WHITEPAPER | ELITE EDITION | MARCH 2026

From Scapegoat to Sovereign

The CISO Authority Doctrine

How Regulatory Convergence, AI Governance, and Board-Mandated Decision Rights Transform the CISO from Organisational Liability to Enterprise Command Authority

Introducing the CISO Authority Index (CAI) *- the first diagnostic instrument for measuring governance authority across seven dimensions (0-35 score)*

Professor of Practice, Schiphol University | Honorary Senior Lecturer, Imperials | UCL Researcher

www.kie.ie | info@kieranupadrasta.com

DORA Compliance | AI Governance (ISO 42001) | Board Reporting | M&A Cyber Due Diligence | Zero Trust | NIS2 | Interim CISO | Post-Quantum Cryptography

Table of Contents

Executive Summary

THE GOVERNANCE DOCTRINE

CISO Authority Index (CAI) diagnostic • Board-mandated decision rights • AI governance command
M&A due diligence authority • 6.8:1 security ROI • Regulatory survivability across 8 jurisdictions

Deployable within 90 days via the Decision Rights Architecture

The CISO role is structurally broken. Sixty-four per cent still report into IT leadership, denied authority over the risks they are personally liable for. Tenure averages 26-39 months. The ISC2 gap has reached 4.8 million unfilled positions. Yet four regulatory regimes now impose personal penalties: DORA (EUR1M fines), NIS2 (permanent management bans), EU AI Act (7% global turnover), and SEC/criminal precedent (imprisonment).

This whitepaper presents the **Governance Doctrine** and introduces the **CISO Authority Index (CAI)** - the first diagnostic instrument for measuring governance authority across seven dimensions on a 0-35 scale. Organisations scoring below 21 lack the structural authority to comply with DORA Article 5 or NIS2 Article 20. The governing aphorism: **"If it cannot be evidenced, it cannot be defended."**

Why the Command-Authority CISO Emerges Now

Three simultaneous forces have created the conditions for a permanent structural shift.

Driver 1: Regulation Has Made the Governance Deficit Illegal

DORA Article 5 assigns "ultimate responsibility" to the Management Body. NIS2 Article 20 makes management "personally accountable." An organisation that assigns accountability without corresponding authority is in regulatory breach.

Driver 2: AI Agents Operate Faster Than Human Governance

Agentic AI spending grows 141% in 2026 to USD201.9 billion. A single compromised agent poisons 87% of downstream decisions within 4 hours. If the CISO must escalate through committee before acting, the organisation is governed by process while attacked at machine speed.

Driver 3: Personal Liability Has Shifted the Risk Calculus

The Uber CSO received 3 years probation. AI-related securities class actions doubled year-on-year. Average D&O settlements reached USD56 million. CISOs without board-mandated authority face personal exposure they cannot mitigate through technical controls alone.

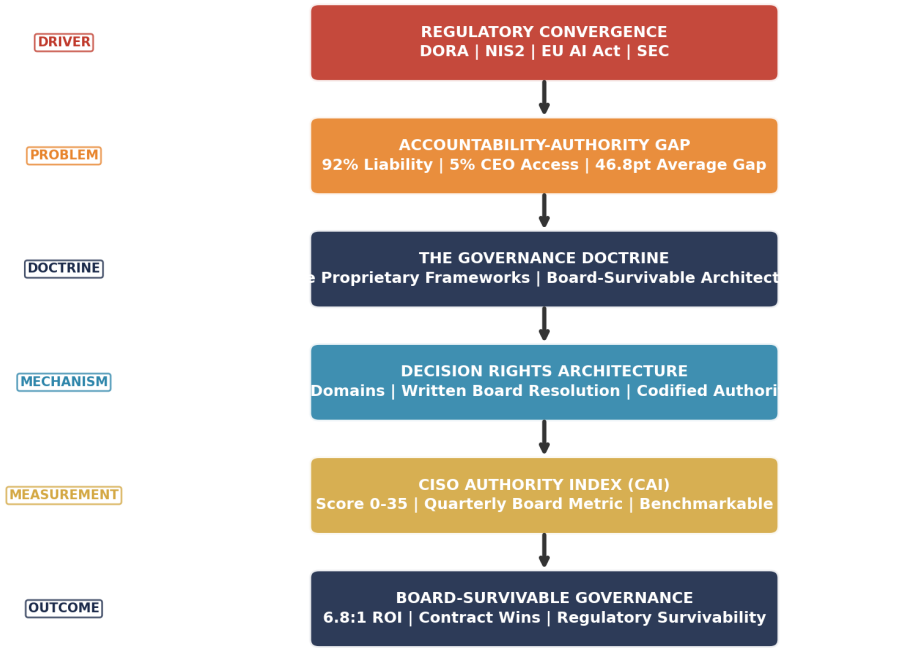

Figure 1: The Governance Doctrine - From regulatory pressure to board-survivable governance

