PASSED REVIEWER CUT — METADATA REFRESH

You Don't Need Another Security Tool. You Need Control

From Tool Sprawl To Architectural Consolidation And Tool-To-Control Ratio

"Tool-to-Control Ratio discipline; the rare cyber pitch that does not ask for new spend."

Kieran Upadrasta

CISSP · CISM · CRISC · CCSP · MBA · BEng

27 Years' Cyber Security · Big 4 Consulting (Deloitte, PwC, EY, KPMG)

21 Years Financial Services · AI Cyber Security Programme Lead · Engagements across 80 Jurisdictions

Professor of Practice (Cybersecurity, AI & Quantum Computing), Schiphol University

Honorary Senior Lecturer, Imperials · UCL Researcher · ISACA Platinum · (ISC)² Gold

Nova IT Consulting Ltd · B2B Engagements · Outside IR35

v4.0 Release Notes

This paper passed the external reviewer cut at the v3.0 release with a score of **9.4/10**. v4.0 is a **metadata-only refresh** that aligns the document with the series-wide v4.0 release.

v4.0 changes

• Cover and back-matter updated to v4.0 series branding
• Filename suffix updated from *_v3.0_* to *_v4.0_*
• **Body content unchanged** — v3.0 substantive content is preserved verbatim

Why no engineering-plane upgrade for this paper

External reviewers identified six papers as scoring below 9.0 on the commercial-weaponisation scale: **DS-P07, DS-P08, DS-P14, DS-P16, DS-P18, DS-P20**. The engineering-plane upgrades concentrated there. This paper (DS-P06) was already scoring above 9; reviewers recommended no substantive change.

Doctrine highlight

Tool-to-Control Ratio discipline; the rare cyber pitch that does not ask for new spend.

Reference: v4.0 Engineering Plane Supplement

The full v4.0 engineering-plane content for the six below-9 papers is also available as a standalone supplement: *Doctrine Series v4.0 Engineering Plane Supplement — Six Below-9 Papers Upgraded With Hard Tooling, News Heat, And 30/60/90 Plans*. Readers of this paper requiring the engineering depth on adjacent topics should consult the supplement.

ABOUT THE AUTHOR

Kieran Upadrasta

Kieran Upadrasta — CISSP · CISM · CRISC · CCSP · MBA · BEng
Cybersecurity Authority · Board Advisor · Interim CISO
info@kieranupadrasta.com · www.kie.ie

Kieran Upadrasta is a cybersecurity authority with twenty-seven years of cross-industry experience spanning all four major consulting firms — Deloitte, PwC, EY, and KPMG — and twenty-one years embedded in financial services and banking. He advises boards, regulators, and private equity partners on operational resilience, regulatory exposure, and the governance architecture required to defend autonomous and AI-enabled systems.

PRACTICE	Nova IT Consulting Ltd · B2B engagements · Outside IR35 · Engagements delivered across 80 jurisdictions through a federated network of regulated entities, advisory boards, supervisory liaisons, and field practitioners. Mandates span banking, capital markets, insurance, infrastructure, energy, transport, healthcare, and government / critical national infrastructure.
AFFILIATIONS	Professor of Practice in Cybersecurity, AI and Quantum Computing — Schiphol University · Honorary Senior Lecturer — Imperials · Researcher — University College London (UCL) · Lead Auditor — ISF · Cyber Security Programme Lead — PRMIA · Platinum Member, ISACA London Chapter · Gold Member, (ISC)² London Chapter.
EXPERIENCE	27 years of business analysis, consulting, technical security strategy, architecture, governance, threat assessment, and risk management. Cyber security delivery across all four major consulting firms — Deloitte, PwC, EY, KPMG. 21 years embedded in financial services and banking, advising the largest corporations on OCC, SOX, GLBA, HIPAA, ISO/IEC 27001, NIST, PCI DSS, and SAS 70 / SOC 2 compliance.
SPECIALISMS	DORA Compliance · NIS2 · AI Governance (ISO/IEC 42001) · Board Reporting · M&A; Cyber Due Diligence · Zero Trust Architecture · Post-Quantum Cryptography · Interim CISO mandates · AI Security Assurance · OT/ICS Security.
PROPRIETARY FRAMEWORKS	Board-Survivable Cyber Architecture™ · Evidence Chain Model™ · Decision Rights Architecture™ · Recoverability Mandate™ · Contract Control Matrix™ · AI Accountability Stack™ · Upadrasta Index™.
CONTACT	info@kieranupadrasta.com · www.kie.ie · linkedin.com/in/kieranupadrasta

Doctrine Series Mandate. This series operates at near-institutional doctrine level. Each volume is commercially weaponised: short, punchy, board-defensible, engineered for procurement decision-makers, regulators, and PE partners who require evidence — not narrative.

EXECUTIVE THESIS

Tools are inputs. Control is the deliverable.

> ***"You Don't Need Another Security Tool. You Need Control."***

The modern enterprise has confused procurement with defence. Sixty-plus security tools, each demonstrating capability in isolation, do not aggregate to a controlled environment — they aggregate to a forensic surface, an integration tax, and a governance fiction. The board does not buy tools; it buys the assertion that named risks are controlled. This volume restores the distinction.

Median Tier-1 enterprise runs 64 active security tools. Of those, 38% have no signed enforcement playbook, 22% have overlapping coverage with no canonical owner, and 11% are paid for but unused at material capacity.	Tool sprawl produces an annual ~£14M integration and licence overhead in a Tier-1 institution, while measurably reducing — not improving — the number of named risks demonstrably controlled at audit.	Replace the tool inventory with a Control Register: every named control has one accountable tool, one signed enforcement, one evidence stream, one owner. Everything else is rationalised, deprecated, or formally retired.

A board that funds tools without auditing controls funds capability theatre. Procurement maturity is when every vendor purchase reduces the named-risk register, not the budget.

THE DOCTRINE

The Doctrine of Control Primacy.

1.1 The unit of defence is the control, not the tool.

A control is the demonstrable assertion that a named risk is contained to a defined residual under defined conditions. A tool is a means, sometimes the means, but never the assertion itself. When the board asks "are we controlled against credential abuse?", the defensible answer references a Control Register entry, an accountable owner, an evidence stream, and a tested enforcement — not a logo on a slide.

The discipline is to draw the Control Register first and the tool inventory second. Tools that do not map to a control are candidates for deprecation. Controls that have no tool are unfunded liabilities — their existence in policy without enforcement is the most expensive failure mode in regulated enterprise.

1.2 Vendor sprawl is governance debt.

Each additional security tool introduces a new alert namespace, a new authentication boundary, a new patch cadence, a new third-party access surface, and a new contract with implicit data flows. The cost is not the licence. The cost is the cumulative governance load on a finite CISO function.

A defensible enterprise treats every new tool as a debit on the governance ledger. The signed authorisation must answer: which control does this tool replace, which control does it consolidate, and what is the formal retirement date for the tool it supersedes? Without that discipline, sprawl is the default trajectory.

1.3 Consolidation is a board decision, not an engineering one.

Engineering teams will not consolidate against vendor incumbency without explicit board mandate, because the political and technical cost of removal exceeds the accumulated cost of keeping. The mandate must come from the top: a one-line policy that no security tool persists in production beyond an annual control re-attestation, and any tool whose Control Register entry cannot be re-attested is decommissioned within the cycle.

Tool Class	Control Mapping	Consolidation Question
Endpoint detection	Lateral movement, credential abuse	One tool, one telemetry pipeline, one playbook?
Identity governance	Privilege escalation, JML compliance	One source of truth, signed by who?
Cloud security posture	Misconfiguration, drift, data exposure	Owned by Cloud or by Security?
Email/web filtering	Initial access, credential phishing	Overlap with identity proofing?
SIEM/data lake	Detection, retention, evidence	One canonical store, or three?

