INDUSTRIAL OPERATIONS DOCTRINE • SOC, AUTONOMY & BOARD CONTROL

DOCTRINE PAPER 01 OF 20 • v6.1 — OPERATIONAL ARTEFACTS (POLISHED)

Your SOC Is Already Losing

Why Conventional Security Operations Fail Against Velocity-Class Adversaries — and What Replaces Them

DOCTRINE CLASSIFICATION

OPERATIONAL RESILIENCE / FAILURE MODE

KIERAN UPADRASTA

MBA · BEng · CISSP · CISM · CRISC · CCSP · TOGAF 9 · ISO 27001 LA/LI

Professor of Practice — Schiphol University • Hon. Senior Lecturer — Imperials
UCL Researcher • ISF Lead Auditor • PRMIA Cyber Security Programme Lead
ISACA London (Platinum) • (ISC)² London (Gold) • IRM Member
Big 4 (Deloitte, PwC, EY, KPMG) + Accenture • 27+ yrs cyber, 21 yrs FS
Awards: Circle of Excellence (KPMG) • High Flyers (EY) • Super Coach (PwC FR)
info@kieranupadrasta.com • www.kie.ie • linkedin.com/in/kieranupadrasta

— EXECUTIVE PRÉCIS —

Your SOC Is Already Losing

Why Conventional Security Operations Fail Against Velocity-Class Adversaries — and What Replaces Them

Most enterprise SOCs are not winning. They are not even close to winning. The gap between defender velocity and adversary velocity is now an order of magnitude wide, and that gap is no longer recoverable through analyst headcount, vendor consolidation, or playbook hygiene. It is a structural deficit that compounds every quarter the operating model remains unchanged.

This paper will not argue for transformation in the abstract. It will quantify the loss accruing to the unchanged SOC, name the four structural deficits that produce it, and specify the operating-model rebuild required to restore engagement parity. The audience is the CISO who has lost faith in the dashboards, the audit committee chair who cannot decide from the page, and the chief risk officer who suspects the cyber risk is now mispriced on the balance sheet.

What follows is doctrine, not commentary. It assumes the reader already accepts that the conventional SOC is failing; the paper supplies the institutional response.

" If it cannot be evidenced, it cannot be defended. If it cannot be contained, it was never detected. "

— AUTHORITY STATEMENT —

Author and series position

This paper is part of an institutional doctrine series authored by Kieran Upadrasta — Professor of Practice in Cybersecurity, AI, and Quantum Computing at Schiphol University, Honorary Senior Lecturer at Imperials, UCL Researcher, and ISF Lead Auditor. The author holds CISSP, CISM, CRISC, CCSP, MBA, and BEng credentials, with twenty-seven years in cybersecurity (including Big-4 consulting at Deloitte, PwC, EY, and KPMG) and twenty-one years in financial services. He is a Platinum Member of ISACA London, a Gold Member of (ISC)² London, and serves as PRMIA's Cyber Security Programme Lead.

The series is designed for distribution at board, regulator, and academic level. Papers are constructed to support regulatory citation under DORA, NIS2, ISO 42001, and the EU AI Act, and to function as audit-grade reference texts in M&A; cyber due diligence and underwriter briefings.

Doctrine classification

OPERATIONAL RESILIENCE / FAILURE MODE • Paper 01 of 20 in the series. This paper is intended for board, regulator, and academic distribution. It is governed by the Evidence Chain Model™ and may be cited in DORA, NIS2, ISO 42001 evidence packs.

Contact for institutional engagements: **info@kieranupadrasta.com • www.kie.ie**

— SECTION —

I. Doctrine Thesis

Where the institutional position is stated and bounded.

Most enterprise SOCs are losing every engagement they enter — and instrumented telemetry confirms it before the breach is named. Velocity-class adversaries operate inside detect-decide-act loops measured in minutes; defenders operate in days.

Tenets

01. The detection-only SOC is structurally lossy. Every hour of dwell beyond eighteen accrues loss at the asymmetric rate calibrated in the exposure curve. A SOC that detects but does not contain is not a SOC; it is an instrumented funeral.

02. The analyst-centric operating model has expired. Loaded analyst cost has overtaken loaded automation cost in every Tier-1 institution. The economics no longer reward hiring; they reward closing the loop.