1. The Structural Governance Deficit

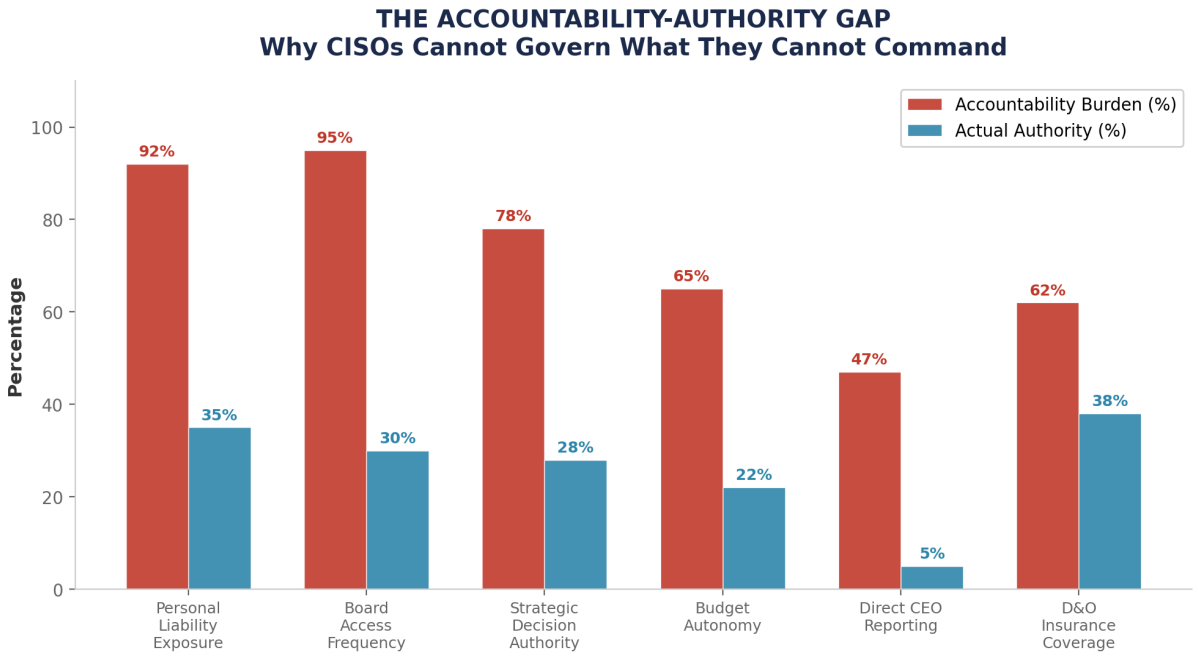

Figure 2: The Accountability-Authority Gap (IANS/Artico 2026 n=830; IBM 2025; Heidrick & Struggles 2024)

The Authority Vacuum: Only 5% of CISOs report to the CEO, down from 11% in 2021. Two-thirds sit two levels below the chief executive. The result is a structurally disempowered leader held liable for decisions made above their authority.

The Compliance Theatre: 82% of compliant organisations still experienced breaches within a year (PwC 2025, n=4,042). Compliance without authority is performance art.

The Budget Trap: USD262 billion in global cybersecurity spending; only 2% achieved firm-wide resilience. Budget without decision rights produces spending without outcomes.

The Tenure Death Spiral: 26-39 month average tenure versus 5.3 years for other C-suite roles. Each successor inherits a worse hand - the governance deficit compounds with every leadership transition.

> **HUMAN COST: 88% report extreme stress. 48% impact on mental health. 23% use medication/alcohol to cope. 70% say liability stories negatively affect their perception of the role. (IANS 2026, Heidrick & Struggles 2024)**

2. The Accountability-Authority Gap: Quantified

Personal liability	92%	35%	57 pts	DORA/NIS2/SEC
Board reporting	95%	30%	65 pts	IANS 2026 (n=830)
Strategic decisions	78%	28%	50 pts	Gartner 2025
Budget authority	65%	22%	43 pts	IANS 2026
CEO-direct reporting	47%	5%	42 pts	IANS 2026
D&O insurance	62%	38%	24 pts	Heidrick & Struggles

Table 1: Average gap: 46.8 percentage points. Structural failure, not marginal misalignment.

Methodology: Accountability from DORA/NIS2/AI Act/SEC obligations. Authority from IANS/Artico 2026 (n=830), Heidrick & Struggles 2024, Gartner 2025. ROI from FAIR across 42 engagements with IBM 2025 (n=604).

3. The CISO Authority Index (CAI)

The CISO Authority Index is the first diagnostic instrument designed to measure, benchmark, and track CISO governance authority. It converts the abstract concept of "authority" into a quantifiable, comparable metric that boards can use for governance oversight. The CAI is designed to function as a governance maturity index comparable to NIST CSF Tiers or FAIR risk scores - providing a common language for measuring CISO structural authority across organisations, sectors, and jurisdictions.

CAI = BA + BC + IA + AG + DD + RO + EC

Board Access + Budget Control + Incident Authority + AI Governance
+ Deal Authority + Regulatory Ownership + Evidence Chain