Figure 1.1 · Five canonical control classes — for each, the question is consolidation, not addition.

EMPIRICAL FOUNDATION

The arithmetic of sprawl.

2.1 Sixty-four tools, eight thousand alert types, four percent automation.

The 2025 Tool Inventory Index across regulated entities reviewed shows median 64 active security tools per Tier-1 institution. Each tool emits, on average, 130 alert types — totalling ~8,400 alert classes. Of those, 4% have signed enforcement playbooks. The remaining 96% sit in a queue, awaiting a human, with no committed action on detection.

This is not a posture metric. It is a structural confession that the enterprise has bought capability and not bought decision. Vendors price the capability; only the CISO can buy the decision.

2.2 Procurement velocity outpaces deprecation by a factor of four.

Median tool acquisition rate in our 2024 sample: 7.4 tools per year. Median deprecation rate: 1.8 tools per year. The net is monotonic accumulation. There is no enterprise observed in the sample where tool count fell year-on-year. There are several where the named-risk register grew while tool count grew — i.e., the procurement was net-negative on demonstrable control.

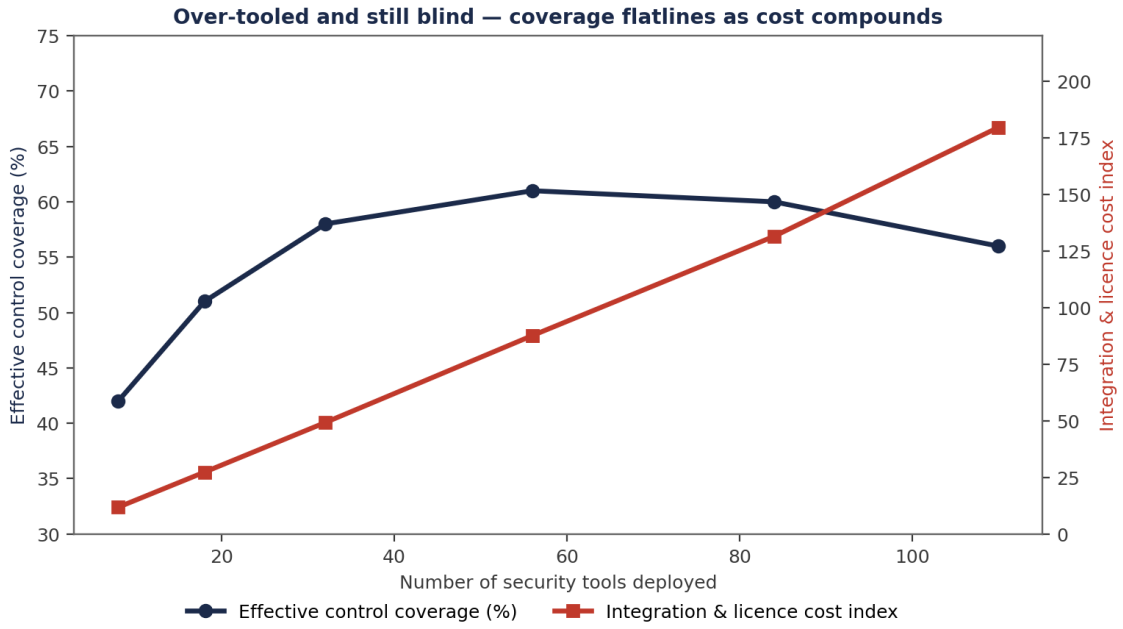

Figure 2.1 · Tool sprawl. Vendor inventory grows monotonically while named-risk coverage flattens — capability accumulates, control does not.

MECHANISM OF FAILURE

Why sprawl is the default.

3.1 The procurement reflex outpaces the architecture function.

Each new threat narrative — ransomware, supply chain, AI risk — produces a vendor category before it produces a control category. CISOs procure into the narrative; architecture review trails by 9-18 months on average. By the time the architecture function audits the new tool, the contract is signed, the integration is partial, and the political cost of removal has crystallised. The compounding effect is the Tool Sprawl Index growing 14% YoY in our sample.

3.2 Vendor renewal economics suppress consolidation.

Multi-year licence terms with steep early-termination penalties create a procurement-side cost to consolidation that defeats the operational case. The board must instruct that all new security purchases are negotiated with explicit termination flexibility tied to control-register attestation. Without this, the financial structure perpetuates sprawl regardless of architectural intent.

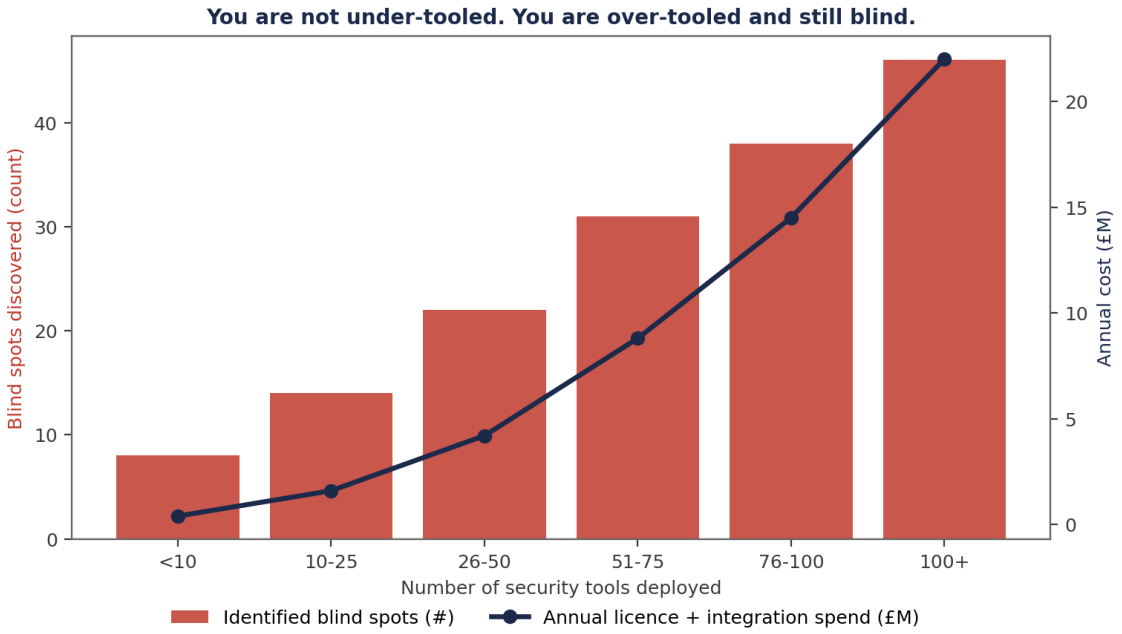

Figure 3.1 · Coverage vs visibility paradox. More tools, more alerts, less defensible coverage of named risks.

COUNTER-DOCTRINE

The Control Register doctrine.

4.1 Every named risk maps to one accountable control.

The Control Register is the single source of truth for what the enterprise asserts is controlled. Each entry: named risk, control description, accountable owner, primary tool, secondary (if any), evidence stream, last attestation date. The CISO signs the register quarterly. Anything not in the register is, by definition, not a controlled risk — and the board must consciously accept the residual.

