InfoSecAI

A BRIEF FOR CISOS · BISOS · GRC LEADERSHIP

WHITE PAPER

The CISO role has been rewritten. Most operating models have not.

A practitioner's white paper for CEOs, boards, CISOs and hiring committees on the evolution of the security leadership role and the operating model boards must now build around it.

AUTHORED BY

Paul Jolliffe

Founder & Director, InfoSecAI · Senior CISO / vCISO · CISSP · ISO 27001 Lead Auditor · MBA ·
Issued May 2026

01 · EXECUTIVE SUMMARY

Executive summary

The Chief Information Security Officer role is no longer best understood as the senior custodian of firewalls, audits and patching cadences. Over fifteen years it has moved from a technology-centred post inside the IT function into an enterprise role that shapes business risk, resilience strategy, technology investment, regulatory posture and stakeholder trust.

47%

EXECUTIVE-LEVEL CISOS

IANS / Artico Search 2026 benchmark — plurality in large enterprises

52%

REPORT SCOPE UNMANAGEABLE

IANS 2025 State of the CISO — over half see scope as no longer fully manageable

73%

STRATEGIC ON TECHNOLOGY

Deloitte 2025 — increased strategic CISO involvement in key technology decisions

7

REGULATORY ACCELERANTS

SEC, NIS 2, DORA, EU AI Act, NIST CSF 2.0 Govern, NCSC code, UK CSR Bill

Deloitte describes the historical arc as a move from a defence-oriented role to a growth-oriented one; the World Economic Forum and the Cambridge Judge Business School go further, characterising the modern CISO as an executive with board influence and a mandate that extends well beyond traditional information security. That evolution has been driven by structural changes, not fashion. Cloud platforms, SaaS portfolios, identity-based attacks, software supply-chain dependency, generative AI adoption, geopolitical pressure and shorter attacker breakout times have all raised the economic and operational stakes of cyber risk.

In parallel, the regulatory environment has hardened: the United States Securities and Exchange Commission (SEC) cyber disclosure rule requires public companies to explain their cyber governance and management's expertise; the Network and Information Security 2 Directive ((EU) 2022/2555, "NIS 2") makes management bodies responsible for approving and overseeing cyber risk-management measures; the Digital Operational Resilience Act ((EU) 2022/2554, "DORA") imposes explicit governance and operational resilience duties on the management bodies of EU financial entities; and version 2.0 of the National Institute of Standards and Technology (NIST) Cybersecurity Framework added a sixth core function, Govern, formalising what good cyber leadership now requires.

SO WHAT **The role has evolved faster than many operating models have. The board question for 2026 is not whether to appoint a CISO, but whether the mandate, reporting line, capability and budget authority match what the role is now expected to do.**

This paper sets out the four-phase evolution of the role, the five forces driving the change, the traditional-versus-modern comparison, the capability model that today's role requires, the pressure points that can make it unsustainable, the vCISO and fractional alternatives, the regulatory accelerants, the 2026-to-2030 horizon, and a practical playbook for boards, CEOs and CISOs themselves.

02 · WHY THIS MATTERS NOW

Why this matters now

Three regulatory and governance moments coincide in 2026 to make this a decisive year for the role. The first is the operational arrival of NIST Cybersecurity Framework 2.0 (NIST CSF 2.0), published on 26 February 2024 and now in widespread use, whose new Govern function elevates governance, accountability and enterprise integration to the same standing as Identify, Protect, Detect, Respond and Recover. The second is the first full year of supervisory practice under DORA, which has applied since 17 January 2025, together with the substantive completion of NIS 2 transposition (deadline 17 October 2024) across European Union (EU) Member States. The third is the start of UK statutory work on the Cyber Security and Resilience Bill, introduced to Parliament on 12 November 2025 and currently in Public Bill Committee scrutiny, which will move comparable accountability duties into UK law during 2026 and 2027.

The Artificial Intelligence (AI) regulatory layer is moving in parallel. The EU AI Act ((EU) 2024/1689) entered into force on 1 August 2024, the prohibited-practices article (Article 5) applied from 2 February 2025, and the high-risk system obligations under Articles 6 to 15 together with the deployer obligations under Article 26 apply from 2 August 2026. Whether AI governance sits formally under the CISO or under a separate Chief AI Officer, the modern CISO is now expected to co-own AI risk governance alongside data, legal, product and technology leaders, with the AI Risk Management Framework from NIST (NIST AI RMF) supplying the common vocabulary.

The market evidence shows the role catching up unevenly. The Information Assurance and Network Security (IANS) 2025 State of the CISO benchmark, refreshed in January 2026, reports that executive-level CISO titles are now the plurality in large enterprises, with a 2026 update finding executive-level CISO titles rising to roughly forty-seven per cent of the population sampled, while a 2025 IANS and Artico Search survey found that fifty-two per cent of CISOs view their scope as no longer fully manageable. PwC reports

that AI and cybersecurity have moved to the top of the boardroom agenda in the United Kingdom (UK), with seventy-three per cent of organisations in a Deloitte sample reporting increased strategic CISO involvement in technology discussions over the prior year. The directional shift is real; the operating-model investment needed to sustain it is not yet universal. The board question for 2026 is not whether to appoint a CISO. It is whether the CISO mandate, reporting line, capability and budget authority match what the role is now expected to do.

