ELDR

GROUP INC. · STRATEGY · TECHNOLOGY · INTELLIGENCE

WHITEPAPER

CYBERSECURITY

The CISO's Documentation Problem

CISOs are increasingly held personally accountable for security posture. The gap between the security program that exists and the one that is documented is where that accountability becomes exposure.

BY **Richard Jones Onyeneho**

March 2026 · 12 MIN READ · ELDR INTELLIGENCE

CYBERSECURITY · ELDR INTELLIGENCE

The CISO's Documentation Problem

CISOs are increasingly held personally accountable for security posture. The gap between the security program that exists and the one that is documented is where that accountability becomes exposure.

A Chief Information Security Officer is sitting across from a federal regulator, two months after a material security incident at a financial services firm. The investigation is going to look at what controls were in place, what evidence exists that those controls were operating as designed, and what the CISO knew or should have known. The CISO is reasonably certain — based on a career spent building security programs — that the controls were in place and operating. The CISO is much less certain that the documentation will demonstrate it. This uncertainty is, in our experience, the dominant operational anxiety of the modern CISO role.

The conversation about CISO accountability has shifted materially over the past five years, and most security programs have not adjusted. The shift is not, primarily, that CISOs are now held responsible for incidents — they always were. The shift is that they are now held personally accountable in ways that have specific legal and financial consequences. The SEC's enforcement actions, the SolarWinds litigation, the regulatory expectations baked into critical infrastructure designations, and the fiduciary expectations now placed on security leadership have collectively changed the operating environment for the CISO role.

What has not changed, in most organisations, is the documentation infrastructure that determines whether a CISO can demonstrate, after the fact, that the security program was operating as designed. The gap between the program that exists and the documentation that proves it exists is where personal accountability becomes personal exposure. This is the CISO's documentation problem, and it is the most consequential operational issue in modern security leadership.

What the regulators *and litigators* actually want

To understand the documentation problem precisely, it helps to start with what regulators and litigators are actually looking for when they investigate a security incident or program failure. They are not looking for proof that the program was perfect. They know — and the case law supports — that no program is perfect,

that breaches happen to mature programs, and that the standard of care is reasonableness, not perfection.

What they are looking for is evidence that the security program was operating as a deliberate, governed, documented function. Specifically, they look for:

01. **Risk identification and acceptance.** Did the organisation identify the risks relevant to its environment? Did it document those risks? Did it make explicit decisions about which risks to mitigate, accept, transfer, or avoid? Are those decisions traceable to the governance structures that should have made them?

02. **Control design and implementation.** Were controls designed in response to the identified risks? Were they implemented? Is there documentation of how they were implemented, who owns them, what dependencies they have on other controls or systems?

03. **Operational evidence.** Did the controls operate as designed during the relevant period? Is there evidence — logs, records, attestations, automated tests — that supports the claim that they did? If they failed, was the failure detected, and was the response appropriate?

04. **Governance and oversight.** Was there appropriate governance over the security program? Were decisions escalated to the right level? Was the board informed? Were the business owners aware of risks they had implicitly accepted?

05. **Continuous improvement.** Was the program responsive to changes — new threats, new technologies, new business contexts? Did it adapt deliberately, or did it drift?

None of this is exotic. Every mature security framework — NIST CSF, ISO 27001, SOC 2, the various sectoral frameworks — describes these expectations explicitly. What is exotic, in our experience, is a security program that can produce all of this evidence on demand, in coherent form, traceable to specific decisions and specific accountabilities.

The two security programs

What we have come to recognise, working with security leaders across regulated and unregulated sectors, is that most organisations have two security programs operating simultaneously, and the gap between them is the CISO's exposure.

The first program is the operational security program. This is what the security team actually does — the controls they implement, the incidents they respond to, the threats they monitor, the assessments they perform. This program is generally competent. The people running it are generally professional. The technology is generally appropriate. The investment is generally reasonable.

The second program is the documented security program. This is what an investigator, regulator, auditor, or litigator could reconstruct from the documentation if they were dropped into the organisation tomorrow. It includes the policies, procedures, standards, control descriptions, risk registers, audit reports, incident records, and governance artefacts that exist in the organisation's documented form.

In mature organisations, these two programs converge. The documented program is a faithful representation of the operational program. In immature organisations — and, in our experience, most organisations are immature on this dimension — they diverge. The operational program is generally better than the documentation suggests. Things happen that are not recorded. Decisions are made that are not memorialised. Controls are operating that are not formally specified. The team knows. The documentation does not.

> *""CISOs are increasingly held personally accountable for security posture. The gap between the security program that exists and the one that is documented is where that accountability becomes exposure.""*

This divergence is, structurally, the CISO's documentation problem. When something goes wrong — when an incident occurs, when a regulator opens an inquiry, when litigation is filed — the question is not what the operational program looked like. It is what the documented program demonstrates. The gap between the two is where the CISO is exposed.

Why the gap exists

The gap between operational and documented security programs is not a function of incompetence. It is a function of three structural pressures that bear on every security organisation we have analysed.

The first pressure is the incident-response orientation of security culture. Security teams are, fundamentally, oriented to the prevention and response of incidents. The work that gets done first, and best, is the work that closes vulnerabilities, blocks attacks, and contains breaches. Documentation work is, in this cultural framing, a secondary activity that happens when there is time. There is rarely time.