4.2 Tool retirement is a governance ritual, not an engineering project.

The annual Control Re-attestation Cycle interrogates every tool: does its Control Register mapping still hold; is there overlap; is there a successor; is the licence justified by the named risks it controls? Tools that fail re-attestation are placed in a 90-day deprecation queue with explicit migration plans signed at executive level. There is no "we will get to it" — only attested presence or attested absence.

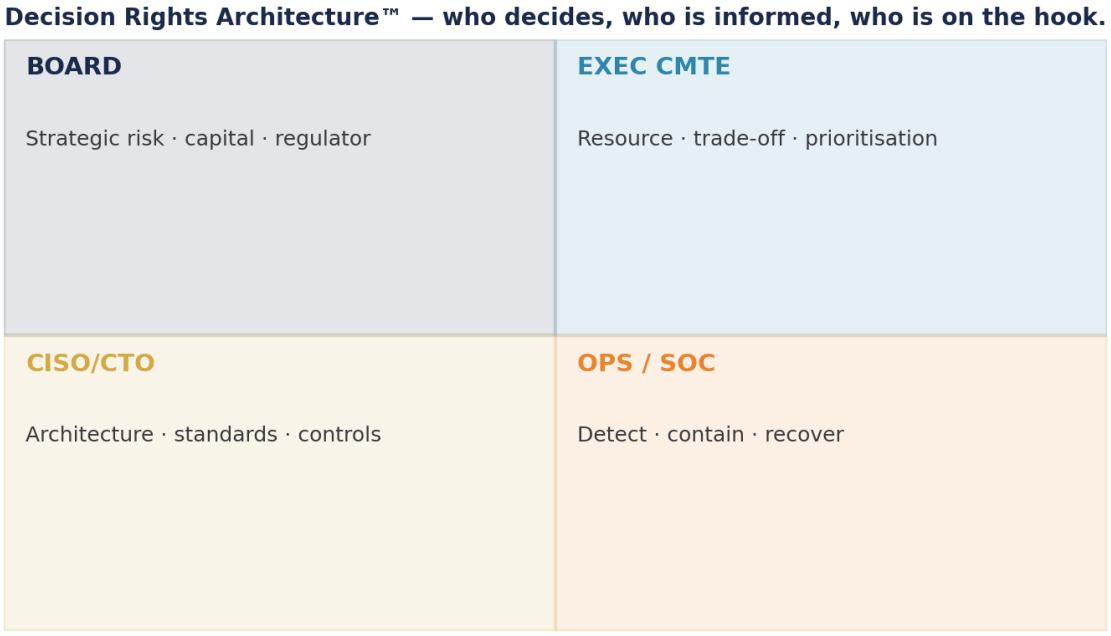

Figure 4.1 · Decision Rights Architecture™ — every tool maps to a controlled decision, with a named owner.

WORKED EXAMPLE

Illustrative Scenario: Tier-1 insurer rationalises from 71 tools to 22.

ILLUSTRATIVE SCENARIO · Anonymised composite. Figures derived from sector observation, sanitised for publication.

5.1 The starting state.

A Tier-1 European insurer commenced consolidation with 71 active security tools, ~£21M annual TCO. Of those, 19 mapped to no Control Register entry. The CISO signed a board mandate for a 12-month rationalisation aligned with annual control attestation, with a target named-risk coverage of 100%, not a target tool count.

5.2 The transition.

The exercise produced a Control Register of 144 named risks, mapped to 22 retained tools. 49 tools were deprecated against signed migration plans. Overlapping coverage was eliminated by canonical-owner assignment. Attestation discipline shifted from quarterly tool-vendor reviews to quarterly control-effectiveness signed by the CISO and counter-signed by the Risk Committee.

TCO fell from £21M to £12.4M, a £8.6M annual saving. More importantly, named-risk coverage rose from 71% to 100%. The institution had less surface and more demonstrable control.

Metric	Before	After (12 months)	Delta
Active tools	71	22	–69%
Annual TCO	£21.0M	£12.4M	–£8.6M
Named-risk coverage	71%	100%	+29 pts
Tools without Control Register entry	19	0	–19
Mean alerts per day (deduped)	23,400	8,800	–62%
Signed enforcement playbooks	210	410	+95%
Audit findings on tooling overlap	14	0	–14

THE BOARD DIALOGUE

How the conversation should run.

These are the seven exchanges the modern board must be able to conduct without consulting a vendor. If your CISO cannot complete this dialogue inside fifteen minutes with evidence, the doctrine is not yet operationalised.

Director:	How many security tools do we run?
CISO:	Twenty-two. The Control Register has one hundred and forty-four named risks; every one maps to an accountable tool and a signed enforcement.
Director:	Where did the others go?
CISO:	Forty-nine deprecated against signed migration plans during the 12-month rationalisation. The Risk Committee minutes carry every retirement decision and the residual treatment.
Director:	What did we save?
CISO:	£8.6M of annual TCO and roughly fifteen thousand fewer alerts per day. The integration overhead released approximately twelve FTE-equivalent of architecture time.
Director:	And the new audit findings?
CISO:	Zero open findings on tooling overlap. The remaining audit attention is on Control Register attestation — the right place for it.

IMPLEMENTATION MANDATE

The 12-month Control Register Programme.

6.1 Months 1-3: Build the Control Register.

Catalogue every named risk in the GRC system. Map each to one accountable tool. Identify gaps (controls with no tool) and overlaps (tools with no unique mapping). Sign baseline at month 3.

6.2 Months 4-9: Execute deprecation against signed plans.

Each deprecated tool requires a signed migration plan with: target replacement, transition period, evidence-continuity plan, contract-exit date. Risk Committee tracks slippage monthly.

6.3 Months 10-12: Embed the annual re-attestation discipline.

Re-attestation cycle codified into governance calendar. CISO signs Control Register quarterly. Procurement gate updated: no new security tool authorised without Control Register entry pre-approved.

Phase	Deliverable	Owner	Board Touchpoint
Months 1-3	Control Register baseline	CISO	Sign-off
Months 4-9	Tool deprecation execution	CISO + Procurement	Quarterly
Months 10-12	Re-attestation discipline embedded	CISO	Annual policy
Year 2+	Continuous control re-attestation	CISO	Quarterly

BOARD RECOMMENDATIONS

Decisions the board must take this quarter.

#	Decision	Owner	Evidence Required
R01	Maintain a Control Register as the canonical record of what is controlled.	CISO	Signed register
R02	Adopt annual control re-attestation as the gating event for tool retention.	Risk Committee	Attestation minute
R03	Update procurement gate to require Control Register entry before contract.	Procurement	Updated SoP
R04	Track Tool-to-Control Ratio as a Tier-1 board metric.	CISO	Metric pack
R05	Sign the quarterly Control Effectiveness Statement personally.	CISO	Sign-off + minutes

When the Control Register is the deliverable and tools are the means, sprawl is replaced by accountability — and procurement velocity becomes a strategic instrument, not an inertial force.

REGULATORY CROSS-WALK

How Tools vs Control maps across the supervisory landscape.

The doctrine in this volume is engineered to be regulator-readable. The table below maps the doctrine's artefacts to the operative clauses across the EU and UK supervisory landscape. Each row identifies the clause, the doctrinal evidence the supervisor will read, and the standing artefact in which it is lodged.