03 · THE EVOLUTION OF THE ROLE

The evolution of the role

The CISO role has passed through four overlapping phases over the past fifteen years. The phases are not clean steps; they overlap, and many organisations still sit in earlier phases by operating model even where the title has caught up.

Figure 1. Four overlapping phases trace the CISO role from technical custodian inside IT to enterprise risk and resilience executive. The dated markers along the lower band are the regulatory and threat-environment moments that pushed the role upward.

In the early phase, roughly 2010 to 2015, the CISO was usually a specialist security head inside the IT function, measured mainly by control implementation, policy compliance, audit closure and technical defence. Reporting lines commonly sat under the Chief Information Officer (CIO) or under an infrastructure leader, which produced a structural

tension: the function had to challenge the same teams that hosted it. Credibility was built on technical depth and on closing findings from Payment Card Industry Data Security Standard (PCI DSS) audits, ISO/IEC 27001 certification cycles and Sarbanes-Oxley Act (SOX) information-technology general control reviews. Board interaction was episodic and technical.

The middle phase, roughly 2016 to 2019, saw the role elevated into security programme leadership. The arrival of the European Union General Data Protection Regulation (GDPR) in May 2018, together with the original NIST Cybersecurity Framework (NIST CSF 1.0, 2014) and accelerating cloud migration, broadened the agenda. Privacy, third-party assurance, customer security reviews and data protection joined the brief. Boards began to ask better questions, but reporting remained control-heavy and backwards-looking. Many organisations during this period appointed their first dedicated CISO rather than continuing to delegate security to a head of IT.

The third phase, roughly 2020 to 2022, was forced. The COVID-19 pandemic in March 2020, the SolarWinds supply-chain compromise disclosed in December 2020, the Microsoft Exchange Server vulnerabilities in early 2021, the ransomware wave that struck Colonial Pipeline, JBS and Kaseya during 2021, and the Log4j vulnerability disclosed in December 2021 together rewrote the threat economy. Identity-based attacks, software supply-chain dependency, remote work and cloud misconfiguration became the dominant operational concerns. The CISO became, in many organisations, a business continuity leader expected to explain blast radius, recovery choices and executive trade-offs to the executive and the board in real time.

A fourth phase has now emerged, roughly 2023 to 2026, in which the role moves into business risk and resilience executive territory. The SEC cyber disclosure rule (adopted 26 July 2023), NIST CSF 2.0 (26 February 2024), NIS 2 (transposition deadline 17 October 2024), DORA (applies from 17 January 2025), the EU AI Act (entered into force 1 August 2024) and the UK Cyber Governance Code of Practice published by the National Cyber Security Centre (NCSC) have together pushed cyber governance into the boardroom as a formal duty. The CISO is now expected to convert technical exposure into business decisions: what level of cyber risk the organisation will accept, which controls and resilience capabilities are non-negotiable, which trade-offs require executive decision, and which material exposures must be escalated to boards, regulators, customers or insurers.

The directional shift across all four phases is consistent. The role has moved from inside-IT-and-technical to enterprise-and-governance. Reporting lines have widened. Time horizons have extended. The unit of analysis has shifted from systems and controls to risk

exposure, resilience and trust. Boards now expect cyber risk in the same language as financial and operational risk, integrated into the same dashboards and the same decisions.

04 · FIVE FORCES DRIVING THE CHANGE

Five forces driving the change

Five structural forces have moved the role. None is new in isolation; the compounding effect of all five together is what has reshaped the job.

Figure 2. Five forces compound on the modern CISO mandate; each alone would have moved the role, together they have rewritten it. Each force compounds the others.

The first force is the fusion of business and technology. Organisations now depend on distributed cloud services, Software-as-a-Service (SaaS) portfolios, digital supply chains and software-mediated operations. The World Economic Forum (WEF) Global Cybersecurity Outlook 2025 describes a cyber landscape made more complex by emerging technologies, regulatory burden and supply-chain interdependence, while NIST's AI Risk Management Framework and Generative AI Profile show that AI has added a new class of governance and operational risks rather than a narrow tooling issue. The result is that cyber risk sits inside product, data, operations and transformation decisions, not beside them.

The second force is the threat environment itself. Verizon's 2025 Data Breach Investigations Report (DBIR) found that third-party involvement in breaches doubled to thirty per cent of cases, exploitation of vulnerabilities rose by thirty-four per cent and now accounts for twenty per cent of breaches, while human involvement remained around sixty per cent. The CrowdStrike 2025 Global Threat Report adds that seventy-nine per cent of initial-access attacks are now malware-free, that average electronic crime breakout time fell to forty-eight minutes, and that valid-account abuse is the leading initial-access tactic in many cloud incidents. The European Union Agency for Cybersecurity (ENISA) Threat Landscape 2024 identifies threats against availability, ransomware and threats against data as the leading threat categories. These patterns force CISOs to think less in terms of perimeter defence and more in terms of resilience, identity, supply chain and time-to-decision.