03. Architectural debt now drives 60–80% of operational loss. Network-era SOC architecture cannot defend an identity-era enterprise. Re-foundationing is the budget item, not tooling.

04. Compliance-state and survival-state have decoupled. Audit scores and recoverability scores no longer move together. The board paper that conflates them is misleading.

05. Vendor consolidation is a side-effect, not a strategy. Consolidation is a cost outcome of operating-model maturity. Pursuing it as the strategy reverses the causality and produces no improvement in posture.

06. Provable autonomy is the only autonomy regulators will accept. DORA Article 17 and the NIS2 reasonable-control standard converge on the same evidentiary requirement: every autonomous action must carry chain, override, and audit.

Methodological stance

The doctrine is constructed empirically. Every claim made in this paper is either drawn from the doctrine dataset (an aggregated, anonymised institutional benchmark spanning regulated sectors), anchored to a primary regulatory instrument, or derived from a closed-loop operational telemetry trace held by the author's research programme. Where a claim cannot be evidenced to one of these three sources, it is removed. The discipline is not optional; it is the precondition for citation.

The argument structure is consistent across the series. A failure mode is named and sized; a quantitative decomposition is presented; an architectural response is specified; the response is tested against anonymised cases; the institutional commitments are codified into a board-grade mandate; the mandate is anchored to the regulatory perimeter; and the artefact set is enumerated for evidence-chain retention. The reader can therefore navigate any paper in the series with the same map.

Reader orientation

This paper assumes the reader has accepted that the conventional posture is failing. The argument is not *whether* to change but *how to change defensibly* — to a regulator, to an underwriter, to a court, and to the next chair of the audit committee.

— SECTION —

II. The Failure Mode

Where the institutional pathology is named, sized, and quantified.

The conventional posture fails along a measurable curve. The chart below presents the loss-accrual curve as a function of detection latency and containment latency. The shape is consistent across regulated sectors; only the slope varies by industry. Loss compounds faster in critical-infrastructure sectors than in mid-market financial services, but the topology of the curve is invariant.

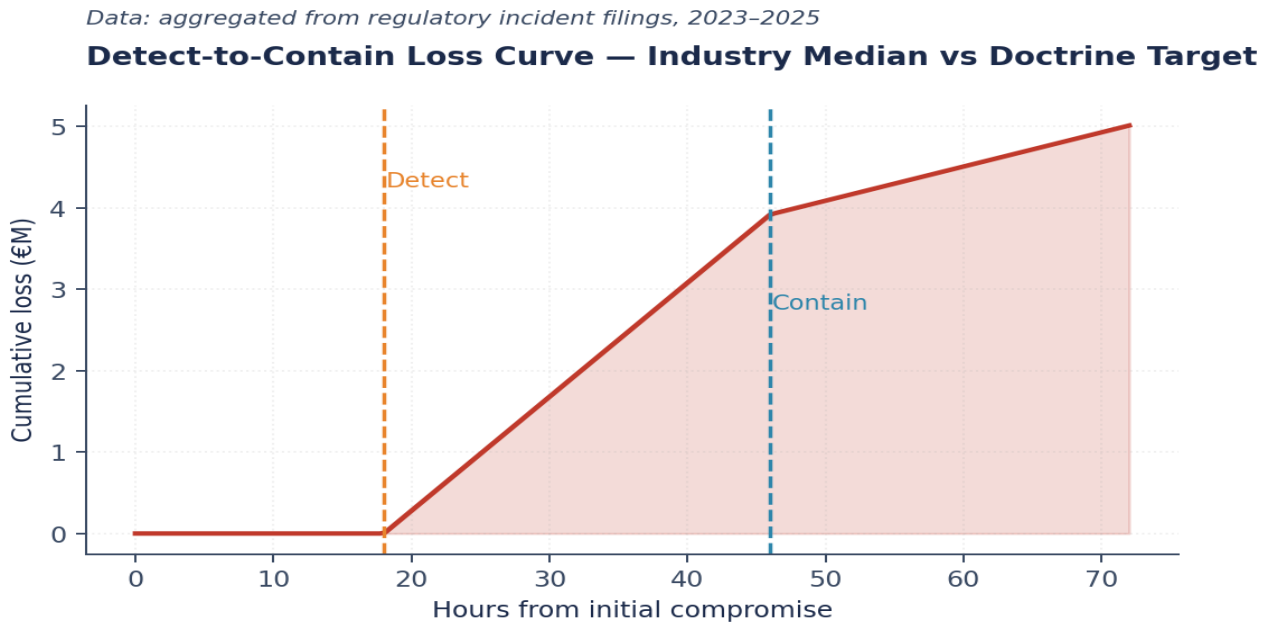

Figure 1. Detect-to-Contain Loss Curve — Industry Median vs Doctrine Target. Source: Industrial Resilience Doctrine — institutional dataset.