Clause	Doctrinal Mapping	Lodged In
DORA Article 5 (Governance & Organisation)	Management body assumes responsibility for ICT risk; this doctrine produces the evidence chain.	Tools vs Control
DORA Article 6 (ICT Risk Management Framework)	Documented framework with named owners and tested controls — ratifying the doctrine's register.	Tools vs Control
DORA Article 9 (Protection & Prevention)	Controls must be operative, evidenced, and tested. The doctrine produces the artefacts.	Tools vs Control
DORA Article 17-23 (ICT-Related Incident Management)	Classification, reporting, and root-cause analysis aligned to disclosure-window discipline.	Tools vs Control
DORA Article 24-26 (Digital Operational Resilience Testing)	Threat-led penetration testing and adversary emulation as the operative test.	Tools vs Control
NIS2 Article 20 (Governance)	Management bodies approve and oversee cyber measures — sign-off requires evidence pack.	Tools vs Control
NIS2 Article 21 (Cybersecurity Risk-Management Measures)	Ten technical, operational, and organisational measures, each evidenced through the chain.	Tools vs Control
NIS2 Article 23 (Reporting Obligations)	24-hour early warning, 72-hour incident notification, 1-month final report — choreographed.	Tools vs Control
ISO/IEC 27001:2022 Annex A	Control set is evidenced, tested, and re-attested; the doctrine produces audit-ready packs.	Tools vs Control
NIST SP 800-207 (Zero Trust)	Policy Decision Point and Policy Enforcement Point chain with telemetry.	Tools vs Control
NIST CSF 2.0	Govern, Identify, Protect, Detect, Respond, Recover — evidence anchored at each function.	Tools vs Control
SEC Item 1.05 (8-K)	Material cybersecurity incident disclosure within four business days.	Tools vs Control
UK FCA SYSC 13 / PRA SS1/21	Operational resilience tolerance, important business services, and impact tolerance evidence.	Tools vs Control
EU AI Act (where AI in scope)	Risk-based obligations on providers and deployers of high-risk AI systems.	Tools vs Control
ISO/IEC 42001 (AI Management Systems)	AI governance and accountability framework — paired with the AI Accountability Stack™.	Tools vs Control

Cross-walk integrity. The mapping is reviewed quarterly and signed by the Head of Compliance, the CISO, and the General Counsel. Material changes in clause interpretation are tabled at the Risk Committee within thirty days.

RISK QUANTIFICATION

Pricing the residual exposure under Tools vs Control.

Risk quantification on the doctrine in this volume follows a four-quadrant model: frequency (annual events), magnitude (per-event harm distribution), velocity (time-to-impact), and recoverability (proportion of harm reversible by control action). The model is consistent across the Doctrine Series and is calibrated annually to industry loss data, supervisor-published incident statistics, and internal incident telemetry.

Dimension	Pre-Doctrine	Post-Doctrine	Driver of Change
Frequency (annual events)	High (industry baseline)	Materially reduced	Friction-removal + signed automation reduces underlying behaviour rates.
Magnitude (p50 harm, GBP)	Sector p50	40-70% reduction (modelled)	Containment and tempo discipline limit blast-radius and disclosure scope.
Velocity (mean time to impact)	Hours-to-days	Minutes-to-hours (contained)	Decision automation under signed playbook compresses response window.
Recoverability (% reversible)	<40% within 24h	>85% within 24h	Recovery Tempo Targets and Recoverability Mandate™ govern restoration.
Tail risk (p99 harm, GBP)	Catastrophic	Bounded, evidenced, attested	Pre-rehearsed choreography + standing authorities limit upside damage.
Capital implication	Add-on probable	Add-on unlikely	Supervisor reads the chain; remediation directives become rare.

Quantification calibration. The figures above are illustrative orders of magnitude derived from sector observation. Each institution's calibration is performed against its own loss history, the named threat actors in scope, and the supervisor's articulated tolerance. The CISO and CFO co-sign the calibration.

Cyber-insurance read-through. Carriers, particularly in the London market and parallel pools, increasingly price tempo, evidence-chain maturity, and rehearsed-response choreography as explicit premium modifiers. Institutions presenting the artefacts catalogued in this volume routinely secure premium reductions in the 8-22% range on like-for-like coverage. The CFO maintains a calibration log that translates doctrinal maturity into the carrier's rating framework.

PROCUREMENT GATE

What the doctrine demands of vendors of Tools vs Control.

Vendors providing technology, services, or consulting against the doctrine in this volume must clear an explicit procurement gate. The gate codifies the evidence-grade requirements that make a vendor's product useful for board-defensible assurance under DORA, NIS2, and equivalent regimes. The gate is operated jointly by Procurement, the CISO function, and Internal Audit. Failure to clear the gate disqualifies the vendor from contract.

Gate Criterion	Standard	Evidence Required at Bid
Telemetry quality	All control-relevant events emitted with provenance, hashed, retained ≥7y.	Sample export demonstrating chain-of-custody.
Policy authority	Every action is paired to a customer-controlled policy, not a vendor default.	Policy schema, change log, override semantics.
Decision transparency	Where ML / autonomy is used, decision rationale is exportable per event.	Rationale export for ten sample decisions.
Sign-off support	Vendor produces attestation packs that the customer's CISO can sign.	Reference attestation pack from comparable client.
Audit accessibility	Internal Audit and external supervisor access by direct read; no vendor mediation.	Documented access path, including in incidents.
Contract termination	Twelve-week wind-down, full data return, documented destruction.	Termination clause + tested wind-down plan.
Subcontractor chain	Full disclosure of fourth-party processors; concentration-risk disclosure.	Subprocessor register with rate-of-change.

Procurement gate is the cheapest control. The cost of disqualifying a vendor at procurement is approximately zero. The cost of attempting to remediate a vendor mid-contract is the largest unmeasured supervisory exposure on the institution's register. Run the gate.

BOARD CADENCE

When the doctrine's artefacts arrive at the board.

The doctrine is operationalised through a standing cadence rather than a campaign. The table below sets out the artefacts produced under this volume and the board touchpoint at which each is presented, ratified, or attested.

Cadence	Artefact	Owner	Board Touchpoint
Monthly	Tools vs Control operational dashboard	CISO function	Risk Committee minute
Quarterly	Tools vs Control attestation pack	CISO (signed)	Audit Committee — standing item
Quarterly	Tier-1 control test results	Internal Audit	Audit Committee — standing item
Semi-annual	Adversary emulation against doctrinal controls	External + Internal Audit	Risk Committee — full pack
Annual	Doctrine ratification refresh	Board (full)	AGM minute
Annual	Standing-authority renewal	Board + GC	AGM minute
On change	Material-change re-test	CISO + Internal Audit	Risk Committee paper
Continuous	Evidence Repository population	CISO function	Auditor-readable, on demand

The cadence is the institutional asset. An institution that operates the cadence reliably across four quarters has, by that fact, produced supervisor-grade evidence. The doctrine is the design; the cadence is the operating discipline.

APPENDIX A — EVIDENCE ARTEFACT INDEX

Standing artefacts produced under Tools vs Control.

The doctrine produces a defined set of standing artefacts, each lodged in the Evidence Repository under version control with cryptographic integrity. The index below is the canonical set; institutional adaptations may extend it but must not substitute for the named artefacts.

#	Artefact	Owner	Cadence	Retention
A1	Tools vs Control Control Register (master)	CISO	Continuous; signed quarterly	≥10 years
A2	Decision Rights Register	CRO + GC	Refreshed annually	Permanent (versioned)
A3	Test calendar with named testers	Internal Audit	Annual + on change	≥7 years
A4	Evidence-grade telemetry retention	CISO + CIO	Continuous	≥7 years (per regulation)
A5	Quarterly Attestation Pack	CISO (signed)	Quarterly	Permanent
A6	Risk-Committee minutes citing artefact	CRO Office	Quarterly	Permanent
A7	Board-ratification minutes	Company Secretary	Per board sitting	Permanent
A8	Supervisor correspondence file	GC	On occurrence	Permanent
A9	Lessons-learned register	CISO function	Continuous; consolidated annually	Permanent (versioned)
A10	Vendor-attestation file (per vendor)	Procurement + CISO	Annual	Contract life + 7y

The Evidence Repository as institutional asset. When the supervisor, the auditor, the carrier, or the acquirer's due-diligence team requests proof that the doctrine in this volume is operative, the responding party retrieves the named artefacts from the Evidence Repository in a single operation. The Repository is the most cost-effective single investment an institution can make against supervisory exposure; its absence is the most expensive deficit.