The third force is regulatory and fiduciary accountability. The SEC's 2023 rule requires annual disclosure of cyber risk-management processes, board oversight and management's role and expertise, together with current disclosure of material incidents under Form 8-K Item 1.05. NIS 2 requires management bodies to approve cybersecurity risk-management measures, oversee their implementation and accept potential liability for infringements. DORA goes further for financial entities, requiring the management body to define, approve, oversee and be responsible for Information and Communications Technology (ICT) risk arrangements, business continuity and crisis communication. NIST CSF 2.0 adds the Govern function as the sixth core function of the framework, lifting governance to the same standing as the other functions. The effect is to formalise cyber governance as a leadership duty, not a technical one.

The fourth force is stakeholder economics. Boards increasingly expect cyber metrics in the language of enterprise risk. The National Association of Corporate Directors (NACD) 2026 materials call for probable financial impact, cyber loss exposure and risk appetite expressed in economic terms. NIST Interagency Report 8286 (NIST IR 8286) centres the integration of cyber risk registers into enterprise risk management and governance oversight. PwC's 2024 commentary observes that the threats companies find most concerning are often the ones for which they feel least prepared, and that fewer than half of organisations involve the CISO deeply enough in strategic planning, board meetings and technology deployment oversight. That mismatch creates pressure for CISOs to move from technical reporting to investment and risk-decision support.

The fifth force is market trust. PwC reports that many companies now position cybersecurity as a competitive advantage for customer trust and brand integrity. The Cybersecurity and Infrastructure Security Agency (CISA) Secure by Design programme and the Software Bill of Materials (SBOM) initiative point to the parallel shift toward product and supply-chain assurance, which increasingly matters to enterprise customers and procurement teams. Insurers have reached similar conclusions from claims data:

Marsh McLennan's 2025 work tied incident response planning, Endpoint Detection and Response (EDR) deployment and phishing-resistant multi-factor authentication to reduced breach likelihood, reinforcing that buyers and underwriters now look for evidence of real operating discipline rather than paper compliance alone.

05 · TRADITIONAL CISO VERSUS MODERN CISO

Traditional CISO versus modern CISO

The dimensions of the role have all moved. The infographic below is a synthesis of regulator guidance, benchmark studies and observed practice.

Figure 3. Eight dimensions of the role, side by side. Every row points the same direction. The role has not been added to; it has been rewritten.

The most useful way to read the comparison is not row by row but as a single integrated shift. The traditional role was defined by activities a single technologist could execute end to end inside an IT function: implement controls, close audit findings, run vulnerability management, draft policies, lead the technical response when an incident occurred. The modern role is defined by outcomes a single executive cannot personally execute and must instead orchestrate across the enterprise: enterprise risk decisions, resilient business services, regulatory evidence, customer and insurer trust, integrated AI governance. Every dimension on the right-hand side of the figure depends on relationships, mandate and authority that the left-hand side did not require.

The implication for boards and hiring committees is structural rather than cosmetic. The traditional role can be filled by a deep technologist working primarily through technology levers. The modern role cannot. It requires the technical credibility to be heard by engineering, plus the risk and governance literacy to be heard by the audit committee, plus the executive judgement to make trade-offs that materially affect the firm. Where organisations attempt to staff the modern role with a traditional profile, the predictable result is a technically excellent leader who is bypassed on the decisions that matter most.

06 · THE NEW MANDATE: WHAT BOARDS AND CEOS NOW EXPECT

The new mandate: what boards and CEOs now expect

Boards and CEOs now expect five things from the role at once: risk translation, resilience leadership, regulatory evidence, customer and insurer assurance, and technology partnership rather than late-stage veto.

Risk translation. The board expects cyber risk converted into business decisions. NACD's current guidance asks directors to expect management reporting that quantifies probable frequency and financial impact, shows alignment to risk appetite, and integrates cyber reporting with financial, operational and strategic dashboards. The NCSC Cyber Governance Code of Practice takes a similar view in the UK, making board ownership explicit across risk management, strategy, people, incident planning and assurance. The modern board does not just want an update on controls; it wants a view on exposure, options, trade-offs and preparedness.

Resilience leadership. Operational resilience is no longer an adjacent discipline. The Financial Conduct Authority (FCA) SYSC 15A operational resilience regime, the Prudential Regulation Authority (PRA) Supervisory Statement SS1/21 on impact tolerances for important business services, and DORA Articles 11 and 12 on response, recovery and backup all expect the CISO to lead, or to participate as a named accountable individual in, the firm's resilience programme. The discipline reaches across business-continuity planning, severe-but-plausible scenario testing, recovery time objectives, recovery point objectives, and the executive incident-management process.

Regulatory evidence. The CISO must now produce defensible evidence of governance and control to boards, regulators, customers, auditors and insurers. SEC Item 106 of Regulation S-K requires registrants to describe their processes for assessing, identifying and managing material cyber risks, the board's oversight, and management's role and expertise. The expectation is evidence, not assertion: documented processes, named owners, dated reviews, and audit-trail integrity.

Customer and insurer assurance. Procurement teams, customers and insurers increasingly require evidence of operating discipline. CISA's SBOM and Secure by Design initiatives have moved software transparency into a normal procurement expectation. Marsh McLennan's claims-linked research shows that tested incident response, EDR and phishing-resistant multi-factor authentication correlate with lower breach likelihood and therefore matter to underwriting decisions. The CISO is now responsible for the trust artefacts the firm exports as well as the controls it operates internally.