The second pressure is the staffing model of most security organisations. Security teams are typically staffed with technical professionals — analysts, engineers, architects — whose comparative advantage is in the technical work of security. Documentation work requires a different skill set: the ability to structure information, write clearly for non-technical readers, maintain consistency across artefacts, and integrate documentation into operational workflows. Few security teams are staffed to produce this work to the standard their accountability environment increasingly requires.

The third pressure is the tooling environment most security teams operate in. Security tools are generally excellent at producing operational data — alerts, logs, scans, reports. They are generally poor at producing documentation that is structured for the audiences that documentation is meant to serve. Translating between operational data and audit-ready documentation is, in most organisations, manual labour performed under time pressure when an audit or investigation arrives. The result is documentation that is rushed, incomplete, and inconsistent — exactly the kind of documentation that produces findings.

What closing the gap actually looks like

Closing the gap between the operational security program and the documented security program is not, primarily, a documentation problem. It is an architectural problem. The organisations that have closed it — and a small number have — have made deliberate choices about how documentation integrates with operational reality.

The first architectural choice is documentation as a structural component of operations, not as an artefact produced separately. This means that key operational events — control implementations, risk acceptances, incident responses, governance decisions — produce documentation as a by-product of the event itself, not as a separate exercise. Modern Docs-as-Code architectures support this, but the architectural choice precedes the tooling.

The second choice is the explicit ownership of documentation within the security organisation. Mature security programs have documentation owners — sometimes a Documentation Manager, sometimes a Security Architecture function, sometimes a Compliance Documentation team — whose specific responsibility is the integrity, currency, and consistency of the documented security program. This is rare, but it is the difference between programs whose documentation drifts and programs whose documentation tracks operational reality.

The third choice is the integration of documentation with the governance functions that consume it. The risk committee, the audit committee, the board's oversight responsibilities — all of these depend on documentation. Programs whose documentation feeds these governance functions cleanly produce documentation that the governance functions actually find useful. Programs whose documentation is produced separately for audit purposes find that the documentation is treated as a compliance exercise rather than a management resource.

The CISO's choice

The CISO's documentation problem is not new. What is new is the personal consequence of leaving it unsolved. In an environment where the SEC is willing to charge CISOs personally, where regulators are

willing to issue personal directives, and where boards increasingly expect their CISOs to have addressed accountability gaps before incidents force the issue, the choice to defer the documentation problem is no longer a low-stakes choice.

What we observe in the field is that CISOs respond to this environment in three patterns. The first pattern is denial — continuing to operate as if the operational program is what matters and the documentation can be assembled if needed. This pattern is, in our analysis, increasingly untenable. The volume and quality of documentation expected at the moment an incident or inquiry occurs is no longer producible on demand.

The second pattern is panic — recognising the gap, attempting to close it under time pressure, and producing a documentation push that consumes resources without addressing the underlying architectural issues. This pattern produces a binder. It does not produce an evidence system. The next incident or inquiry reveals that the binder, while better than nothing, is not what was needed.

The third pattern is deliberate architectural investment — recognising that the documented security program needs to be built as deliberately as the operational program, resourcing it appropriately, and making the structural choices that allow operational reality and documentation to converge. This pattern is rare. It is, in our experience, the only pattern that addresses the underlying problem.

The CISO who chooses this third pattern is making a difficult sell to their organisation. The investment is real. The visible deliverables are unglamorous. The benefits accrue under conditions that everyone hopes will not occur. But when those conditions do occur — when the incident happens, when the regulator calls, when the board needs to be assured that the program has been operating as deliberately as it has been described — the CISO who has invested in documentation infrastructure is in a fundamentally different position than the CISO who has not. The first can demonstrate. The second can only assert. The difference is often the difference between defensible accountability and personal exposure.

This is the choice the modern CISO is being asked to make, whether or not the organisation has framed it explicitly. The documentation problem is solvable. It is not solved by accident. And the consequences of leaving it unsolved are no longer abstract.

KEY TAKEAWAYS

01. CISO accountability has shifted from professional to personal in ways with specific legal and financial consequences — SEC enforcement, litigation exposure, and fiduciary expectations have changed the operating environment for security leadership.

02. Most organisations operate two security programs simultaneously: the operational program (what the team actually does) and the documented program (what an investigator could reconstruct). The gap between them is where the CISO is personally exposed.

03. Regulators and litigators look for five things in security investigations: risk identification and acceptance, control design and implementation, operational evidence, governance and oversight, and continuous improvement.

04. The operational/documented gap is not a function of incompetence — it is a function of three structural pressures: incident-response cultural orientation, technical staffing without documentation capacity, and tools that produce operational data rather than audit-ready documentation.

05. Closing the gap requires architectural choices, not more documentation effort: integrating documentation as a structural component of operations, assigning explicit ownership, and integrating with the governance functions that consume the documentation.

ABOUT THE AUTHOR

Richard Jones Onyeneho · *Senior Principal & Enterprise Documentation Architect*

Richard is the Founder and Senior Principal of ELDR Group Inc., an advisory, intelligence, and technology firm operating across Canada, the United States, the United Kingdom, and Nigeria. He has led documentation, GRC, and enterprise technology mandates for organisations including Apple, IBM, Mastercard, Capital One, SAP, PwC, ServiceNow, and the U.S. Export-Import Bank.

ENGAGE ELDR GROUP

If this is the conversation your organisation is having — we should talk. Request a confidential consultation at **www.eldr.io/contact**.