents avoided or time to remediate control failures. Board reporting built on that kind of data ends up, in his words, **"backwards-looking and reassuring by design,"** with little narrative on residual risk appetite or emerging exposure.

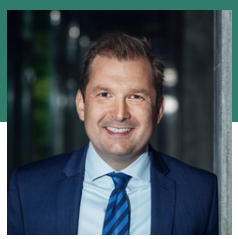
In the experience of Tom Cornelius, founder of the Secure Controls Framework:

> *"The board wants to know, are we secure, compliant and resilient, and be able to then answer that question with granular control-level evidence."*
>
> Tom Cornelius, Founder of the Secure Controls Framework & Senior Partner at ComplianceForge

That's a harder question to answer with an activity-based dashboard, because it asks for **evidence that holds up over time**, not a checklist completed once.

There's also a third failure mode, less about what's measured than about what gets read ... or not. Anders Søborg, co-founder of SANNOS, describes the problem with third-party evidence:

> *"A lot of companies get tons of SOC 2 reports from their critical IT vendors. None of them have time to review that, so do they really understand how the risk they've outsourced is managed?"*
>
> Anders Søborg, Co-Founder, SANNOS



A board pack stuffed with unread evidence isn't meaningfully different from one with none. It just **feels safer.**

Research published by Corporate Board Member, with EY's Center for Board Matters, a Q2 2026 survey of nearly 150 US public company directors, backs this up. It found that:

- **Only 32%** of directors say **reporting on emerging risks has improved,** even though 60% say their board now spends more time on risk oversight.
- **Just 25%** say their **board regularly receives reporting on concentration or dependency risk**, such as overreliance on key vendors.

A board that only sees a lagging snapshot, or a pile of evidence nobody reviewed, they can't tell the difference between a program that's improving and one that's quietly getting worse. That's precisely **why regulators in multiple jurisdictions are now asking boards to show their working.**

The global drive towards compliance trend reporting

The demand for a defensible trend rather than a compliance snapshot, is showing up in board-level regulation around the world.

In the US, SEC rules require **public companies to disclose in their annual report how the board oversees cybersecurity risk, and to report material incidents within 4 business days**, a shift from an annual box-tick to continuous, evidenced oversight.

The EU's Digital Operational Resilience Act requires an **ongoing ICT risk management framework covering resilience testing, incident reporting and third-party risk**, not a one-off assessment.

Australia's CPS 230 goes further again, **requiring banks and insurers to set board-approved tolerance levels for their critical operations and monitor performance against them on an ongoing basis.**

And in the UK, Provision 29 of the Corporate Governance Code requires boards to declare that **material controls were effective across the year and explain how they know.** CoreStream GRC has set out what that means for control evidence elsewhere. It's one more example of the same pattern: wherever the regulation sits, boards are increasingly expected to show a trend, not a snapshot.

What does effective GRC reporting actually measure?

Asked on CoreStream GRC's webinar what single metric or dashboard view a CISO should take to the board to prove a new compliance program is working, Paul Cadwallader didn't suggest a compliance percentage. He recommended a **trend.**

> *"If I had to pick one view, I'd look at it as a **risk exposure trend versus control effectiveness,** and not a point-in-time compliance score... The most defensible metric is time to remediate, weighted by risk severity: how long Critical versus Low findings sit open, trended over quarters. That tells the board more than 100 green, amber, red tiles, because it shows the organization where they actually close risk, not just identify it."*
>
> Paul Cadwallader, GRC Strategy Director, CoreStream GRC

He paired that with a second signal worth watching: the **percentage of control failures with a recurring root cause.** This answers a different question, **"are we fixing things, or are we learning?"**

And he added an important caveat: **a clean remediation trend is only credible if it's backed by finding-source diversity**, meaning issues surfaced through internal audit, external audit, self-identified reviews and incidents, not just one narrow channel repeating the same result.

CoreStream GRC's own guide to building a value-based compliance culture sets out a similar structure in practical form, splitting metrics into two buckets rather than one long list. **"Execution and proof" covers the percentage of key controls with evidence on time, the time to produce an audit-ready evidence pack, and exception volume. "Confidence and trust" covers the repeat findings trend, escalation health, and, tellingly, leadership confidence in reporting, or "do they believe the green?"**

That last measure matters more than you'd imagine. EY's Global Integrity Report 2024 found that:

- **38%** of respondents globally said they would **be prepared to behave unethically in one or more ways to improve their own career progression.** But, the percentage rises to...
- **51%** among senior management, and
- **67%** among board members.