Technology partnership. Deloitte's 2025 work reported that seventy-three per cent of surveyed organisations had seen increased strategic CISO involvement in discussions about key technologies over the prior year. PwC reports that fifty-eight per cent of UK organisations say CISOs work to a large extent with CIOs and CTOs on technology and infrastructure deployments. The role works earlier and deeper in the build cycle than it once did, on cloud architecture, identity, product release decisions, AI use-case approvals and merger or acquisition due diligence.

WORKED EXAMPLE · FICTIONAL FIRM

Hartfield Asset Management plc moves its head of information security to a CISO role.

Hartfield is a fictional UK Alternative Investment Fund Manager that promoted its head of information security to a CISO role reporting to the Chief Operating Officer, with a dotted line to the Audit and Risk Committee, in early 2026. Before the change, the role was a technology-control lead reporting to the head of IT, with episodic board exposure.

After the change, the CISO presents a quarterly cyber-risk paper at the Audit and Risk Committee against the firm's risk appetite, owns the Article 5 ICT governance framework under DORA, runs the integrated incident classification process across DORA Article 19, GDPR Article 33 and FCA SUP 15.3.11R, sits on the AI Governance Committee, and produces a single quarterly view of resilience against the important business services map.

The titles changed less than the cadence; the cadence less than the conversation.

07 · THE MODERN CISO CAPABILITY MODEL

The modern CISO capability model

A high-performing CISO now needs a capability blend that would have been unusual in the role a decade ago. The model below is organised into four domains.

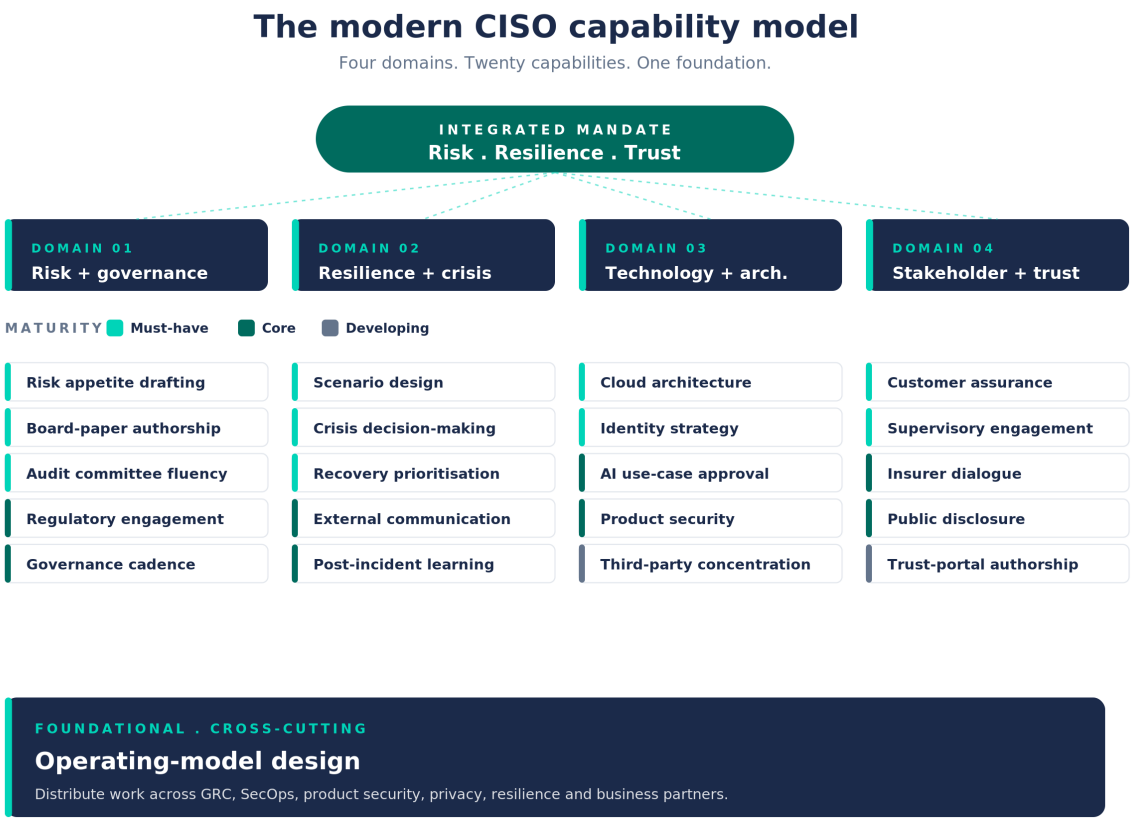

Figure 4. Four capability domains, twenty named capabilities, one cross-cutting foundation. Maturity tags reflect practitioner consensus.

Risk and governance translation. The first domain is the ability to move between technical evidence and business consequence. NACD expects cyber loss exposure, risk appetite and cyber return on investment to be discussed in economic terms, while NIST IR 8286 makes integration with enterprise risk management a core expectation. Named capabilities include risk appetite drafting, board-paper authorship, audit-committee fluency, regulatory engagement, and the design of the governance cadence itself. Without this capability the CISO remains informative but not influential.