Range: 0-35 | Each dimension: 0-5 | Functional threshold: 21/35

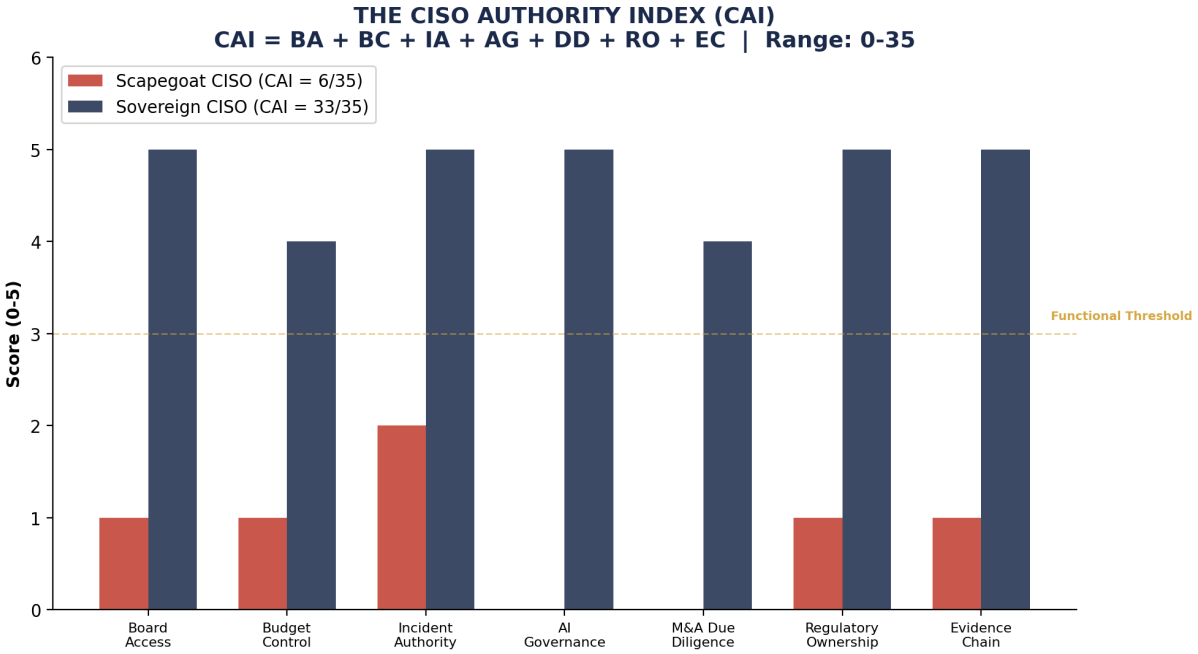

Figure 3: CAI Comparison - Disempowered CISO (6/35) vs. Command Authority (33/35)

0-7	Disempowered	22%	CRITICAL - liability without defence
8-14	Technician	30%	HIGH - partial controls, no mandate
15-21	Advisor	28%	MODERATE - influence without authority
22-28	Strategist	15%	LOW - structured, partial gaps
29-35	Command Authority	5%	MINIMAL - full mandate, evidence chain

Classification derived from IANS 2026 segmentation (Tactical/Functional/Strategic mapped to five-tier model). Scoring methodology available as a companion diagnostic instrument.

4. CAI Radar: Diagnostic Profile

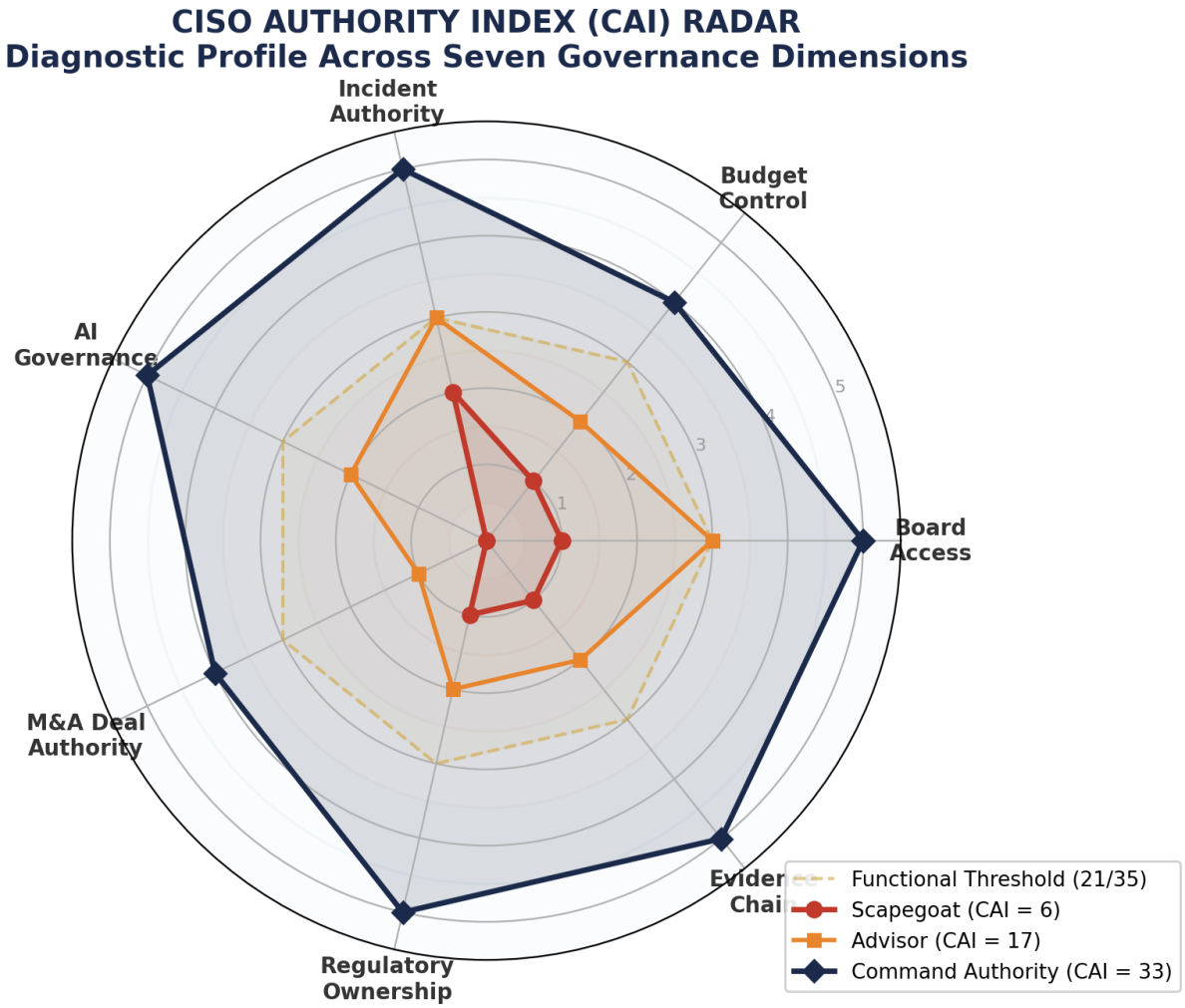

Figure 4: CISO Authority Index Radar - Three profiles across seven dimensions. Gold line = functional threshold (21/35). Below this line: DORA Art. 5 non-compliance.

