EXECUTIVE WHITE PAPER

Governing Security When the CISO Advises but Doesn't Command

Organizational Design, Risk Ownership, and Compliance Challenges When the SOC Reports to the CTO

Kim | Chief Information Security Officer | CyAN Member

linkedin.com/in/kimabdalian

Target audience: Executive and Senior Management

July 2026

Executive Summary

A significant share of organizations still place the Security Operations Center (SOC) organizationally under the Chief Technology Officer, while the Chief Information Security Officer and a small security function operate in a largely advisory capacity: setting policy and standards, but without direct authority over SOC staffing, tooling roadmaps, or incident-response resourcing. This paper examines the governance consequences of that model.

It sets out why the structure persists, the accountability-without-authority problem it creates, and how that problem intersects with three concurrent compliance obligations many organizations now carry: PCI DSS, ISO/IEC 27001, and the newer ISO/IEC 42001 standard for AI management systems. It answers a question boards frequently leave unresolved: who owns the risk register and the Risk and Control Self-Assessment (RCSA) process when operational security sits inside the technology function. It closes with a SWOT analysis of the model and a set of recommendations, foremost among them elevating the CISO's reporting line to the CEO or the Board and giving the function its own CAPEX and OPEX budget, since it is the CISO who ultimately answers for every certification the organization holds.

The central argument is straightforward: an advisory-only CISO can still be held accountable for outcomes, but only if the organization is explicit, in its governance charter, its risk policy, and its board reporting, about where advice ends and authority begins. Left implicit, the gap becomes visible at the worst possible moment: during a major incident, an audit, or a certification assessment.

Table of Contents

Executive Summary 2

Table of Contents 3

1. Introduction: The Advisory CISO 4

2. Why This Model Persists 4

3. The Core Governance Problem: Authority Without Command 4

4. Compliance Overlay: PCI DSS, ISO/IEC 27001, and ISO/IEC 42001 5

4.1 PCI DSS 5

4.2 ISO/IEC 27001:2022 5

4.3 ISO/IEC 42001:2023 5

4.4 Certification Accountability Sits with the CISO 6

5. The Biggest Headaches for the CISO in This Model 6

6. Who Must Own the Risk Register and the RCSA Process? 7

7. SWOT Analysis: The Advisory-CISO / SOC-Under-CTO Model 8

8. Recommendations: From Advisory to Effective Oversight 9

9. Conclusion 10

About the Author 11

Disclaimer 11

References 11

1. Introduction: The Advisory CISO

Security reporting lines have been shifting for over a decade, yet the destination has not changed as much as the debate around it suggests. Industry benchmarking places a majority of CISOs reporting into the technology organization rather than to the CEO, board, or a risk-focused executive.

This paper focuses on a specific and common variant of that structure: the Security Operations Center (detection, monitoring, triage, and incident response) sits organizationally inside the CTO's function, typically alongside infrastructure and engineering teams that already own the underlying platforms. The CISO and a lean security team sit apart, in an advisory or "second opinion" capacity: they write policy, set standards, review architecture, and speak to the board, but they do not hold budget, staffing, or operational decision rights over the SOC itself.

That distinction, advisory versus operational authority, is the subject of this paper. It is not, on its own, an indefensible model. It is, however, a model that requires deliberate governance design to avoid becoming an accountability trap for the CISO.

2. Why This Model Persists

Three practical forces keep security operations inside the technology organization rather than under a fully empowered CISO function.

- **Toolchain and platform overlap:** SIEM, EDR, cloud logging, and network telemetry are frequently built on the same infrastructure the CTO's team already operates, making co-location administratively convenient.
- **Cost and headcount efficiency:** a shared operations model avoids duplicating monitoring and on-call capability across two reporting lines.
- **Historical inertia:** security began as a technical sub-discipline of IT, and in many organizations the reporting line has simply never been revisited as the risk profile matured.

Independent benchmarking supports how common this remains: recent industry research puts the share of CISOs reporting into IT leadership (typically the CIO or CTO) at roughly two-thirds of organizations surveyed, with direct reporting to the CEO still a minority position [1]. Longitudinal studies from major advisory firms have also tracked a rise in CISOs reporting to CIOs or CTOs over recent years, even as commentators have argued this trend runs in the wrong direction for governance purposes [2].

3. The Core Governance Problem: Authority Without Command

The recurring critique of this structure, echoed consistently across governance commentary, is that it creates a structural conflict of interest. The function responsible for delivery speed, uptime, and cost efficiency is placed above the function responsible for flagging the risk that speed and cost efficiency create. One widely cited comparison likens it to asking a fire marshal to report to the person whose bonus depends on cutting the number of sprinklers [1].