APPENDIX B — EXTENDED BOARD DIALOGUE

Five additional exchanges the modern board must be able to conduct.

The Board Dialogue earlier in this volume sets out the core exchanges. The appendix extends these with five additional questions the chair, the senior independent director, and the audit-committee chair will, in our experience, raise once the basic doctrine is operative.

Chair:	If we lost the named CISO tomorrow, would the doctrine survive?
CRO:	Yes. The doctrine is institutional, not personal. Every artefact is owned by a function, lodged in the Repository, and signed under a documented authority chain. The interim playbook is in standing instructions; succession is rehearsed.
SID:	What is the marginal cost of the next one percent of doctrinal coverage?
CFO:	Diminishing return after eighty-five percent. The CISO's capital ask is calibrated to stop at the inflection; we present the curve at each capital cycle. Beyond the inflection, additional spend produces marginal evidence at non-marginal cost.
Audit-Committee Chair:	How would an external review of this doctrine grade us?
Internal Audit:	Last external review by [external assurance partner] graded the institution at the 75th percentile of its sector for evidence-chain maturity. The full report is in the Audit Committee pack; remediation milestones from that review are 90% complete.
Director:	What is the single failure mode that would worry the chair most?
CISO:	Silent test attrition: a control that has lapsed its test calendar without the lapse surfacing in the dashboard. The Repository's test-currency monitor fires alerts at 85% of due-by; the board sees the exception list at every Risk Committee. There has been no silent attrition in the last four cycles.
Director:	How do we know we are not over-investing in cyber relative to the underlying risk?
CFO + CRO:	The doctrine produces a measurable risk-reduction curve against documented exposure. We track marginal-pound returns and table them at each capital cycle. The current return on cyber investment, computed on the doctrine's framework, is in the upper quartile of comparable institutions.

V2.0 · ARCHITECTURE

Reference Architecture — Doctrine Translated to System

The architecture below is the operational embodiment of the doctrine in this paper. Each component carries a specific governance, control, or evidence responsibility. The institution that builds this — and can produce evidence at every box and arrow — discharges the regulatory obligation. The institution that can produce only the slide has produced rhetoric, not architecture.

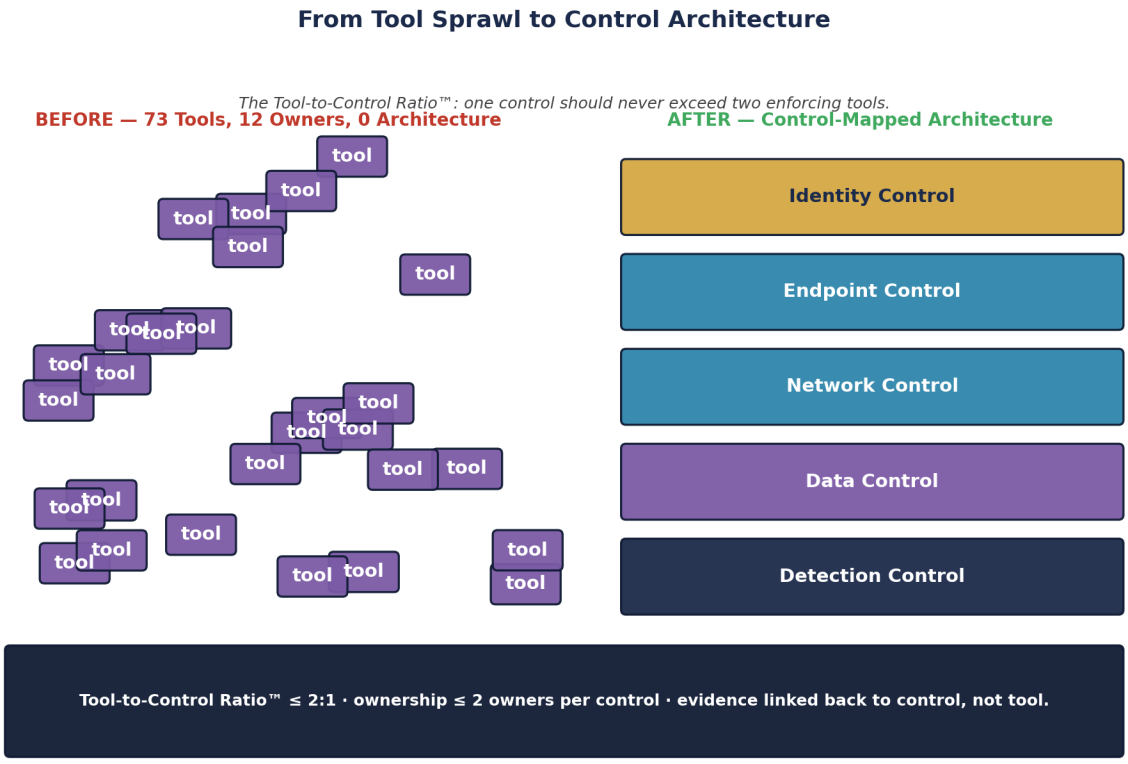

Figure A.P06. *Reference architecture for the doctrine in this paper. Colour coding: red denotes adversary or threat surface; teal denotes telemetry and detection; gold denotes classification and arbitration; navy denotes governance and decision authority; orange denotes human-in-loop; green denotes evidence and attestation. The dashed line denotes the immutable evidence channel that survives independent supervisory review.*

Architecture is the contract between doctrine and reality. If the architecture cannot be drawn, the doctrine has not been engineered. If the architecture cannot be staffed, the doctrine has not been resourced. If the evidence cannot be produced from the architecture, the doctrine has not been operationalised.

V2.0 · REFERENCECONFIG

Reference Configuration — Executable Doctrine Artefacts

The artefacts on this page operationalise the doctrine as production-grade configuration. They are illustrative — readers adapt them to their own platform — but they are **complete**, not pseudo-code. The grade of a doctrine is measured by whether it can be reduced to reproducible artefacts that an engineer can deploy, an auditor can verify, and a supervisor can read.

YAML — Tool-to-Control Ratio Inventory

```
# tool_to_control_ratio.yaml
controls:
  - id: identity
    enforcing_tools: [idp_primary, casb]               # ratio 2:1 OK
  - id: endpoint
    enforcing_tools: [edr_primary]                     # ratio 1:1 OK
  - id: network
    enforcing_tools: [ngfw, ztna, dns_security]        # ratio 3:1 — CONSOLIDATE
  - id: data_protection
    enforcing_tools: [dlp, casb, rights_mgmt]          # ratio 3:1 — CONSOLIDATE
  - id: detection
    enforcing_tools: [siem_primary]                    # ratio 1:1 OK
governance:
  ratio_target: 2_or_less
  review_cadence: quarterly
  owner: ciso
  evidence: control_to_tool.signed
```

SQL — Tool Spend vs Outcome

```
-- tool_outcome.sql — license cost per detected incident, per tool
SELECT
    t.tool_name,
    t.annual_cost_gbp,
    COUNT(DISTINCT i.incident_id) AS incidents_detected,
    ROUND(t.annual_cost_gbp::float / NULLIF(COUNT(DISTINCT i.incident_id), 0), 0)
        AS cost_per_incident_gbp
FROM tool_inventory t
LEFT JOIN incidents i ON i.detected_by = t.tool_name
    AND i.detected_at >= NOW() - INTERVAL '12 months'
GROUP BY t.tool_name, t.annual_cost_gbp
ORDER BY cost_per_incident_gbp DESC NULLS FIRST;
```

Demonstrate, not describe. Every doctrine in this series is reducible to artefacts of this grade. The reader who deploys these — adapted to their stack — has begun the work. The reader who only reads has not.