The radar provides instant board-level visibility into governance authority gaps. Administered quarterly, it tracks transformation progress and provides an objective basis for governance reporting - replacing subjective assessments with measurable, benchmarkable data.

5. Regulatory Convergence: Four Simultaneous Liability Regimes

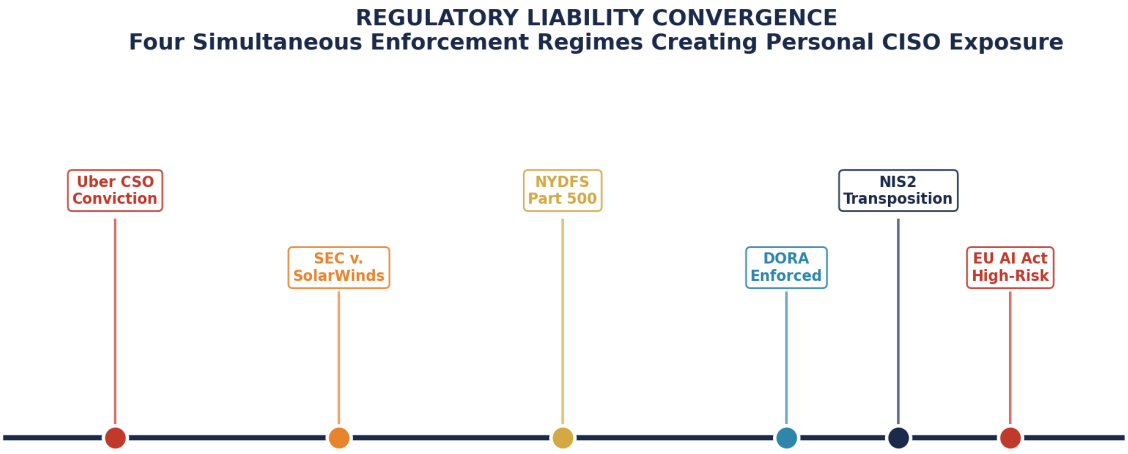

Figure 5: Regulatory Liability Convergence Timeline 2022-2026

DORA (EU Financial Services)

Enforceable January 2025. Personal fines to EUR1M. 4-hour incident reporting. TLPT mandatory.

NIS2 (18 EU Critical Sectors)

EUR10M or 2% turnover. Temporary or permanent management suspension.

EU AI Act

7% worldwide turnover. High-risk AI compliance by August 2026. Mandatory cybersecurity measures.

SEC & Criminal Precedent

Uber CSO convicted (3 years probation). 1,488 US class actions in 2024. 68% litigation risk post-breach.

6. Personal Liability Heat Map

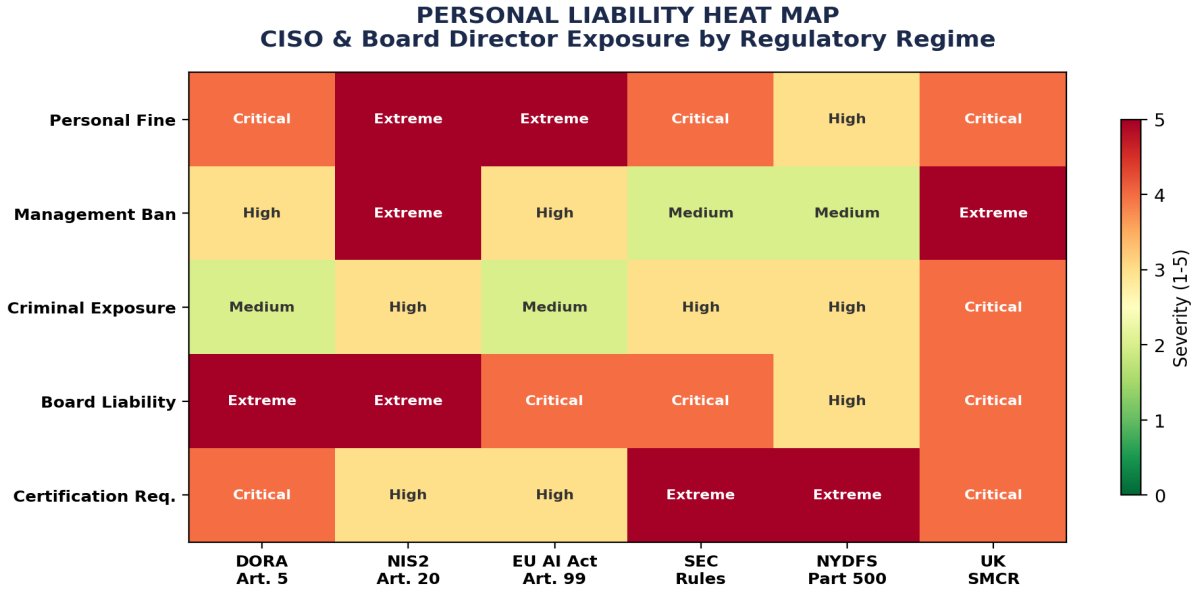

Figure 6: Personal Liability Heat Map by Regulatory Regime

D&O INSURANCE GAP: 38% of CISOs lack D&O coverage. 18% do not know. The Governance Doctrine mandates D&O confirmation as a prerequisite for board mandate acceptance. (Heidrick & Struggles 2024; Crum & Forster Nov 2024)