The advisory-CISO variant sharpens this further. The CISO is not merely reporting through a leader with competing incentives; the CISO frequently has no line authority at all over the team executing detection and response. Policy can be written, but its execution, prioritization, and resourcing are decided elsewhere. This produces a distinctive governance failure mode: accountability without authority. When an incident, audit finding, or board question arrives, it is the CISO who is expected to answer for outcomes the CISO could recommend but not direct.

This is not a theoretical concern. Regulators have begun to act on it directly. India's securities regulator, for example, has proposed separating technology and risk/compliance reporting verticals for market infrastructure institutions specifically to remove the conflict created when technology and security accountability sit under the same executive line [3]. The underlying logic applies equally to the advisory-CISO-under-CTO model: where the same organizational unit is both the risk-taker and the party assessing whether that risk has been adequately controlled, independent challenge is structurally weakened.

4. Compliance Overlay: PCI DSS, ISO/IEC 27001, and ISO/IEC 42001

Operating an advisory-only CISO model does not, by itself, break compliance with any of the three frameworks the organization must satisfy. It does, however, make each of them harder to evidence convincingly, because all three assume a defensible answer to "who is accountable for this control, and do they have the standing to enforce it?"

4.1 PCI DSS

PCI DSS requires formally assigned information security responsibilities and a tested incident response capability. Where the team executing monitoring and incident response reports to the CTO, and the CISO's role is advisory, assessors will look for evidence that the security function can still influence prioritization of security findings against competing delivery priorities, not merely document a policy that says it should.

4.2 ISO/IEC 27001:2022

Clause 5.3 obliges top management to assign and communicate information security roles, responsibilities, and authorities. An advisory CISO whose formal authority does not match the responsibility implied by the ISMS documentation is a common source of nonconformities: the management system says the CISO owns a control, but operational reality shows the CTO's team makes the relevant decisions. Segregation-of-duties expectations embedded in the Annex A control set are similarly harder to demonstrate when the same reporting line both operates and is expected to self-assess a control [5].

4.3 ISO/IEC 42001:2023

As SOC tooling increasingly incorporates AI-assisted detection, triage, and even semi-autonomous containment actions, ISO/IEC 42001 introduces a parallel question: who is the accountable risk owner for an AI system's decisions when the team configuring and tuning that AI system reports outside the security function entirely? Without an explicit answer, AI governance under 42001 inherits the same authority gap already present in the underlying SOC/CTO structure.

The practical consequence is that an organization can hold all three certifications while still carrying a structural governance weakness that a QSA, a lead ISMS auditor, or an AI-management-system auditor may not initially

detect on paper, but that becomes very visible the first time a serious incident, or a serious finding, requires someone to have had the authority to act and didn't.

4.4 Certification Accountability Sits with the CISO

Whatever the reporting line, the final responsibility for each certification, the PCI DSS attestation of compliance, the ISO/IEC 27001 certificate, and the ISO/IEC 42001 certification, rests with the CISO, not with the CTO or the SOC. Assessors and certification bodies address their findings to the executive who signs for the management system, and it is that executive who must answer for a suspended certificate or a failed surveillance audit. This is precisely why the role requires enough independence, in reporting line, in budget, and in challenge authority, to stand behind what is being certified rather than merely coordinate it on someone else's behalf. An organization cannot reasonably hold the CISO accountable for certification outcomes while denying the CISO the standing needed to influence the controls those certifications depend on.

5. The Biggest Headaches for the CISO in This Model

In practice, CISOs operating under this structure describe a recurring set of frustrations. Ranked by how often they surface as material issues in governance reviews and board escalations:

- **No operational authority over detection and response:** the CISO can recommend a control or a re-prioritization, but cannot direct the SOC to implement it on a given timeline.
- **Audit and regulatory findings land on the CISO, not the SOC:** accountability follows the title, not the org chart, even when the underlying control gap sits inside a team the CISO does not manage.
- **Board reporting inconsistency:** the CTO's team reports uptime, throughput, and delivery metrics; the CISO is expected to translate the same operational data into a risk narrative it did not generate and cannot independently verify.
- **Slow incident escalation across reporting lines:** a security event discovered inside the CTO's operational hierarchy may be triaged against delivery priorities before the CISO is even informed.
- **Compliance evidence gaps from weak segregation of duties:** the same reporting line frequently designs, operates, and is asked to self-assess the same control.
- **SOC talent, tooling, and priorities set by the CTO:** hiring, retention, and tool selection for detection and response follow engineering priorities rather than a risk-led roadmap.
- **Security budget competing directly with delivery budget:** with a single technology budget owner, security investment is evaluated against feature velocity rather than enterprise risk reduction.