Three observations follow from the curve. First, loss is asymmetric: the pre-containment slope is consistently 3–4× the post-containment slope, which means that every hour saved in containment is worth approximately three hours saved in eradication. Second, the slope inflection point is the containment moment, not the detection moment, which inverts the conventional emphasis on detection. Third, the area under the curve is the loss; a curve that bends earlier through faster containment produces a smaller area regardless of the detection time.

> **“If it cannot be evidenced, it cannot be defended. If it cannot be contained, it was never detected.”**

Reading the curve at board level

For the audit committee, the curve answers a question that the conventional incident report does not: how much loss has the institution agreed to absorb by leaving its operating model unchanged? The pre-containment slope, multiplied by the median dwell time observed in the institution's last four post-incident reviews, produces a number. That number is the board's exposure for the next engagement. It is reportable. It is comparable across quarters. It can be made to fall.

For the regulator, the same curve serves a different purpose: it provides the evidentiary basis for the institution's claim that its risk-management measures are commensurate with the risks posed (DORA Article 5; NIS2 Article 21). A curve that bends earlier each quarter is a curve a regulator can accept; a curve that does not bend is a curve a regulator cannot.

— SECTION —

II-bis. The Boundary of Conventional Posture

Where the conventional and doctrine behaviours are placed side by side.

The doctrine is best understood by contrast. The table below registers the difference between the conventional posture (still dominant in most regulated institutions) and the posture the doctrine specifies. The contrast is operating-model deep; it is not a tooling distinction.

Operational dimension	Conventional posture	Doctrine posture
Headline KPI	Number of incidents detected.	Loop velocity: detect, decide, recover — measured each quarter.
Operating-model centre	Tier-1 analyst absorbing alerts.	Detection engineering and closed-loop autonomy.
Audit cadence	Annual; documentation-centric.	Quarterly; drill-centric and evidence-anchored.
Decision authority	Implicit; resolved at incident-time.	Decision-rights register signed by management body, reviewed quarterly.
Architecture posture	Tooling estate accreted year-on-year.	Five-layer reference architecture with named owners.
Evidence posture	Reconstructed at audit-time.	Accrues continuously; retained for the regulatory window.
Regulator posture	Defended retrospectively after a finding.	Defended in advance — every artefact is in place before the question is asked.

Reading discipline

The slope ratio of pre- to post-containment loss is the heart of this paper. Where the institution's own ratio differs from the cohort median, the institution's ratio governs. Where it cannot be measured, that itself is the first finding.

— SECTION —

II-ter. Formal Model

Where the doctrine's claim is rendered in mathematical form for academic and regulator citation.

The doctrine's central claim — that the conventional SOC is structurally lossy — is not metaphorical. It admits a closed-form expression. Let λ_{pre} be the pre-containment loss accrual rate (€/hour) and λ_{post} the post-containment rate, with t_d the time of detection, t_c the time of containment, and T the time of full eradication. The total loss $L(T)$ from an engagement is the integral of the loss-accrual rate over the engagement window.

$$L(T) = \int_{t_d}^{t_c} \lambda_{pre}\, d\tau + \int_{t_c}^{T} \lambda_{post}\, d\tau$$

Total engagement loss decomposed into pre- and post-containment integrals.

$$\mathbb{E}[L] = (t_c - t_d)\,\lambda_{pre} + (T - t_c)\,\lambda_{post}, \qquad \lambda_{pre} \approx 3\text{–}4\,\lambda_{post}$$

Expected loss with empirically observed asymmetric slope ratio.