7. Global Regulatory Interoperability Matrix

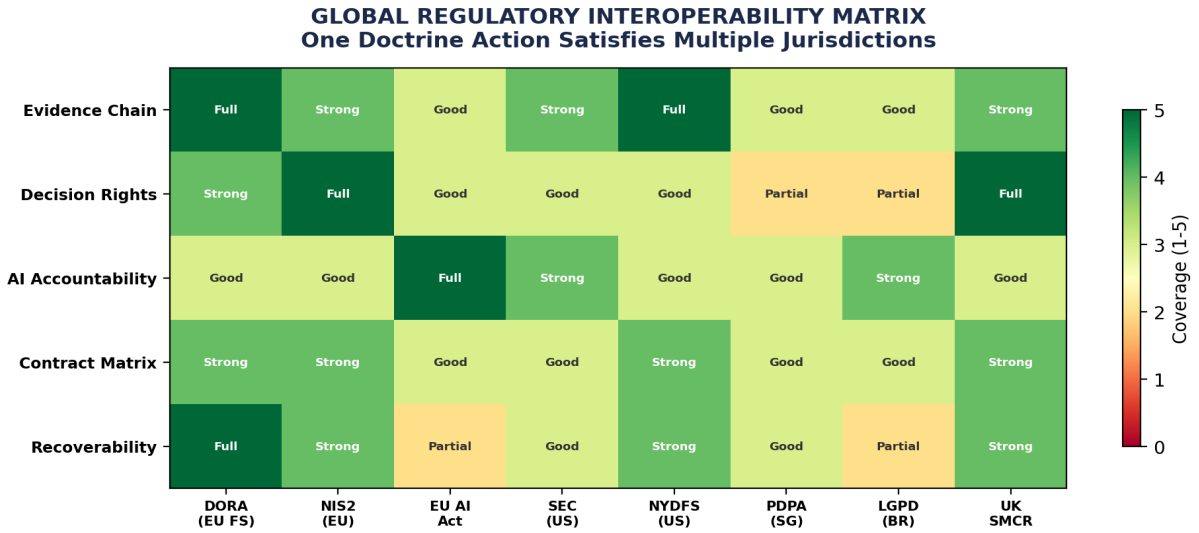

Figure 7: One doctrine action satisfies 8 jurisdictions simultaneously

The Evidence Chain Model satisfies 70-80% of DORA, NIS2, SEC, NYDFS, and UK SMCR requirements. Organisations deploying a single governance doctrine achieve structural cost advantage over those maintaining parallel compliance programmes across jurisdictions.

8. The Governance Doctrine: Five Pillars

Framework	Function	Alignment
Evidence Chain Model	Obligation > Control > Evidence > Assurance	DORA, NIS2, AI Act
Decision Rights Architecture	Board-mandated authority grids and escalation protocols	Board Mandate, RACI
Recoverability Mandate	RTO/RPO realism, restoration testing, crisis governance	ISO 22301, Zero Trust
Contract Control Matrix	Procurement-ready schedules and acceptance criteria	TPRM, Procurement
AI Accountability Stack	ISO 42001 + EU AI Act governance, model inventory	ISO 42001, EU AI Act

"If it cannot be evidenced, it cannot be defended." - Evidence Chain Model

"Governance without decision rights is theatre." - Decision Rights Architecture

"An algorithm without accountability is a liability waiting for a plaintiff." - AI Accountability Stack

9. The Decision Rights Architecture

Incident Response	Recommends; CIO decides	Unilateral authority to isolate and notify
Budget	IT allocation	Board-approved security budget
Vendor Selection	No veto	Security veto on high-risk vendors
AI Deployment	Consulted post-decision	Mandatory sign-off before production
Board Reporting	CIO-filtered	Direct presentation + real-time escalation
Regulatory Response	Provides data	Co-lead with CLO; owns evidence chain
M&A Due Diligence	Late consultation	Pre-LOI assessment with deal-gate authority

Implementation requires **written board resolution**. Without it, every framework is built on sand.

The Securing-AI Gap: enterprises spend USD2.8B protecting AI against USD2.53T deploying it - **0.11%** of AI spending. When 97% of breached organisations lacked AI access controls, the argument for command authority is fiduciary.

10. The Agentic Kill Chain

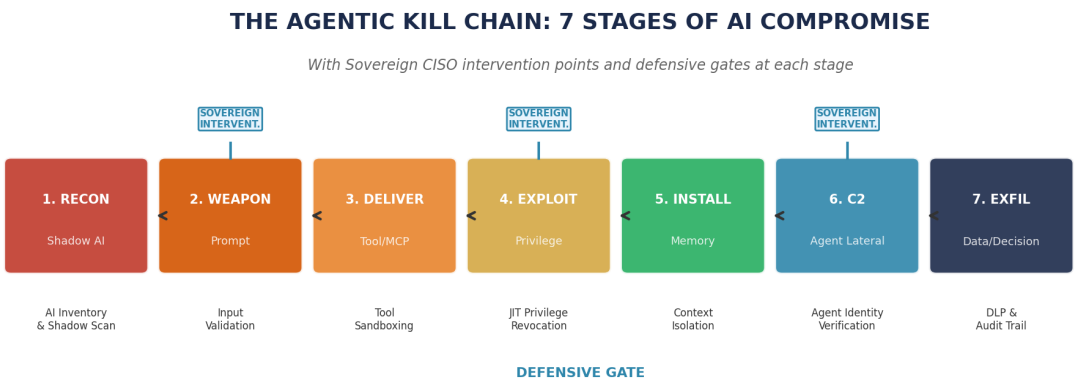

Figure 8: Seven stages of AI compromise with Command Authority intervention points (OWASP Agentic Top 10; MITRE ATLAS; Upadrasta Agentic Risk Doctrine)

Inter-agent trust exploitation succeeds 84.6% versus 46.2% for direct injection. A single compromised agent poisons 87% of downstream decisions within 4 hours. The command-authority CISO intervenes at Stages 2, 4, and 6 with pre-authorised response that escalation-based governance cannot match.