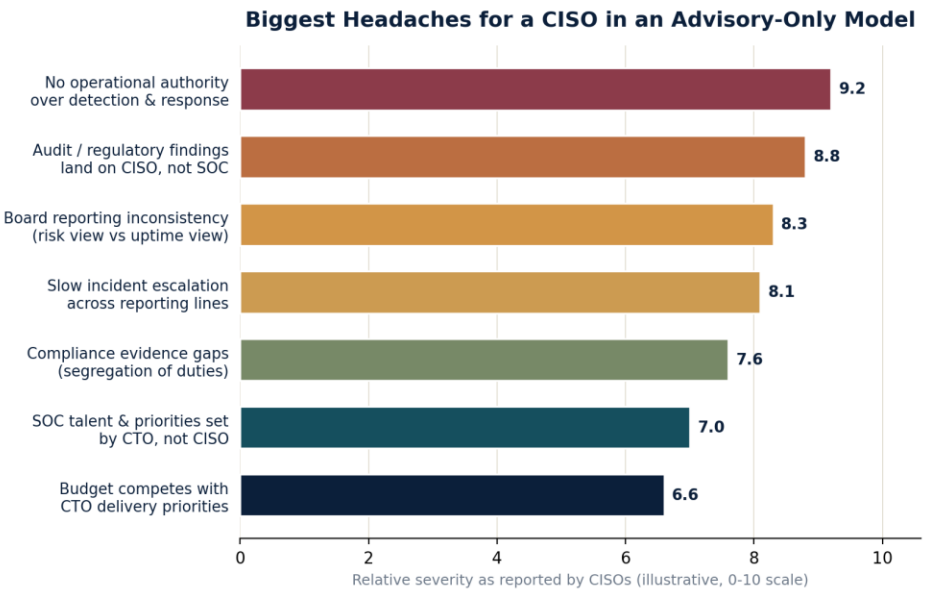

Figure 1. Illustrative ranking of the most frequently reported CISO headaches under an advisory-only, SOC-under-CTO model.

The cumulative effect of these headaches is that a disproportionate share of the CISO's time is spent on activity that does not directly reduce risk (chasing, translating, and evidencing) rather than on risk-reduction work itself.

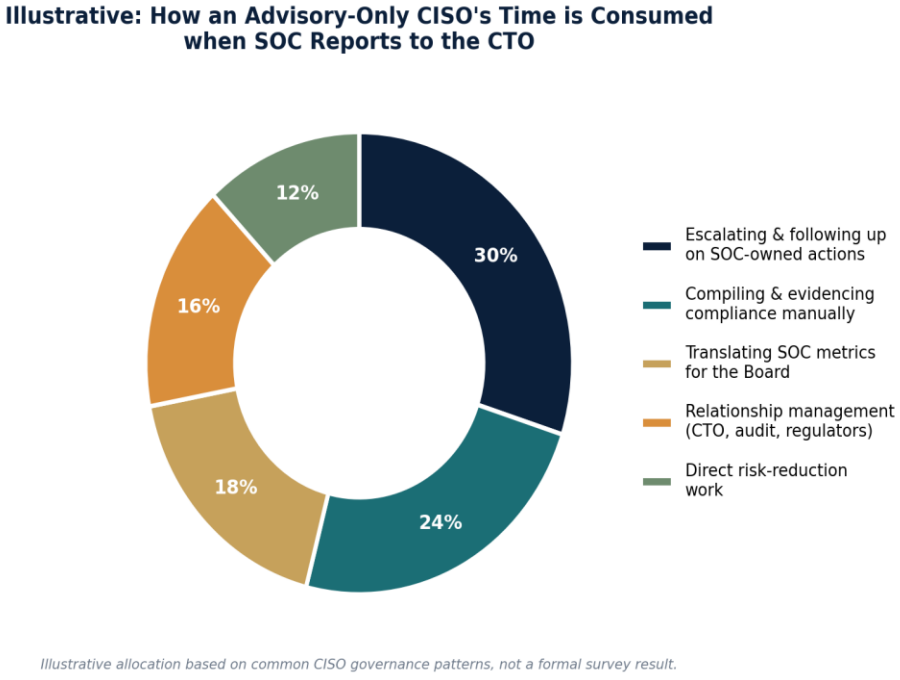

Figure 2. Illustrative allocation of an advisory-only CISO's time under this model.