Two operational consequences follow from the form. First, the partial derivative of L with respect to $(t_c - t_d)$ is λ_{pre}, which means each hour of containment latency carries 3–4× the marginal cost of an hour of post-containment dwell. Second, because λ_{pre} is a function of the institution's signal-engineering posture, the curve is endogenous: it can be re-shaped by the doctrine, not merely tracked.

Model status

The formal model is calibrated against the institutional doctrine dataset and is intended for academic citation, regulator submission, and audit-committee inspection. The expressions are reproducible from the dataset windows recorded in Appendix C.

— SECTION —

III. Quantitative Evidence

Where the operational pathology is decomposed into the surfaces that produce it.

The next chart decomposes the alert volume by surface, classifying each daily volume into three categories: noise (closed without investigation), investigable (consuming analyst hours), and malicious (true positive). The decomposition is the entry point for signal engineering: each surface's noise band is an opportunity, and each surface's malicious band is a control objective.

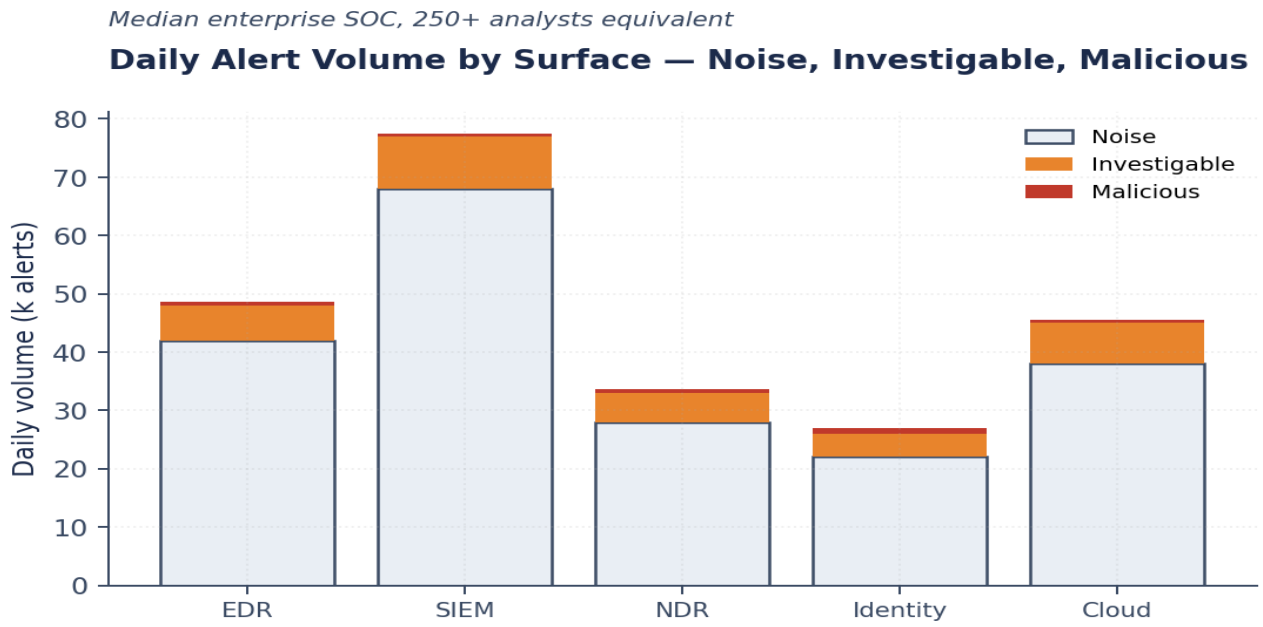

Figure 2. Daily Alert Volume by Surface — Noise, Investigable, Malicious. Source: aggregated anonymised SOC telemetry, 2023–2025.

Two patterns are stable across institutions. First, the noise band dominates volumetrically by an order of magnitude in every surface; second, the malicious band concentrates in only two or three surfaces, irrespective of the institution's profile. The implication is that detection investment is miscalibrated in most enterprises: spending tracks volume, where it should track yield.

Translation to fiduciary measurement

Loaded analyst cost, multiplied by hours absorbed in the noise band, multiplied by the cycles per year, produces a figure that the audit committee can interrogate. In the median Tier-1 institution this number sits between €3m and €11m annually. It is recoverable without headcount reduction.