Resilience and crisis leadership. The second domain is the ability to lead the organisation through severe-but-plausible scenarios. The NCSC code places incident planning, response and recovery at the heart of governance; the UK Government CISO role profile expects the CISO to prepare the organisation, lead critical incidents and run simulations with the board; and Marsh McLennan's 2025 work shows that incident response planning measurably reduces breach likelihood. Named capabilities include severe-but-plausible scenario design, executive crisis decision-making, recovery prioritisation, regulator and external-stakeholder communication, and post-incident learning. The highest-performing CISOs are not simply incident commanders in waiting; they are business-continuity and decision-preparedness leaders.

Technology and architecture partnership. The third domain is embedded technology judgement. Cloud, identity, SaaS, product development and AI adoption now shape the threat surface, and the CISO must be credible in architecture and engineering conversations. Deloitte's research on rising strategic CISO involvement, NIST's AI RMF, and CISA's Secure by Design and SBOM work all point to the same conclusion: security leadership must reach upstream into design, product and supplier choices. Named capabilities include cloud architecture review, identity and access strategy, AI use-case approval, product security, third-party concentration analysis, and security-by-design partnership with engineering teams.

Stakeholder and external trust. The fourth domain is the management of the trust relationship with customers, partners, regulators, insurers and the market. PwC's commentary on cybersecurity as competitive advantage, CISA's Secure by Design commitments and the rise of customer-trust portals all point to a role that exports evidence as well as managing internal controls. Named capabilities include customer assurance authorship, supervisory engagement, insurance broker dialogue, public disclosure (post-SEC rule) and the management of the firm's published trust posture.

A fifth supporting capability sits across all four domains: operating-model design. One person cannot sustainably own enterprise governance, threat operations, product security, privacy, resilience, third-party risk, AI oversight and security culture at execution depth. The practical response in mature organisations is to distribute work through specialist leaders and functions (Governance, Risk and Compliance (GRC); Security Operations (SecOps); product security; privacy; resilience; business-facing security partners) while keeping the CISO accountable for integration, prioritisation and enterprise narrative.

08 · THE UNSUSTAINABLE MIDDLE: PRESSURE POINTS AND PATHOLOGIES

The unsustainable middle: pressure points and pathologies

The role is expanding faster than its operating-model support in many organisations. Several pressure points are now widely visible.

Scope strain. The 2025 IANS and Artico Search benchmark reported that fifty-two per cent of CISOs view their scope as no longer fully manageable, and the 2026 update found scope expansion continuing while executive-level titles rose to roughly forty-seven per cent of the population sampled. Cambridge Judge Business School's 2026 research is explicit: the role can become unsustainable when boards expand expectations without matching authority, capability and support.

Accountability without authority. A persistent pathology is the gap between what the CISO is accountable for and what the CISO can decide. Modern governance frameworks place approval and oversight duties on management bodies (NIS 2 Article 20; DORA Article 5) and on boards (UK NCSC code; SEC rule), but the day-to-day decisions that shape exposure (product release timings, third-party selection, cloud architecture, hiring profiles) often sit with other executives. The CISO is accountable for the consequence of choices the role does not always own.

Compliance-resilience conflation. A second pathology is the assumption that "more compliance" automatically means "more resilience". Cambridge Judge's 2026 report warns explicitly against the conflation, and ENISA's threat work shows why: the highest-impact threats now involve availability attacks, ransomware, data threats and complex supply-chain exposure that are only partly visible through checklist-style assurance. Boards that treat audit closure as proof of resilience will systematically under-read enterprise exposure.

Personal liability. The former Chief Security Officer of Uber was sentenced in May 2023 to three years of probation following his handling of a 2016 breach, establishing that personal accountability can extend to security leaders when disclosure and regulatory interaction are mishandled. The SEC's civil case against the SolarWinds CISO ended with most claims dismissed in 2024 and the remaining claims dismissed in 2025, narrowing the immediate disclosure-fraud risk for individual CISOs. The combined lesson is not that every breach will expose a CISO personally, nor that liability fears were overstated; it is that the role now sits close enough to disclosure, governance and public statements that personal legal exposure is a real, if uneven, feature of the job.

Burnout and attrition. Scope strain, accountability gaps, insurance and regulatory pressure, after-hours incident exposure and the cumulative weight of breach disclosure work have made CISO attrition a visible workforce issue. Organisations that expand the role's expectations without expanding the role's mandate, budget and bench strength face a predictable failure mode: the CISO leaves, the replacement inherits the same constrained model, and the cycle repeats.

09 · THE VCISO AND FRACTIONAL MODEL: WHEN, WHY AND WHAT CHANGES

The vCISO and fractional model: when, why and what changes

A growing share of UK and EU mid-market organisations now meet the CISO need through a virtual CISO (vCISO) or fractional CISO model rather than a full-time appointment. The market term "vCISO" is not a standardised regulatory role; service descriptions and

practitioner commentary exist, but no formal standard defines vCISO responsibilities. The pattern, however, is now well-enough established that it can be described with confidence.

A full-time CISO is the right model when the organisation has the scale, regulatory exposure, third-party assurance demand and product-security agenda to justify a dedicated executive. A vCISO is the right model when the organisation has the same governance requirements but lacks the scale or the candidate pool to fill the role permanently, or when the organisation is at a transitional moment (pre-fundraise, pre-certification, pre-merger, post-incident) that benefits from senior leadership at part-time intensity.