6. Who Must Own the Risk Register and the RCSA Process?

This question sits at the heart of the governance gap, and it has a clear answer once the Three Lines Model is applied consistently, regardless of where the SOC reports.

- **First line: operational management owns the risk.** SOC and IT operations leadership, as the process owners actually running detection, monitoring, and response, must complete and attest to the RCSA for the controls they operate, and they own the underlying risk entries in their domain. Reporting to the CTO does not change this; it only changes who the first-line owner reports to.
- **Second line: the CISO owns the register and the methodology.** The CISO's function sets the risk taxonomy, scoring methodology, and RCSA cadence; consolidates the enterprise-wide security and technology risk register; independently challenges first-line self-assessments; and is accountable for presenting the aggregated risk view to the Risk Committee and the Board.
- **Third line: Internal Audit owns independent assurance.** Internal Audit confirms that both the RCSA process and the register itself are operating as designed, including whether second-line challenge is genuine rather than nominal.

Applied to the specific structure in this paper: ownership of the risk register (the document, the schema, the consolidated enterprise view) sits with the CISO as the second line, even where the CISO's role is described internally as advisory. Ownership of the individual risks and their remediation sits with the first-line process owner, which in this model is SOC/IT operations leadership under the CTO. The two are not in tension; they are complementary, and confusing them is precisely what allows risk to go unowned in practice.

The one condition that makes this arrangement defensible is that the CISO's second-line challenge role must be explicit and codified, in the risk policy, the ISMS documentation, and the RCSA charter, rather than assumed. An advisory CISO with no formal challenge mandate over first-line self-assessments does not provide independent second-line oversight; the RCSA becomes an uncontested self-assessment, which is itself a control gap that both internal and external auditors will identify.

7. SWOT Analysis: The Advisory-CISO / SOC-Under-CTO Model

The table below summarizes the model's structural position. It is offered as a discussion tool for the Board and Executive Committee, not as a verdict on any individual organization.

STRENGTHS	WEAKNESSES
• Faster integration of security tooling with shared infrastructure and platforms • Single technology roadmap reduces duplication of monitoring capability • Lower direct operating cost than a fully separate security operations function • Leverages the CTO's existing platform and automation investment	• Authority-responsibility mismatch: the CISO is accountable without operational control • Ambiguous incident escalation and decision rights during live events • Segregation-of-duties conflicts complicate audits and certifications • Board reporting mixes uptime metrics with risk metrics, obscuring both
OPPORTUNITIES	**THREATS**
• Elevate the CISO's reporting line to the CEO or Board to remove the conflict of interest • Establish an independent CAPEX/OPEX budget for the CISO's function	• Growing regulatory precedent for separating technology and risk reporting lines • Major nonconformities where segregation of duties cannot be evidenced

• Establish a governance charter granting the CISO explicit escalation and challenge rights • Use the ISO/IEC 42001 rollout as a trigger to re-baseline the whole governance model	• Reputational and legal exposure if incident response is delayed by competing priorities • Security talent attrition where the function is structurally under-empowered

8. Recommendations: From Advisory to Effective Oversight

Some of the weaknesses and threats identified above can be mitigated without disturbing the operating model. The two recommendations below cannot; they call for a change in where the CISO sits and how the function is funded, because compensating controls alone cannot fully close a structural independence gap.

- **Elevate the CISO's reporting line to the CEO or the Board:** the CISO, and by extension the function accountable for PCI DSS, ISO/IEC 27001, and ISO/IEC 42001 certification outcomes, should report directly to the Chief Executive Officer or to the Board (typically through a Risk or Audit Committee), rather than through the COO, CIO, or CTO. Reporting through the leader of the function being overseen is the conflict of interest at the root of most of the headaches in Section 5; removing it is the single highest-leverage change available to the organization.
- **Give the CISO an independent CAPEX and OPEX budget:** security capital and operating expenditure, including SOC tooling, staffing, and detection and response platforms, should be planned, owned, and defended by the CISO's own budget line directly to the Board or Finance Committee, rather than sitting as a sub-line inside the CTO's technology budget. Without a separate budget, even a CISO with a strong reporting line will still see security investment traded off against delivery velocity by whoever controls the purse.