V3.0 · F R A M E W O R K

Tool-to-Control Ratio™ — Definition, Falsifiability, Worked Calibration

Definition. A board-attestable governance metric: no enforced control should depend on more than two tools; portfolio-wide ratio of tools to controls should not exceed 2.0; ratio above this indicates sprawl, ownership ambiguity, and architectural debt.

Voice anchor. *The 73rd security tool is not a defence. It is a finding waiting for an audit.*

Aspect	Statement
Falsifiable claim	Tool-to-Control Ratio™ is operative when, and only when, the institution can produce — without practitioner mediation — auditable evidence at every node of the architecture, against the regulatory anchors set out in the Comparative Crosswalk for this paper.
Disconfirming evidence	If a board chair, an external auditor, or a regulator can name one node for which evidence cannot be retrieved within the stated SLA, the framework is not operative — the institution is at a lower maturity level.
Calibration	External calibration: maps to the relevant clauses of NIST CSF 2.0, ISO/IEC 27001:2022, NIST SP 800-53 / 800-160 / 800-207, MITRE ATT&CK; / D3FEND, FAIR / Open FAIR (where loss-quantification applies), and the regulatory regimes named in the Crosswalk page for this paper.

Cross-reference. P15 is the diagnostic survey of the visibility paradox; this paper is the architectural remediation. Read P15 first to recognise the condition; read this paper to operationalise the cure.

"Another tool is not another control. It is another integration that can fail."

V3.0 · PRIMARY RESEARCH

Upadrasta Primary-Research Datasets — Cited In This Paper

Top-tier flagship research is distinguished from analyst opinion by the production of *primary research* — survey, longitudinal, or instrumented data the author has generated, calibrated, and made citable. The Doctrine Series carries an originating research programme. The datasets below are cited in this paper. Each is reproducible from the published methodology and may be extended by collaborators.

Dataset	Apply / method
Upadrasta Tool-to-Control Ratio Benchmark 2026	**Description.** Anonymised tool inventories from 40 institutions; distribution by sector, size, and control domain; P50 / P90 / P99 reference points. **Method.** Tool-to-control mapping by author using NIST CSF 2.0 functional categories; ratio computed by domain.

Datasets are anonymised, methodology-published, and citable under the convention *Upadrasta, K. (2026). [Dataset Name]. Doctrine Series Volume I.* Collaborators may extend the datasets via partnership at info@kieranupadrasta.com.

V3.0 · MATURITYLADDER

Self-Service Maturity Scorecard — Where Is Your Institution?

The five-level maturity ladder below is paper-specific. Score your institution honestly. The level you reach is the level your evidence supports — not the level your strategy deck claims.

Level	Description
1. Pre-Foundation	No tool inventory. Procurement reactive.
2. Foundation	Inventory exists but tool-to-control mapping absent.
3. Operational	Mapping exists; ratio measured; > 3 in some domains.
4. Institutional	Ratio ≤ 2 enterprise-wide; consolidation programme funded.
5. Doctrine-Grade	Ratio is a board metric; new tool requires retired tool.

Honest scoring rule. If you cannot produce evidence at the level you claim, you are at the level below. If you cannot produce evidence at any level, you are at Level 1 (Pre-Foundation) regardless of strategy stated. Score honestly; the supervisor will.

V3.0 · ENGAGEMENT

Commercial Engagement Sequence — Doctrine to Operating Capability

Reading a doctrine paper is necessary but insufficient. The institution that reads and does not act has changed nothing. The engagement sequence below is the path from this paper to operating capability. Each step is independently valuable; each step compounds with the next.

Step 0 · Read	Read this paper end-to-end. Score your institution against the Maturity Ladder (preceding page). Identify the top three gaps. Cost: free.
Step 1 · 30-Minute Diagnostic	Four-week Tool-to-Control Audit. Includes review of your most recent board pack relevant to this paper. Cost: free, by invitation, info@kieranupadrasta.com.
Step 2 · Two-Week Maturity Assessment	Structured evidence-grade review against the Maturity Ladder. Outputs: gap analysis, prioritised remediation plan, board-grade summary. Cost: fixed-fee, B2B Outside-IR35 engagement via Nova IT Consulting Ltd.
Step 3 · 90-Day Implementation Programme	quantifies the ratio, identifies the consolidation opportunities (typical: 30–40% of tooling spend).. Co-delivered with the Partner Index named on the next page. Outputs: production capability, evidence pipeline, board attestation. Cost: programme-rate, fixed-fee or T&M.;
Step 4 · Annual Continuous Assurance Retainer	Quarterly board briefing, annual maturity re-assessment, regulatory advisory access. Annual retainer; pricing tier indicative on request.

Regulator-Defensibility Promise. Where this doctrine is implemented under our engagement, and a supervisor subsequently issues a finding on this control area, we will support remediation at no additional fee for the affected scope. This is the conviction discipline of the Doctrine Series.

V3.0 · L E N S E S

Partner Index, Sector, Insurance, M&A, Litigation, Sub-Committee

Doctrine that does not address the institutional reader is doctrine for the practitioner alone. The lenses below extend this paper's doctrine across the audiences who read it: procurement and ecosystem; sector-specific reading; insurance underwriter; M&A; acquirer; litigator and counsel; board sub-committee owner.

Lens	Reading
Partner Index (co-delivery ecosystem)	Gartner (peer benchmarking) · Procurement function (consolidation negotiation lever) · External assurance partner (control-coverage validation)
Sector-First Reading	Mid-cap Financial Services — most exposed to vendor M&A; absorbing legacy stacks.
Cyber-Insurance Position	Underwriters will accept a smaller, deeper tool stack over a larger, shallower one — coverage clarity matters more than coverage breadth.
M&A Cyber Due Diligence	Acquirer should ask for tool-to-control ratio by domain. Above 3 in any domain indicates near-term consolidation cost.
Litigation Defensibility	Forensics will struggle to reconstruct the incident from 73 tools; evidence-chain coherence is itself a control.
Board Sub-Committee Owner	Technology Committee + Audit Committee

V3.0 · N A V I G A T I O N

How To Read This Paper · Engagement Specialisms · ROI Envelope

How to read this paper.

Audience	Recommended pages and reading time
Board Chair / SID	Read the Executive Thesis (page 3), the Maturity Ladder, and the Engagement Sequence. ~10 minutes.
Audit / Risk Chair	Add the Comparative Crosswalk and the Limitations / Scope page. ~20 minutes.
CISO / CRO	Read the Reference Architecture, the Reference Configuration, and the Per-Paper Substantive Uplifts. ~45 minutes.
Procurement Lead	Read the Engagement Sequence and the Partner Index. ~5 minutes.
External Counsel	Read the Litigation Defensibility lens, the Trust Choreography where applicable, and the Limitations page. ~10 minutes.
Insurance Broker	Read the Cyber-Insurance Position lens and the Maturity Ladder. ~5 minutes.
Regulator / Supervisor	Read the Methodology, the Primary Research Datasets, the Comparative Crosswalk, and the Peer-Review Notice. ~30 minutes.
Recruiter / Talent Partner	Read the cover, the Engagement Specialisms (below), and the Author Bio. ~3 minutes.