Day-90 outcomes differ. For a full-time CISO, defensible day-90 outcomes include trusted relationships with the CEO, the Chief Financial Officer (CFO), the CIO or CTO and board or audit leadership; a current-state assessment tied to business services; a top-risk view with named owners; a prioritised roadmap; a defined governance cadence; an initial board report; a measurable set of quick wins; and a clear investment or resourcing case. For a vCISO, day-90 outcomes are tighter: risk triage, governance setup, decision-ready executive reporting, a prioritised remediation plan, and a retained cadence or handover model that fits the engagement intensity.

> **The full-time CISO leaves day 90 with enterprise traction and ownership; the vCISO leaves day 90 with enterprise clarity, sponsor confidence, and a workable execution model for internal teams or providers.**
>
> — INFOSECAI 90-DAY RESEARCH BASE · MAY 2026

The market signal is consistent across UK mid-market data. The InfoSecAI 90-day research base, drawing on forty-six primary and secondary sources, finds that the day-90 minimum viable position for a CISO or vCISO at a UK mid-market organisation in 2026 includes twenty-seven artefacts spread across information-security governance, AI governance, third-party risk, incident readiness and assurance. The model is not a replacement for in-house execution; it is a vehicle for senior judgement at proportionate cost.

Misuse patterns. The model fails in three common ways. First, when the vCISO is hired to "tick the box" for an insurer or a customer without authority to change anything, the engagement produces evidence without outcomes. Second, when the vCISO is asked to be the firm's permanent operating CISO without the time or bench strength to discharge the role, the engagement collapses under scope. Third, when the engagement is procurement-led rather than executive-sponsored, the vCISO has no path to influence the decisions that determine cyber exposure. The remedy is clear in all three cases: executive sponsorship, a scoped mandate, named decision rights, and a renewal review at 90 and 180 days.

The hybrid model. A growing pattern is the hybrid: an in-house head of security delivers operational execution while a vCISO provides senior strategic and governance leadership, board reporting and regulatory dialogue. The hybrid is well-suited to scale-ups and mid-market organisations where the in-house lead has technical credibility but lacks executive bandwidth, and where the vCISO has executive bandwidth but cannot personally own day-to-day operations.

10 · REGULATORY ACCELERANTS AND THE GOVERNANCE IMPERATIVE

Regulatory accelerants and the governance imperative

Seven regulatory and governance instruments have collectively rewritten the CISO role since 2023. Each one alone would have moved the role; the seven together have rewritten it. The pattern across the seven instruments is consistent: cyber risk is now framed as a leadership obligation discharged at board level, evidenced through documented processes, and exposed to supervisory examination on a fixed cadence. The technical specifics differ by jurisdiction and sector. The structural direction does not.

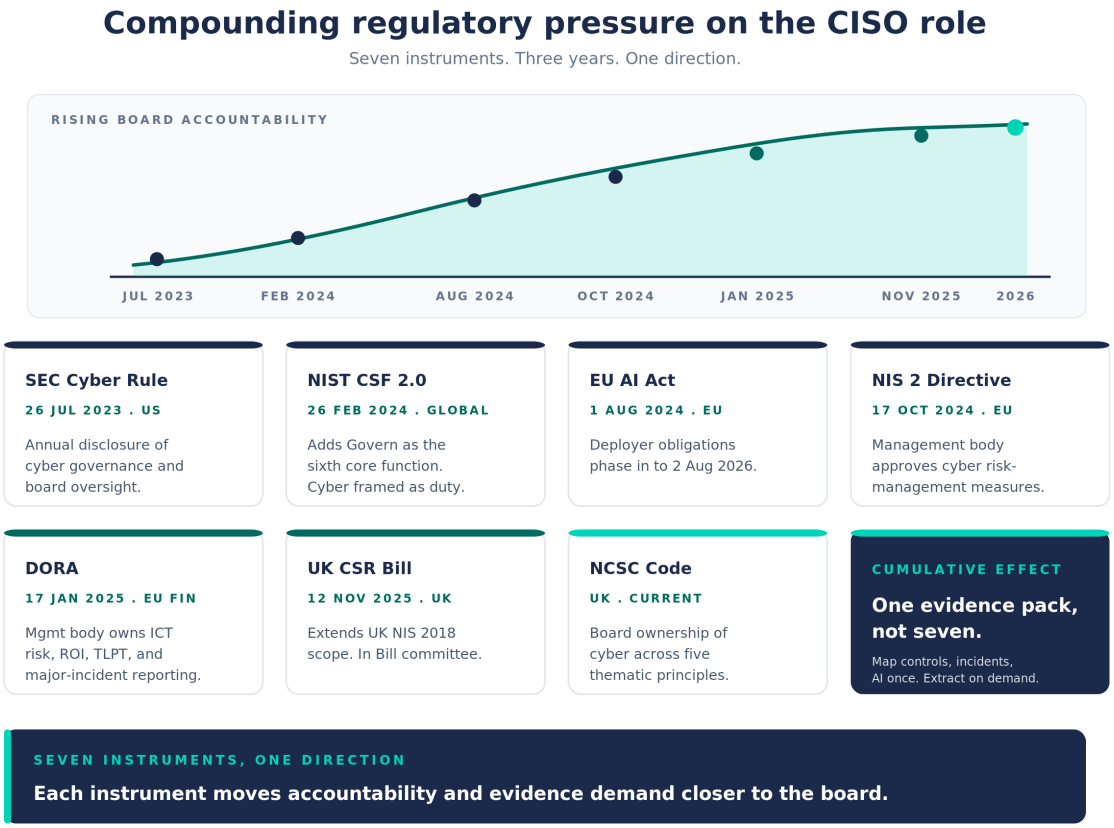

Figure 5. Seven regulatory and governance instruments have rewritten the CISO role since 2023. Timeline strip shows the five-year acceleration from July 2023 to November 2025.