Where the reporting line and budget cannot be changed immediately, the following measures reduce, but do not eliminate, the exposure described in this paper:

- **Codify a security governance charter:** document the CISO's escalation rights and second-line challenge authority over SOC-owned RCSA entries, independent of the reporting line.
- **Separate risk acceptance from operational delivery:** require joint CISO and CTO sign-off on high and critical risk acceptances, with disagreement escalated to the CEO or Board rather than resolved unilaterally by either party.
- **Adopt joint, risk-weighted KPIs:** measure the SOC on detection and response effectiveness (e.g., mean time to detect/respond, control-test pass rates) alongside the CTO's delivery metrics, reported jointly to the Board.
- **Run one integrated RCSA, mapped to three frameworks:** assess each control once against a common control library, then map results to PCI DSS, ISO 27001, and ISO 42001 requirements rather than repeating the exercise per standard.
- **Translate SOC metrics into board-ready risk language:** cyber reporting to the Board should connect technical findings to business impact, investment trade-offs, and disclosure obligations, not simply relay dashboard counts.

- **Periodically benchmark the reporting line:** revisit the structure as the organization's risk profile, regulatory exposure, and AI adoption evolve, rather than treating today's model as permanent.

9. Conclusion

An advisory CISO working alongside a SOC that reports to the CTO is not, by itself, a governance failure. It becomes one only when the gap between the CISO's accountability and the CISO's authority is left unaddressed, assumed away rather than governed. For organizations pursuing or maintaining PCI DSS, ISO/IEC 27001, and ISO/IEC 42001 compliance simultaneously, that gap is no longer a private organizational-design question; it is something assessors, auditors, and increasingly regulators will test directly.

The most durable fix is structural: the CISO should report to the CEO or the Board rather than to the COO, CIO, or CTO, and should hold an independent CAPEX and OPEX budget for the security function. Both changes follow directly from where accountability already sits, since it is the CISO, not the CTO or the SOC, who must answer for every certification the organization holds. Where those changes take time to implement, the Board should still insist that authority is made explicit wherever accountability already exists: in the governance charter, in the risk register ownership model, and in how the organization reports cyber risk upward. Boards that make this explicit position their organizations to govern cyber risk with the same discipline applied to financial and operational risk; those that leave it implicit will discover the gap at the least convenient possible moment.

About the Author

Kim | Chief Information Security Officer | CyAN Member

ISACA Platinum Member | Member, Pakistan Engineering Council (MPEC) | Member, Cyber Security Advisors Network | Cyberr®

linkedin.com/in/kimabdalian

Kim is a Chief Information Security Officer with more than 28 years of experience in information security leadership, risk assessment, and IT governance, including over 20 years within GCC Central Bank-regulated financial institutions. Kim has led enterprise-wide cybersecurity strategy, penetration testing and vulnerability management programs, cyber fraud investigations, and RCSA processes, while maintaining continuous PCI DSS certification with zero critical findings across multiple audit cycles. Kim's governance work spans NIST CSF, ISO/IEC 27001, ISO/IEC 42001, and ISO 22301, alongside Central Bank mandates and data protection regulation across the GCC and North Africa, and includes leading AI governance and AI Act readiness programs and directing incident response for organizations handling more than 1,000 security events per year. Kim holds CISM, CCSP, CDPO, and CBCMP certifications, among others, and advises Executives, Boards, and Senior Management on translating technical security risk into business decisions and board-level cyber oversight.

Disclaimer

The views, analysis, and recommendations presented in this white paper are those of the author alone, informed by professional experience and publicly available research and standards. Nothing in this document constitutes legal, audit, or compliance advice, and it does not represent the official position of any current or former employer, client, or organization with which the author is or has been associated.

References

[1] IANS Research and Artico Search, 2026 State of the CISO Benchmark Report, as reported in "It's time to rethink CISO reporting lines," CSO Online, Feb. 24, 2026.

[2] Deloitte cybersecurity governance survey findings on CISO reporting lines, as cited in "Cybersecurity & CISO Authority: The Risks of Reporting to a CIO," Wolf & Company, P.C.

[3] Securities and Exchange Board of India, consultation on Key Managerial Personnel reporting lines for Market Infrastructure Institutions, as reported in "CIOs, CISOs at MIIs: SEBI's KMP Reforms Could Be a Turning Point," Financial Express CIO, Jul. 15, 2025.

[4] Institute of Internal Auditors, The IIA's Three Lines Model: An Update of the Three Lines of Defense, IIA, Jul. 2020.

[5] International Organization for Standardization, ISO/IEC 27001:2022 Information Security, Cybersecurity and Privacy Protection: Information Security Management Systems Requirements (including Annex A reference controls), ISO, 2022.

[6] International Organization for Standardization, ISO/IEC 42001:2023 Information Technology: Artificial Intelligence Management System, ISO, 2023.

[7] PCI Security Standards Council, Payment Card Industry Data Security Standard (PCI DSS), Version 4.0.1, PCI SSC, 2024.

[8] ISC2, "CISO Reporting Lines – Why?," Jul. 19, 2024.