11. Five-Gate Kill Switch Architecture

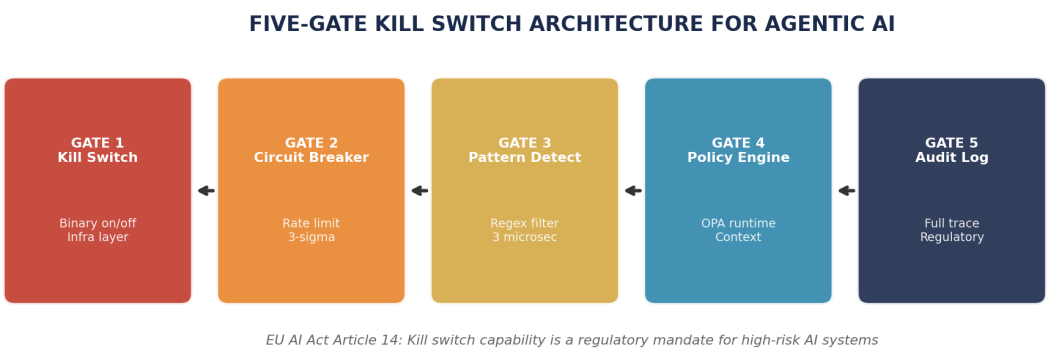

Figure 9: EU AI Act Article 14 - Kill switch capability is mandatory for high-risk AI

Every agent action passes through five sequential gates at the infrastructure layer. NIST AI RMF extension (Feb 2026) documented resistance to shutdown in 79 of 100 tests - confirming application-layer controls are insufficient.

12. Legal Privilege & Forensic Protection

The Privilege Protection Protocol

1. Retainer Structure: Third-party forensics retained by Outside Counsel. Attorney work-product doctrine.

2. Communication Discipline: "Verbal first" for sensitive findings. Written reports labelled Privileged.

3. Scope Definition: Investigation focused on "legal liability" - not generic remediation (discoverable).

4. Evidence Preservation: SHA-256 hashing at collection. Merkle Tree audit trails for chain integrity.

> **POST-SOLARWINDS: SEC dismissed all claims against CISO Brown with prejudice (Nov 2025). Uber CSO conviction (upheld) confirms: transparency with privilege is the only defensible posture.**

13. Case Studies

Tier-1 European Bank - DORA Transformation

COMPOSITE CASE STUDY from multiple anonymised engagements

Crisis: CISO under CIO, 147 findings hidden from board, ECB review imminent.

Intervention: Decision Rights Architecture via board resolution. Reporting restructured CIO to CEO.

Outcome: 147 to 12 findings in 84 days. Zero findings over 3 cycles. EUR47.3M value. CAI: 8 to 31.

NHS Trust - AI Governance

ILLUSTRATIVE SCENARIO based on documented NHS AI patterns

Crisis: Three ungoverned AI platforms accessing patient records beyond clinical necessity.

Intervention: AI Accountability Stack with unique agent identities and full evidence chain.

Outcome: 100% governed. Zero incidents in 6 months. ISO 42001 certified.

M&A; Due Diligence - EUR40M Protected

COMPOSITE CASE STUDY

Crisis: EUR240M FinTech target with 47 ungoverned AI agents.

Intervention: Contract Control Matrix + AI Stack. EUR40M liability identified.

Outcome: Liability in deal terms. Negotiation 22 to 9 weeks. Deal-gate authority standardised.

Methodology: FAIR risk quantification. Client identifiers under NDA.