For a multi-regime UK and EU firm, the seven instruments compound rather than substitute. A regulated financial entity is simultaneously inside DORA (ICT risk and operational resilience), NIS 2 (cybersecurity risk management), the EU AI Act (where AI is in scope), the SEC rule (where US-listed), the NCSC Cyber Governance Code (in the UK), the operational view of NIST CSF 2.0 (as the working framework most firms map to internally), and the prospective UK Cyber Security and Resilience Bill. The CISO sits at the centre of the compounded set, and the operating model needs to reflect that compounding rather than treat each instrument as a separate project.

The cumulative effect is to make cyber leadership a documented governance discipline. SEC rules require evidence that the board oversees cyber risk and that management has expertise. NIS 2 requires management-body approval of risk-management measures. DORA requires the management body to define, approve and oversee ICT risk arrangements. NIST CSF 2.0 elevates Govern to the same standing as Identify, Protect, Detect, Respond and Recover. The NCSC code places the duty of care on directors. Whichever instrument applies first, the direction is the same: the role of the CISO has been rewritten by the regulators as much as by the threat economy.

The seven instruments do not stack independently. Where a multi-regime firm operates inside several at once, the practical question is which evidence pack discharges the largest share of the obligations from a single integrated production. For a UK or EU regulated firm, an ISO/IEC 27001:2022 Information Security Management System (ISMS), an ISO/IEC 42001:2023 Artificial Intelligence Management System where AI is in scope, the DORA Register of Information, the NIS 2 risk-management framework, the SEC governance disclosure and the NCSC code-aligned board pack draw on the same underlying artefacts: risk register, control library, third-party register, incident log, AI inventory, board minutes, training records. The mistake to avoid is running seven parallel programmes; the discipline to build is a single evidence library with regime-specific extracts produced on demand. The CISO who owns the integrated evidence library is also the CISO who survives the next supervisory examination with the smallest amount of last-minute work.

11 · THE 2026 TO 2030 HORIZON: WHERE THE ROLE GOES NEXT

The 2026 to 2030 horizon: where the role goes next

Four trajectories are now visible in market data and supervisory dialogue. Each will reshape the role over the next three to four years.

AI governance, integrated or split. The first trajectory is the integration of AI governance into the CISO role, or its separation into a Chief AI Officer (CAIO). Both patterns are now visible. NIST's AI RMF and the Generative AI Profile supply the common vocabulary for either model. PwC's UK 2026 survey shows AI and cybersecurity rising together on board agendas, and NACD's latest cyber toolkit already includes a dedicated board discussion guide for AI. In practitioner experience, most UK mid-market organisations co-locate AI governance with the CISO under a joint operating committee rather than appoint a separate CAIO; large enterprises in regulated sectors are more likely to split the role.

The Chief Technology Risk Officer model. The second trajectory is the convergence of the CISO, the head of operational resilience, the head of third-party risk and (in some sectors) the head of model risk under a Chief Technology Risk Officer (CTRO) umbrella. The model is most advanced in EU financial services where DORA's combination of ICT risk, third-party concentration, operational resilience and threat-led penetration testing maps neatly onto a single executive scope. The CTRO model is not yet universal, but the supervisory dialogue under DORA in 2026 is accelerating it.

The strategic and operational split in large enterprises. The third trajectory is the formal split between a Strategic CISO (responsible for board engagement, regulatory dialogue, customer trust, AI governance and the operating model) and an Operational CISO or Head of Security Operations (responsible for the day-to-day controls, detection and response

programme). The IANS 2025 benchmark separated CISOs into "strategic", "functional" and "tactical" segments; the 2026 update found executive-level titles becoming the plurality, with continued separation between the strategic and tactical populations. Large enterprises are increasingly making the split explicit in the org chart rather than expecting one executive to do both.

Alignment with operational resilience, third-party risk and customer trust. The fourth trajectory is the closer integration of the CISO role with adjacent governance functions: operational resilience under FCA SYSC 15A and PRA SS1/21; third-party and outsourcing risk under PRA SS2/21 and DORA Articles 28 to 30; data protection under UK GDPR, the EU GDPR and the Data (Use and Access) Act 2025; and customer-trust portals that export Statements of Applicability, System and Organization Controls (SOC) 2 reports and certifications. The CISO is now the integrating executive for these adjacent disciplines in most mid-market UK organisations, even where formal accountability sits with another executive.

The Gartner 2025 cybersecurity outlook adds a useful summary: generative AI, digital decentralisation, supply-chain interdependence, regulatory change and talent shortages are the dominant security-management trends of the period. None of those forces shrinks the CISO role. All of them push it further into business risk and resilience leadership.