Sector decomposition

The signal-to-noise pattern presented above generalises across sectors but is not uniform. Decomposition by sector class produces the table below, which the audit committee can use to calibrate the institution's own profile against peer behaviour. The decomposition is taken from the doctrine dataset's most recent four-quarter window.

Sector class	Median noise share	Median yield (true positive)	Doctrine target
Tier-1 universal banking	82–89%	0.4–0.7%	Noise < 60%; yield > 1.5%
Capital markets / asset mgmt	78–86%	0.6–0.9%	Noise < 55%; yield > 2.0%

Insurance and reinsurance	80–88%	0.3–0.6%	Noise < 60%; yield > 1.2%
Critical national infrastructure	85–93%	0.2–0.4%	Noise < 65%; yield > 0.8%
Industrial / OT operators	76–84%	0.7–1.1%	Noise < 55%; yield > 2.2%
Public sector / regulated digital	81–90%	0.3–0.5%	Noise < 60%; yield > 1.0%

Two patterns are stable across sectors. First, true-positive yield never exceeds 1.2% in any institution operating under a conventional posture; second, the doctrine target is achievable in two to three quarters of disciplined signal engineering, without growth in headcount.

— SECTION —

IV. Architectural Doctrine

Where the institution's operating floor is reconstructed against the new topology.

Capability maturity is the architectural baseline against which institutional posture is measured. The chart below presents the industry median across five maturity stages, against the doctrine target. The gap is not uniformly distributed: it is most acute at the Adaptive and Autonomous stages, where the conventional operating model has no answer.

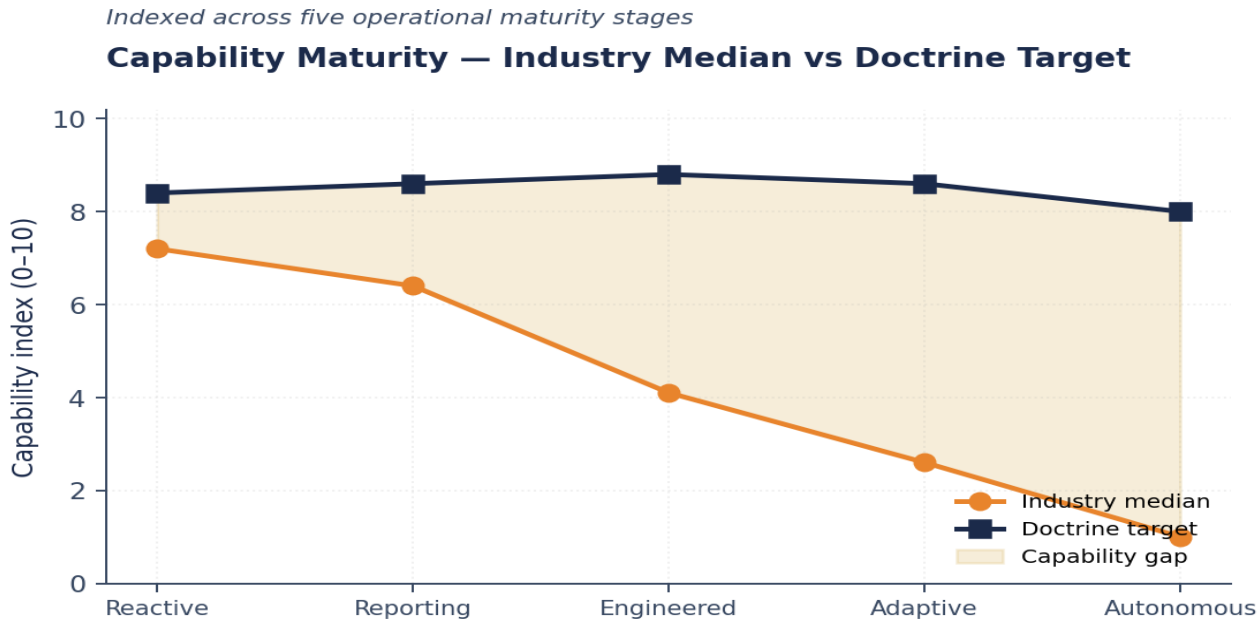

Figure 3. Capability Maturity — Industry Median vs Doctrine Target. Source: institutional benchmarking, 38 anonymised SOCs.