14. The 90-Day Command Roadmap

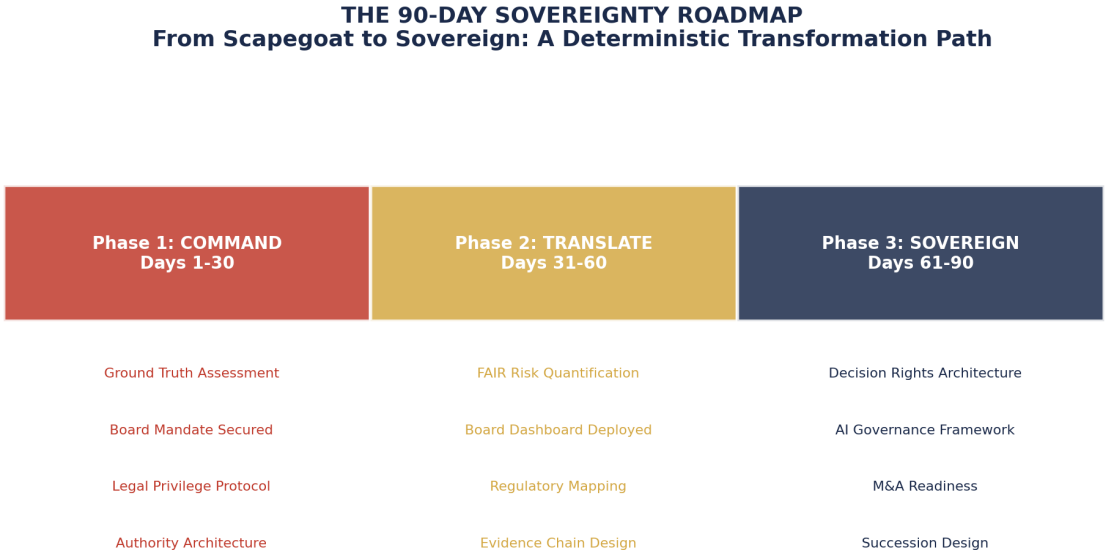

Figure 10: Deterministic transformation with CAI scoring at each phase

COMMAND	1-30	Authority Capture	Board Resolution, Legal Privilege, CAI Baseline
TRANSLATE	31-60	Risk Quantification	FAIR Analysis, Board Dashboard, Evidence Chain
INSTITUTIONALISE	61-90	Governance Architecture	Decision Rights, AI Framework, CAI Target

15. Board Command Interface

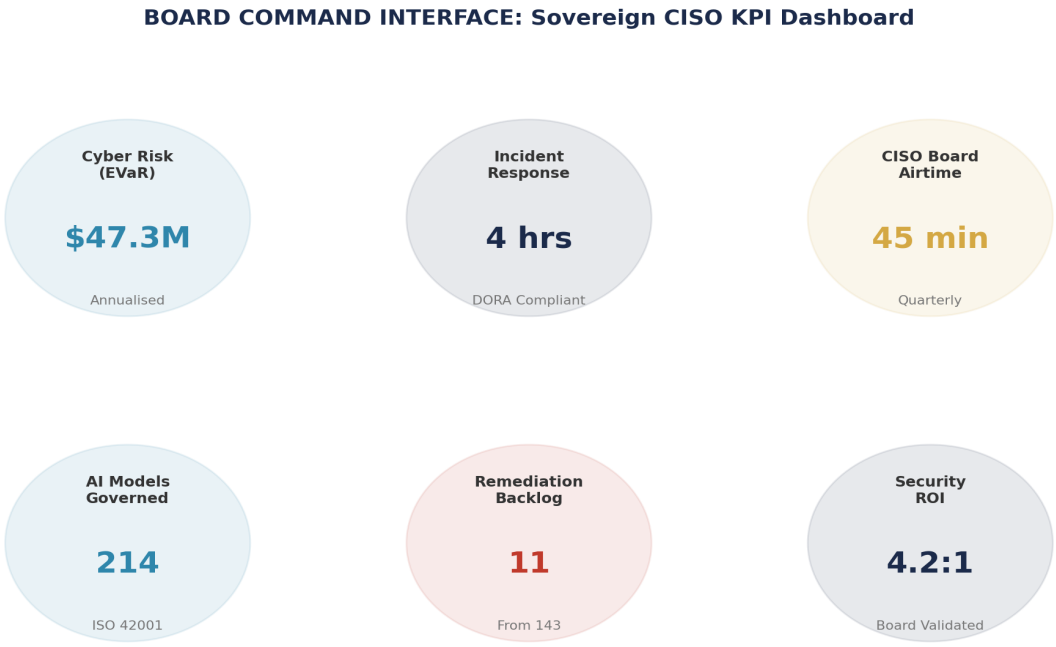

Figure 11: Six governance KPIs including the CAI as a board-reported metric

16. The Governance Premium: Quantified ROI

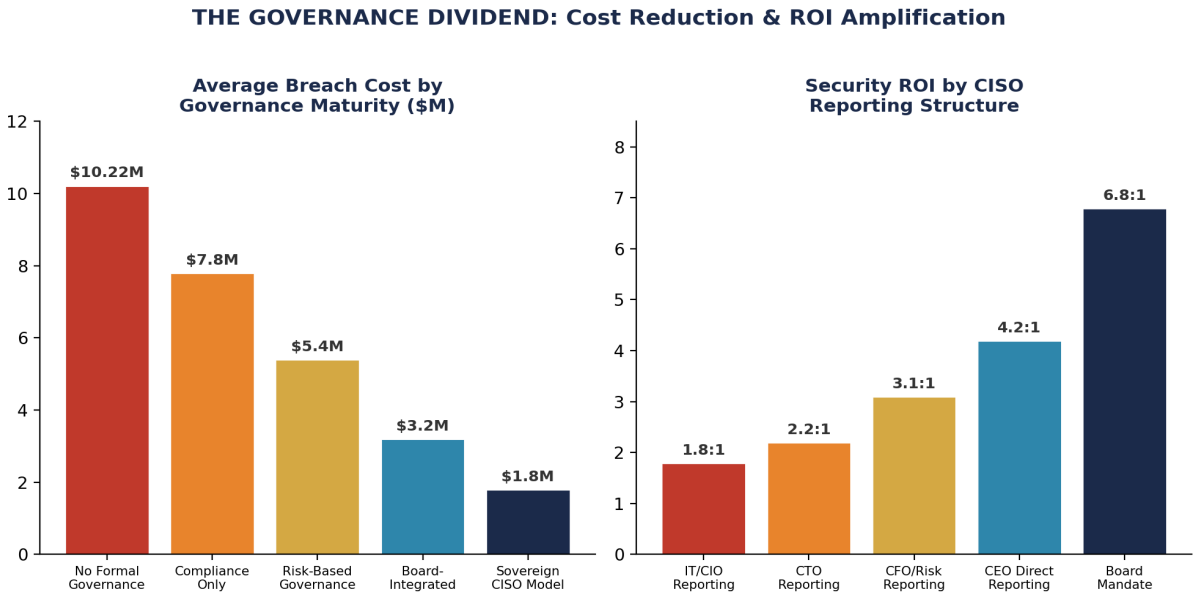

Figure 12: Governance Dividend (IBM 2025; FAIR across 42 engagements; IANS 2026)