12 · PRACTICAL IMPLICATIONS FOR ORGANISATIONS

Practical implications for organisations

The directional shift is clear. The practical question for any organisation is whether the operating model has caught up. Six concrete moves apply.

Redefine the mandate in writing. The mandate document should name what the CISO is accountable for, what decisions the role can take alone, what decisions the role recommends to a named executive, and what decisions sit elsewhere. Without that document the role drifts into accountability without authority.

Clarify the reporting line. A reporting line inside IT was defensible in 2014. In 2026, the better defaults are CEO, COO, CRO or executive committee with a dotted line to the Audit and Risk Committee. The IANS 2026 benchmark shows executive-level titles and outside-IT reporting rising together; if your CISO still reports to the head of IT, ask why.

Allocate budget authority. The CISO needs a defined budget for the security programme, a defined input to broader technology budget decisions, and a defined route to escalate budget questions to the board or audit committee. Accountability without budget authority is structurally unstable.

Align with the audit committee. A standing item on the Audit and Risk Committee agenda, with the CISO present, is the simplest single change. The committee gains a credible source on cyber risk; the CISO gains visibility, calibration and a clear governance channel.

Build the capability model into the job description. Hire to the four-domain model in Section 07. A pure technologist will struggle with risk translation and board fluency; a pure communicator will struggle with technology partnership and crisis leadership. The role now requires both, plus operating-model design.

Resource the role. The CISO cannot personally cover enterprise governance, threat operations, product security, privacy, resilience, third-party risk, AI oversight and culture at execution depth. Resource the role with named deputies and named function heads; do not expect a single executive to discharge the entire enterprise security mandate alone.

Review the operating model annually. The role has moved fast enough over the past five years that an operating model designed in 2022 is already out of date. An annual review against the four-domain capability model, the seven regulatory accelerants and the latest IANS or Deloitte benchmark catches drift before it becomes a board issue.

For CISOs themselves, three personal moves apply. The first is to invest in board and audit-committee fluency, including the language of risk appetite, loss exposure, scenario testing and disclosure. The second is to build a named deputy and a named successor early; the role's scope has grown to the point where succession planning is now a governance obligation, not a personal preference. The third is to document personal accountability and decision rights in writing; the post-SolarWinds and post-Uber landscape rewards documented authority and punishes ambiguity, and a CISO who cannot evidence what they decided, when, and on what basis will struggle in both regulatory and litigation contexts.

CLOSING TAKEAWAY

Appointing a CISO is not enough. Build the operating model around the role.

- Redefine the mandate in writing. Clarify the reporting line: CEO, COO, CRO or ExCo with a dotted line to Audit.
- Allocate budget authority and a direct route to the audit committee.
- Hire to the four-domain capability model. Resource the role with named deputies and function heads.
- Review the operating model annually against the regulatory accelerants and benchmark.

How InfoSecAI helps

InfoSecAI works with UK and EU organisations to design and operate the modern CISO role. We deliver the mandate document, the four-domain capability model, the audit-committee cadence, the regulatory-evidence pack and the operating-model design as a single engagement. We deliver vCISO services for mid-market organisations that need senior leadership at part-time intensity, and the hybrid model for scale-ups that need both senior judgement and in-house execution.

Three engagement patterns apply. The CISO Reset, a six-to-twelve-week diagnostic that produces the mandate document, reporting-line recommendation, capability gap analysis and board-cadence design. The vCISO retainer, in which a senior InfoSecAI practitioner discharges the executive elements of the CISO role at a defined intensity alongside the in-house head of security. The regulatory-evidence build, which produces the artefacts a firm needs to satisfy SEC, NIS 2, DORA, EU AI Act and UK Cyber Governance Code expectations from a single integrated evidence pack.

For self-assessment, the InfoSecAI 90-day research base, the AI Governance Board Pack, the DORA 12-Month Reality Check and the Multi-Framework Crosswalk supply practitioner artefacts grounded in primary regulatory sources. To start a thirty-minute review or scope a vCISO engagement, contact paul.jolliffe@infosecai.net or book at infosecai.net.

InfoSecAI

About InfoSecAI

InfoSecAI is an independent UK consultancy helping organisations turn security, regulatory, resilience and AI governance requirements into practical operating models, stronger controls and robust delivery.

We work across strategy, governance, risk, compliance, AI security, assurance, operations and engineering. Our services help leadership teams assess their current position, align to standards and regulation, define the target operating model, and deliver the governance, controls, artefacts and ways of working needed to move from intent to implementation.

Our toolkit capability accelerates structured work across ISO 27001, ISO 22301, ISO 42001, NIST CSF, NIST AI RMF, CIS Controls, Cyber Essentials, DORA, NIS 2, the EU AI Act, GDPR, UK GDPR, SOC 1 and SOC 2. The approach combines AI-enabled workflow support with senior practitioner judgement, so outputs remain proportionate, usable and connected to the way the organisation actually operates.

InfoSecAI was founded in **2025** by **Paul Jolliffe**. The company is built for organisations that need clarity, senior leadership and hands-on delivery across information security and AI governance, without adding unnecessary complexity or treating compliance as a paperwork exercise.

infosecai.net · paul.jolliffe@infosecai.net