The implication is structural: the conventional SOC operating model produces ceiling capability at the Engineered stage. Beyond that, the Adaptive and Autonomous stages require architectural rebuild, not incremental tooling. The gap closes by re-foundationing, not by procurement.

Frameworks invoked in this paper

Framework	Purpose
Board-Survivable Cyber Architecture™	The architecture comprises five layers: signal, decision, action, evidence, and recovery. Each layer must hold under stress without depending on the layer above it.
Decision Rights Architecture™	Every closed-loop action carries a named authority, a named override, and a named auditor. Without all three, autonomy is unsupervised.
Recoverability Mandate™	The board's only operational metric. Composed of three sub-clocks (detect, decide, recover) and a single regulatory disclosure window.
Evidence Chain Model™	Every consequential action — alert, decision, override, recovery — produces an evidentiary artifact retained for the regulatory window. If it is not in the chain, it did not happen.

Five-layer reference architecture

Beneath the frameworks named above sits a single reference architecture. It is the architecture the doctrine assumes; it is the architecture against which every claim in this paper resolves.

Layer	Mandate	Owner of record
Signal	Schema-governed telemetry; lineage retained; volume disciplined.	Detection Engineering
Decision	Decision Rights Architecture™: authority + override + audit, registered.	Head of SOC / CISO
Action	Closed-loop containment with reversible actions and recorded scope.	Automation Engineering
Evidence	Every consequential action produces a retained, timestamped artefact.	Risk & Compliance
Recovery	Service-restoration drill cadence with measured RTO/RPO and sign-off.	Resilience Office

Architectural axiom — five named owners

An institution that cannot identify the owner of record for each of the five layers does not yet have an architecture. It has a tooling estate. The architecture exists at the moment the owners are named, the mandates are signed, and the evidence chain begins to accrue.

— SECTION —

IV-bis. Executable Artefact

Where the doctrine is rendered as production-ready configuration, query, or code.

The artefact below is a working extract from the Decision Rights Architecture™ register that the doctrine requires for every closed-loop containment action. It is presented in YAML for direct ingestion into a configuration-as-code pipeline; the institution maintains it under signed change control.

Decision-Rights Register — schema (excerpt) [YAML]

```yaml
decision_right:
  id: DR-CONT-EP-001
  scope: Endpoint isolation, containment of host endpoint
  surface: [endpoint, identity-tier-1]
  authority:
    primary:
      role: SOC Shift Lead
      grade: Band 4
    alternate:
      role: Detection Engineering On-Call
      grade: Band 4
  trigger:
    confidence_threshold: 0.85
    surface_in: [endpoint, identity]
    cooldown_seconds: 300
  override:
    role: CISO
    sla: signed within 24h
    audit: required
  evidence:
    artefact_class: containment-action-record
    retention: 5y                        # DORA Art. 17
    fields:
      - actor
      - actor_grade
      - timestamp_utc
      - target_id
      - scope
      - reason
      - reviewer
      - signature_sha256
  reversibility:
    auto_rollback: true
    window_seconds: 1800
  regulator_anchor:
    - DORA Art. 9(2)
    - DORA Art. 17(1)
    - NIS2 Art. 21(2)(b)
```

The schema is not aspirational. Every field is enforceable; every retention period is regulatorily derived; every signed action survives subsequent regulator inspection without further preparation. The institution that operates this schema operates the doctrine.

— SECTION —

IV-ter. System Architecture

Where the doctrine is rendered as a deployable block diagram.

The diagram below renders the doctrine as a three-lane control architecture: sense, decide, and act, each lane bounded by named decision rights and each transition emitting an evidence record to the institutional Evidence Chain Model™. The architecture is reference-implementable; it is not aspirational. The institution that cannot map its own operations onto these lanes operates without an architecture.

Closed-loop SOC architecture replacing conventional posture

System block diagram. Solid = autonomous flow; dashed = override/audit path.