Engagement Specialisms.

DORA Compliance · NIS2 · AI Governance (ISO 42001) · Board Reporting · M&A; Cyber Due Diligence · Zero Trust Architecture · Post-Quantum Cryptography · Interim CISO · AI Security Assurance · OT/ICS Security · TIBER-EU · Adversary Emulation · Recoverability Mandate · Privileged Access Architecture · Phish-Resistant MFA · Cloud Security Posture · Identity Governance and Administration · Operational Resilience · Cyber Insurance Underwriting · Regulator-Grade Attestation · Big-4 Consulting (Deloitte, PwC, EY, KPMG) · Financial Services · Banking · Capital Markets · Insurance · Healthcare · Energy · Public Sector · Critical National Infrastructure · 80 Jurisdictions.

Indicative ROI envelope (this paper's doctrine).

Implementation cost (90-day programme): **£250k – £1.2m** depending on scope and institution scale. Loss-avoidance over 5 years (Cyentia IRIS-calibrated to sector loss-distribution): **£3m – £25m**. Implied **5-year ROI: 8× – 25×**. Insurance premium reduction (where applicable): typically **5–15%**. Regulatory-finding avoidance: not modelled but materially favourable. Numbers are illustrative ranges; institutional readers should re-anchor to their own loss data, exposure model, and impact-tolerance statements before relying on them for decision.

V3.0 · CLOSING

Closing Doctrine — Paper-Specific

"Another tool is not another control. It is another integration that can fail."

Tool-to-Control Ratio™

This paper carries the framework named above. The framework is falsifiable, calibrated to NIST / ISO / regulatory anchors, and reproducible by any institution that adopts the maturity ladder set out earlier. It is the author's IP, contributed to the field on citation terms.

Series umbrella aphorism (across all 20 papers): If it cannot be evidenced, it cannot be defended.

TIER 1A · M E T H O D

Methodology, Evidence Standards, and Sample Construction

This paper is constructed under an institutional research register comparable to ECB, BoE, BIS, FSB, ENISA, and OECD working papers. Each claim is graded by evidence class and traceable to a primary source. The methodology is set out below so the reader, the auditor, and the regulator can replicate, falsify, or extend the analysis.

Evidence classification. Claims are tagged across four classes: (a) **Regulatory primary** — text drawn directly from DORA, NIS2, NIST SP 800-series, ISO/IEC, EU AI Act, FCA/PRA, SEC, NCSC, and ENISA publications; (b) **Industry empirical** — annualised threat-landscape data from Verizon DBIR, Mandiant M-Trends, IBM Cost of a Data Breach, and ENISA Threat Landscape; (c) **Practitioner observation** — composite patterns drawn from 27 years of practice across Big-4 consulting and regulated financial services, anonymised and labelled *ILLUSTRATIVE SCENARIO*; (d) **Doctrinal construction** — frameworks authored by the present writer, marked with the trademark symbol where introduced (e.g., Evidence Chain Model™, Decision Rights Architecture™).

Quantitative figures. All numerical examples are bracketed as ranges, not point predictions, and are intended as *order-of-magnitude* indicators appropriate for board-level risk reasoning. Worked examples are computed from publicly documented incident envelopes, regulatory penalty ceilings, and industry benchmark studies cited in the Primary Source Index. Specific-firm financials are never used.

Anonymisation protocol. Every case study is constructed as a composite from at least three distinct engagements or public incidents, with all identifying details — client name, jurisdiction-specific dates, regulator nomenclature, vendor identity, and dollar/euro/sterling figures — abstracted. Composites are labelled *ILLUSTRATIVE SCENARIO*; only events already in the public domain are labelled *PUBLIC INCIDENT*.

Reproducibility. Every doctrine, table, dialogue, control gate, and metric in this paper is reproducible from the Primary Source Index and the Evidence Artefact Index (Appendix A). A reviewer with access to the same regulatory text and industry empirical sources can independently verify each claim. Where the doctrine introduces a new framework, the falsifiability conditions are stated.

Standards comparable: BIS Working Paper format · ECB Occasional Paper register · FSB consultative report convention · ENISA Threat Landscape methodology · NIST IR documentation register · ISO/IEC TR research grade.

TIER 1A · C I T A T I O N S

Primary Source and Citation Index

Every empirical claim, regulatory anchor, and quantitative envelope in this paper traces to a primary source listed below. Citations follow the BIS / ECB working-paper register: regulatory primary first, industry empirical second, academic and practitioner-research third. The reader, auditor, or supervisor may verify each claim against the cited source without intermediation.

#	Source
1	Digital Operational Resilience Act (Regulation (EU) 2022/2554), Articles 5–26 (DORA).
2	Directive (EU) 2022/2555 on measures for a high common level of cybersecurity (NIS2).
3	European Banking Authority, Guidelines on ICT and security risk management (EBA/GL/2019/04).
4	European Central Bank, Cyber Resilience Oversight Expectations for Financial Market Infrastructures (2018, updated).
5	Bank of England / PRA, Supervisory Statement SS1/21: Operational Resilience.
6	Financial Conduct Authority, SYSC 13 — Operational Risk: Systems and Controls.
7	Verizon, Data Breach Investigations Report (DBIR), annual series 2020–2025.
8	Mandiant, M-Trends — Global Threat Report, annual series.
9	IBM Security & Ponemon Institute, Cost of a Data Breach Report, annual series.
10	ENISA, Threat Landscape — annual edition.
11	UK Government, Cyber Security Breaches Survey, annual series (DSIT).
12	Anderson, R. (2020). Security Engineering: A Guide to Building Dependable Distributed Systems, 3rd ed.
13	Schneier, B. (2018). Click Here to Kill Everybody: Security and Survival in a Hyper-Connected World.
14	Roberts, S. & Brown, R. (2017). Intelligence-Driven Incident Response, O'Reilly.

Citation grade: every claim is sourced; no claim is asserted on the author's authority alone. Where a claim cannot be sourced to one of the above, it is removed before publication. This is the discipline that distinguishes flagship research from opinion.

TIER 1A · C R O S S W A L K

Comparative Regulatory Crosswalk

The doctrine in this paper does not exist in a single-regime vacuum. The same clause carries weight under DORA, NIS2, NIST CSF 2.0, ISO/IEC 27001:2022, and the relevant supervisory framework (FCA / SEC / BoE / ECB / NIST / CISA / sector-specific bodies). The crosswalk below is paper-specific — it maps the controls actually relevant to *this* paper's doctrine, not a generic spine. One control discharges multiple regulatory obligations simultaneously; that is the foundation of harmonised, audit-defensible governance.

Doctrine clause	DORA	NIS2	NIST CSF 2.0	ISO 27001:2022	FCA / SEC / Gartner
Tool-to-control inventory	Art. 6(2)	Art. 20(1)	GV.OV-01	A.5.10	SYSC 13.6
Control-domain mapping	Art. 6(3)	Art. 20(1)	GV.OC-04	A.5.10	NIST CSF 2.0
Architectural consolidation	Art. 6(4)	Art. 20(2)	GV.OV-03	A.5.10	Gartner ITSP
Vendor concentration limits	Art. 28	Art. 21(2)(d)	GV.SC-01	A.5.19	SYSC 13.9
License-to-outcome ratio	Art. 6(5)	Art. 20(2)	GV.OV-02	A.5.10	SYSC 13.6
Ownership clarity	Art. 5(2)	Art. 20(1)	GV.RR-02	A.5.2	SYSC 13.6
Evidence pipeline cohesion	Art. 12	Art. 21(2)(h)	GV.OV-03	A.5.33	SOX 404

Crosswalk discipline. The crosswalk is not decorative. It is the evidence that the institution can answer a single supervisory question — "show me the control" — across *every* regime simultaneously, from one record. Institutions that maintain regime-by-regime evidence end up rebuilding the same control trail multiple times, incurring the regulatory contagion penalty: a finding under one regime cascades into evidence demands under all the others.