A dashboard is only as trustworthy as the culture reporting into it.

The same guide recommends a matching rhythm: trending issues and exceptions reviewed monthly, repeat findings and control failures reviewed quarterly, and a full program effectiveness and evidence-readiness review annually, so each layer feeds the next and a **genuine multi-year trend** can build up rather than resetting every quarter.

How AI-powered risk and compliance platforms make the narrative possible

This isn’t just a problem of reporting design. It’s also a capacity problem, and that's where Anders Søborg's SOC 2 complaint and Paul Cadwallader's own prediction about the future of board reporting meet. **“Board reporting … will be a live dashboard, not a quarterly pack,”** Cadwallader said later in the same webinar, adding that compliance teams will shift from manual evidence gathering toward being **“compliance engineers… looking at trending, building or validating automated pipelines from AI and Agentic, pulling it all together.”**

CoreStream GRC's own product roadmap is built around that shift. Its CoreStream GRC x SANNOS x SCF solution, built on the Secure Controls Framework's library of more than 1,400 controls across 33 domains, lets a compliance team **assess a control environment once and map it automatically across 200+ laws, regulations and frameworks including NIST, ISO 27001, DORA and NIS2, cutting framework assessment time by 88%** according to CoreStream GRC's own client data.

The aim is to **“empower GRC teams to move from point-in-time snapshots to a live compliance posture with structured evidence traceability and audit-ready outputs,”** always available for regulators, auditors, boards and employees to review.

The same logic applies to third-party evidence, the SOC 2 report pile Søborg was describing. CoreStream GRC's third-party risk solution, built with SANNOS and Xapien, **replaces one-time vendor questionnaires with continuous monitoring and automated evidence review, reviewing more than 100 pages of vendor evidence in 1 or 2 minutes and shortening onboarding cycles by up to 70%.** GRC analyst Michael Rasmussen has argued the real value isn't just speed:

"The value is not simply in improved efficiency, but in the broader impact on the ***effectiveness*** *and* ***agility*** *of the GRC program... the* ***greater value*** *is in the added depth, precision, and quality of insight that can support* ***better decisions****."*

Michael Rasmussen,
GRC Analyst & Pundit,
GRC 20/20 Research

Cadwallader's caveat on the webinar was that a **clean remediation trend is only credible if it's backed by finding-source diversity**, evidence pulled from internal audit, external audit, self-identified reviews and incidents, not one narrow channel. The depth, precision and quality of AI-powered evidence review makes that diversity practical to **maintain at pace**, rather than being a burden that quietly gets dropped once the reporting deadline passes.

Moving GRC from flat dashboard to action-enabled storyboard

A static metric tells the board little. It needs **“narrative and story and trends over time.”**

> “We don't manage compliance by counting controls, we manage it by **how fast we close the gap between a risk being found and the risk being fixed.”**
>
> Paul Cadwallader, GRC Strategy Director, CoreStream GRC

That focus moves compliance from a cost-center conversation to a risk-velocity conversation, and one with which the board will engage.

Doing that well means resisting the temptation to report on a single quarter in isolation. Cadwallader's advice on the webinar was to **present board metrics as a 2-3 year trend: “Boards care about trajectory and risk appetite alignment, not what's going on in the noise this month.”**

That **trajectory-first approach** is what regulators are now expecting boards to demonstrate.

Conclusion: build the compliance report you'd want to defend

The test for any piece of GRC reporting is simple: could the **person presenting it defend every line if a board member asked "how do you know?"** A static, all-green dashboard usually can't survive that question. A trend line built on time-to-remediate, root-cause recurrence and finding-source diversity, reported on a steady monthly and quarterly rhythm and framed as a story rather than a scorecard, can.

That is what effective GRC reporting actually looks like: not more data, but **better-chosen data, gathered continuously** rather than assembled from scratch each quarter, and **presented as a trajectory a board can question, challenge and ultimately trust.**

If your board reporting still reads as static rather than story, CoreStream GRC can help you rebuild it around the metrics that matter.

Book a workshop to review your current reporting model, or request a demo to see how CoreStream GRC's SANNOS x SCF and SANNOS x Xapien solutions turn **scattered compliance and vendor evidence into the kind of continuous, board-ready trend reporting this guide describes.**

Book a workshop **Request a demo**

axiom
corestream grc

For more information please contact:

Email us to book your demo:
demo@corestreamgrc.com

corestreamgrc.com

Book a demo

Book a workshop

Follow us on LinkedIn