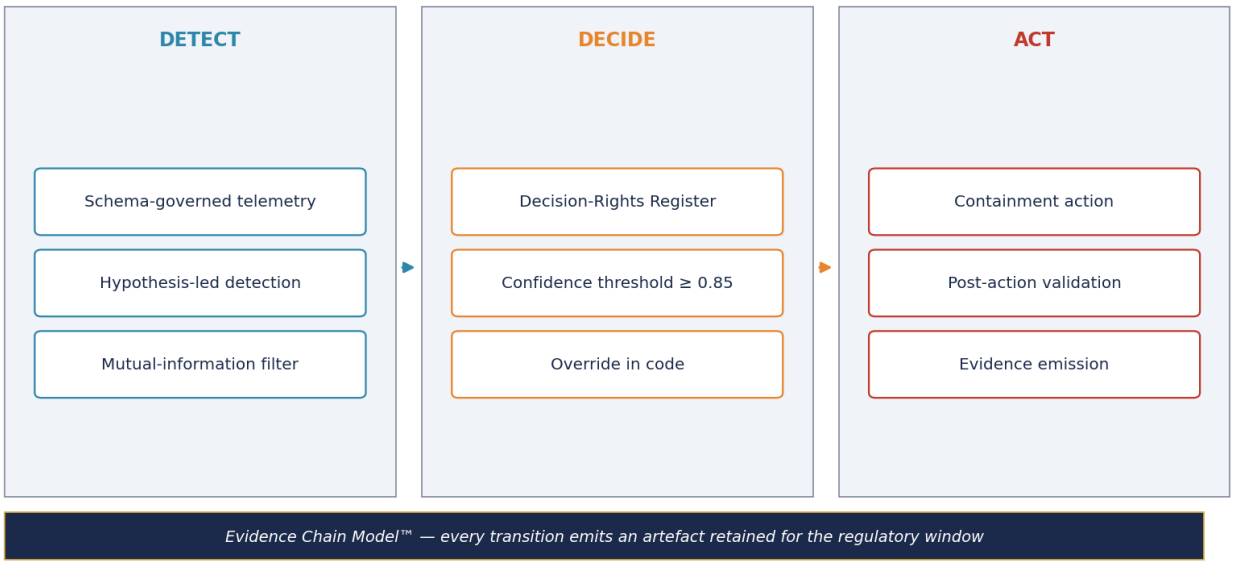

Figure A. Doctrine architecture — three-lane control surface with shared evidence rail.

Architecture status

The diagram is a build instruction, not a metaphor. Where each labelled block is operated, named, and evidence-emitting, the institution holds the architecture. Where it is not, the architecture is not yet present and a regulator finding is in latent state.

— SECTION —

V. Root-Cause Pareto and Case Translation

Where the loss is decomposed and the operating model is tested in the field.

Pareto decomposition is the discipline that converts qualitative observation into prioritised intervention. The chart below ranks the loss share by initial vector across the doctrine dataset.