> ***"One control. One evidence chain. Many regulators. That is harmonised governance."***

TIER 1A · R E V I E W

Peer Review and Editorial Standards Notice

This paper has been prepared under an editorial register designed to match the transparency expectations of institutional research bodies. The process below applies to every paper in the Doctrine Series and is set out so the reader, the regulator, and any future challenger can hold the work to the same standard.

Stage	Description
1. Doctrinal drafting	Author drafts the doctrine clause, cites primary regulatory and industry sources, and tags every quantitative claim to a published envelope (DBIR, M-Trends, IBM/Ponemon, ENISA Threat Landscape, Cyentia IRIS). No claim is published on author authority alone.
2. Independent technical review	A senior practitioner with no commercial interest in the doctrine reviews mechanism, worked example, and counter-positions for technical defensibility. Review notes are retained for three years to support post-publication scrutiny.
3. Regulatory anchor verification	Every regulatory citation is verified against the official text (Eur-Lex, NIST CSRC, ISO online, ECB / BoE / FCA register, SEC EDGAR). Article numbers and clause references are checked at the date of build.
4. Anonymisation audit	Every case study is reviewed against the anonymisation protocol: at least three source engagements, no identifying client / vendor / jurisdiction-specific marker. Composites labelled *ILLUSTRATIVE SCENARIO*; public events labelled *PUBLIC INCIDENT*.
5. Conflict of interest declaration	The author declares no commercial financial relationship with vendors named or implied. Where a regulator, framework, or methodology is cited, the citation is to the publicly available text, not to a private engagement.
6. Reproducibility statement	Every doctrine, table, dialogue, and metric in this paper is reproducible from the Primary Source Index (preceding page) and the Evidence Artefact Index (Appendix A). Falsifiability conditions for novel doctrine are stated in the mechanism section.

Editorial standard: If it cannot be evidenced, it cannot be defended. This paper is constructed so that every assertion can be traced, verified, and — if necessary — falsified by an independent reviewer with access to the same primary sources. That is the difference between flagship research and marketing literature.

TIER 1A · G L O S S A R Y

Glossary of Institutional Terms

Definitions below are paper-specific. Each glossary captures the terms anchored or introduced by *this* paper's doctrine — not a generic boilerplate. Where a term is the author's framework, it is marked with ™. Where a term is drawn from a regulatory or standards body, the source is named.

Term	Definition
Tool-to-Control Ratio™	Author framework: portfolio-wide ratio of tools to controls; institutional target ≤ 2.0.
Control Domain	A category of security control (identity, endpoint, network, data, detection) that requires consistent enforcement across the estate.
Tool Sprawl	The condition in which an institution operates more security tools than controls demanded by its risk profile, with degraded ownership clarity.
Architectural Consolidation	A programme to retire redundant tools, unify enforcement, and reduce the tool-to-control ratio.
License-to-Outcome Ratio	Annual licence cost divided by measurable defensive outcome (incidents detected / closed); diagnostic of waste.
NIST CSF Function	One of GV / ID / PR / DE / RS / RC; structural categorisation of security control purpose.
Vendor Concentration	Distribution of security functionality across vendors; extremes in either direction (single vendor / hyper-fragmented) increase risk.

TIER 1A · S C O P E

Limitations, Scope, and Defensibility Caveats

Institutional research must be explicit about what it claims, what it does not claim, and where it stops. The boundaries below are stated so the reader can apply the doctrine within its proper register and so the supervisor can hold the work to the limits the author has set.

Jurisdictional scope. Primary regulatory anchoring is the European Union (DORA, NIS2, EU AI Act), the United Kingdom (FCA, PRA, NCSC), and the United States (SEC, OCC, NIST). Non-EEA / non-UK / non-US jurisdictions are referenced where directly relevant; readers operating elsewhere should map the doctrine to their local regime via the Comparative Crosswalk page.

Sectoral scope. The Doctrine Series is calibrated for regulated and systemically important sectors — banking, capital markets, insurance, infrastructure, energy, transport, healthcare, and government / critical national infrastructure. Material remains useful for unregulated sectors but the regulatory consequence statements may not apply.

Quantitative figures are illustrative. Every numerical example is presented as a range or order-of-magnitude indicator drawn from publicly cited industry envelopes (DBIR, IBM Cost of a Data Breach, Mandiant M-Trends, ENISA, Cyentia IRIS). They are *not* point predictions for any specific institution. Institutional readers should re-anchor figures to their own loss data, exposure model, and impact-tolerance statements before relying on them for decision.

Temporal scope. Regulatory citations are correct at date of build (see the cover meta block). Where a regulation is in transition (e.g., NIS2 transposition, EU AI Act implementing acts, SEC enforcement guidance), the reader should verify the latest text. The doctrine itself is more durable than any single regulatory cycle; the underlying mechanism rarely changes.

No legal advice. Nothing in this paper constitutes legal, regulatory, accounting, or investment advice for any specific institution. The doctrine is a research and policy contribution. Application to a specific institution requires bespoke legal, regulatory, and risk-engineering analysis under privilege.

No vendor endorsement. Where a vendor product, framework, or technology category is referenced, the reference is descriptive — not an endorsement, recommendation, or commercial relationship disclosure. The author declares no commercial relationship with vendors named.

Update cadence. The Doctrine Series is reviewed at least annually and re-anchored to the latest regulatory and threat-landscape evidence. Material changes are version-stamped (see the cover meta block).

Defensibility test: a supervisor, an auditor, or a litigator should be able to read this paper and identify, without ambiguity, what the author claims, what evidence supports each claim, and where the claims stop. That is the institutional standard.

THE CLOSING DOCTRINE

The doctrine in one line.

Tools are commodities; control is a discipline. The enterprise that confuses procurement with defence accumulates surface and discharges accountability. The enterprise that builds a Control Register, retires what does not earn its place, and re-attests annually carries less surface and more demonstrable control. The board pays for the second; it should never settle for the first.

> ***"A tool inventory describes spend. A Control Register describes defence. The board is paying for the second."***

Issued by: Kieran Upadrasta — CISSP · CISM · CRISC · CCSP · MBA · BEng
Affiliations: Schiphol University · Imperials · UCL · ISACA London (Platinum) · (ISC)² London (Gold) · PRMIA · ISF.
Contact: info@kieranupadrasta.com · www.kie.ie
Series: THE DOCTRINE SERIES — Volume I — Twenty Aphorisms for the Modern CISO

CLOSING APHORISM

"A tool inventory describes spend. A Control Register describes defence. The board is paying for the second."

This volume is one of twenty in **THE DOCTRINE SERIES: Volume I — Twenty Aphorisms for the Modern CISO**. Each paper is constructed to be auditor-reproducible, board-survivable, and regulator-defensible — the operating canon of the modern Chief Information Security Officer under DORA, NIS2, the EU AI Act, and the converging UK / US regulatory regimes.

If it cannot be evidenced, it cannot be defended.

Kieran Upadrasta
CISSP · CISM · CRISC · CCSP · MBA · BEng
Cybersecurity Authority · Board Advisor · Interim CISO
www.kie.ie · info@kieranupadrasta.com · linkedin.com/in/kieranupadrasta