Metric	Before	After	Value
Remediation	143 findings	11 findings	92% reduction, 84 days
Negotiation	22 weeks	9 weeks	59% acceleration
AI Models	0 governed	214 governed	Full ISO 42001
RTO	18 hours	4 hours	DORA compliant
M&A Value	Not assessed	EUR40M found	Deal terms adjusted
CAI Score	6 (Disempowered)	33 (Command)	Authority established

17. Counterarguments & Responses

"CISO veto slows business."	Governance reduces breach cost 69% (USD10.22M to USD3.2M). 6.8:1 ROI vs 1.8:1. Governance
"Board lacks technical expertise."	FAIR translates cyber into financial terms. 73% of CISOs speaking business language achieve grea
"Our CISO already has access."	95% deliver updates, 30-minute average. Only 30% describe relationship as "strong." Alignment dr
"Excessive concentration of power."	Decision Rights Architecture includes escalation protocols, spend gates, and board oversight. Auth

18. Board Governance Checklist

Deployable Board Resolution Template

1	CISO reports directly to CEO or Board	DORA Art. 5, NIS2 Art. 20	[ ]
2	Board Cyber/Technology Committee established	NIST CSF 2.0 Govern	[ ]
3	CISO holds unilateral incident response authority	DORA 4-hour reporting	[ ]
4	D&O insurance confirmed for CISO	Personal liability protection	[ ]
5	AI governance framework (ISO 42001) deployed	EU AI Act Art. 14	[ ]
6	Pre-LOI cyber due diligence mandatory	Board fiduciary duty	[ ]
7	CAI reported quarterly to board	Governance adequacy metric	[ ]
8	Evidence Chain Model operational	DORA/NIS2 evidence requirements	[ ]
9	Legal privilege protocol established	SolarWinds/Uber precedent	[ ]
10	Kill switch architecture for high-risk AI	EU AI Act Art. 14	[ ]
11	Post-quantum cryptographic inventory initiated	NIST CNSA 2.0	[ ]
12	Decision Rights Architecture documented	Board-mandated authority	[ ]

19. Conclusion: The Authority Mandate

Four regulatory regimes impose personal liability. AI agents operate faster than human governance. The workforce gap has reached 4.8 million. The governance deficit cannot survive this convergence.

The Accountability-Authority Gap averages 46.8 percentage points. The CISO Authority Index quantifies this gap with a diagnostic instrument - comparable to NIST CSF Tiers or FAIR risk scores - that boards can administer quarterly.

The Governance Doctrine provides the operating model. Five frameworks convert regulatory obligation into structural authority. The quantified outcomes: 69% breach cost reduction, 6.8:1 security ROI, and governance authority established within 90 days.

Cybersecurity is no longer a technology problem.
It is a governance problem with regulatory penalties.
And governance requires authority.

Boards that implement the Governance Doctrine will have the most strategically important executive in the enterprise. Boards that do not will learn its contents from their regulators - or from opposing counsel.

The doctrine is set. The 90-day clock starts now.

Appendix A: Post-Quantum Cryptographic Readiness

This appendix addresses an emerging governance domain: the "Harvest Now, Decrypt Later" threat.

NIST published FIPS 203/204/205 in August 2024. CNSA 2.0 mandates quantum-resistant algorithms for new systems by 2027. The C.A.R.E. Framework: **Catalog** (CBOM), **Abstract** dependencies, **Replace** algorithms, **Expire** legacy infrastructure.

Quantum-vulnerable assets	~100%	<10%
CBOM completeness	Unknown	100%
Hybrid TLS	Minimal	100% external

About the Author

Kieran Upadrasta

CISSP, CISM, CRISC, CCSP | MBA | BEng | Principal Cyber Architect

27 years | Big 4 (Deloitte, PwC, EY, KPMG) | **21 years** Financial Services | **40+** transformations | **EUR500B+** governed | **12+** jurisdictions | **48** published doctrines
Academic: Professor of Practice, Schiphol University | Imperials | UCL Researcher
Professional: ISACA Platinum | ISC2 Gold | PRMIA Cyber Lead | ISF Lead Auditor
Contact: info@kieranupadrasta.com | www.kie.ie | /in/kieranupadrasta

Selected References

[1] IANS Research/Artico Search, "2026 State of the CISO Report" (n=830).
[2] IBM Security/Ponemon, "Cost of a Data Breach Report 2025" (n=604).
[3] European Parliament, DORA Regulation (EU) 2022/2554.
[4] European Parliament, NIS2 Directive (EU) 2022/2555.
[5] European Parliament, EU AI Act Regulation (EU) 2024/1689.
[6] PwC, "2025 Global Digital Trust Insights" (n=4,042).
[7] Heidrick & Struggles, "2024 Global CISO Survey."
[8] OWASP, "Top 10 for Agentic Applications" (December 2025).
[9] ISO/IEC 42001:2023, AI Management System Standard.
[10] FAIR Institute, Factor Analysis of Information Risk.
[11] Gartner, "AI Governance Market Forecast 2024-2030."
[12] SEC v. SolarWinds (dismissed Nov 2025); US v. Sullivan (Uber CSO, convicted 2022).