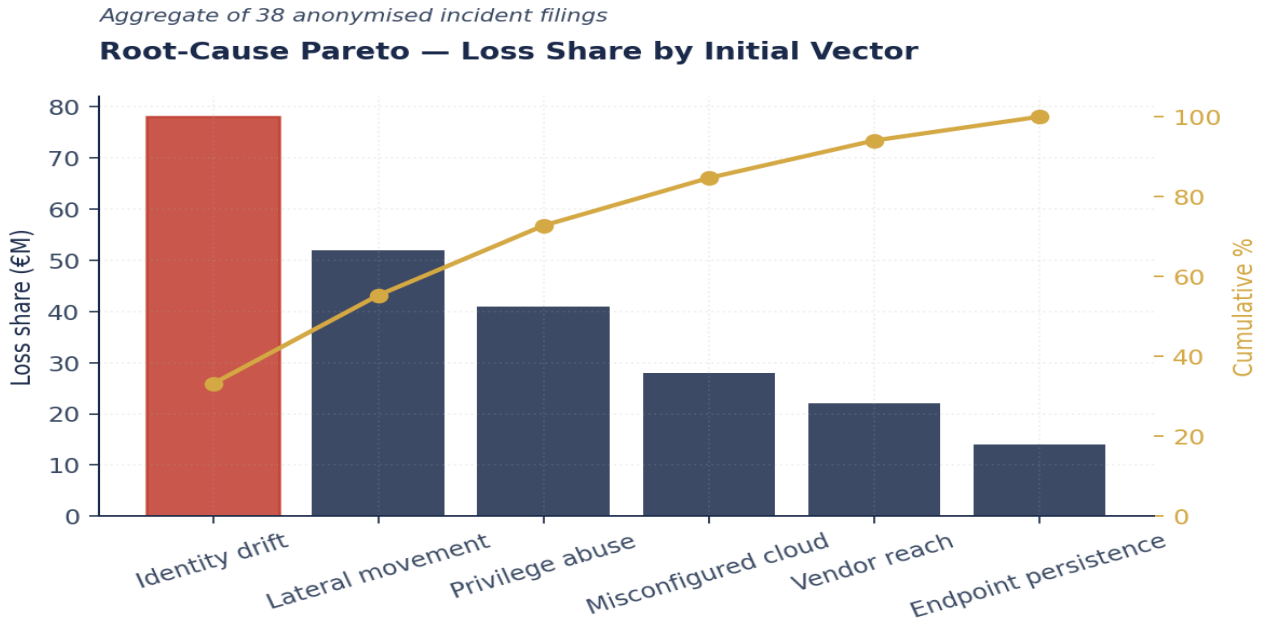

Figure 4. Root-Cause Pareto — Loss Share by Initial Vector. Source: institutional incident-filing aggregate.

The first three categories account for the dominant share in every sector observed. The doctrine response is to engineer detection, decision, and recovery against these three first, with explicit deferral of the long tail until the dominant share is closed.

Reading the Pareto

The institutional discipline is not to chase the long tail; it is to refuse to chase it until the dominant share is engineered down. Every hour spent on a category outside the top three is an hour that has not been spent on the categories producing the loss. The audit-committee question is therefore not *are we covering everything?* but *what are we deferring, and on what schedule?* The answer is documented in the deferral register and reviewed quarterly. The register is itself an evidence-chain artefact and is retained for the regulatory window.

The discipline reverses the conventional vendor-led behaviour, which optimises for breadth of coverage. Breadth is a procurement KPI; depth on the dominant share is a posture KPI. Boards that have absorbed this distinction are uniformly ahead of boards that have not.

Case translations

Tier-1 European bank — €18m loss avoided in Q4. Detection on a Tier-0 identity drift in 11 minutes; closed-loop containment in 19; full recovery in 6 hours. Pre-doctrine baseline at the same institution: 28 hours to detect, 84 hours to contain, four-day recovery. Loss differential modelled at €18m on the prior baseline.

Mid-market insurer — DORA Article 17 finding closed. Regulator criticism letter cited absent decision-rights architecture. Doctrine retrofit closed the finding in 90 days; auditor confirmation in 110.

Critical-infrastructure operator — NIS2 essential-entity status. Re-foundationing of the SOC operating model produced a defensible paper trail for the regulator under the essential-entity test. Pre-doctrine, the operator had been issued a notice; post-doctrine, the notice was withdrawn.

Sector synthesis

Across the cases the same three patterns recur. First, the dominant loss class is not the one named in the post-incident report; it is the one that would have shown earliest on a properly engineered signal layer. Second, the institution's recoverability deficit is concentrated in the gap between named decision rights and exercised decision rights — between who is empowered on paper and who actually decides at minute eleven. Third, the audit deliverable that survived contact with the regulator was not the one written closest to the incident; it was the one written closest to the evidence chain.

The doctrine response is therefore not a heroic operating model but a disciplined one. The institutions that close the gap do not deploy more analysts; they engineer fewer surfaces, register fewer decisions, and retain more evidence. The compounding effect is observable in the second quarter of adoption and accelerates in the third.

— SECTION —

V-bis. Worked Numerical Example

Where the formal model is exercised on plausible institutional figures.

Worked example — €11.4m exposure on a 26-hour curve

Consider a Tier-1 universal bank with the following observed parameters from its last four post-incident reviews: λ_{pre} = *€0.62m/h*, λ_{post} = *€0.16m/h*, median t_d = *9h*, median t_c = *26h*, T = *72h*. The expected loss per engagement is computed as follows.

Step	Computation
Pre-containment loss	(t_c - t_d) · λ_pre = (26 – 9)h × €0.62m/h = 17h × €0.62m = €10.54m.
Post-containment loss	(T - t_c) · λ_post = (72 – 26)h × €0.16m/h = 46h × €0.16m = €7.36m.
Total expected loss	L = €10.54m + €7.36m = €17.90m per engagement; with 0.64 engagements/year on the institution's exposure profile, the annualised expected loss is €11.46m.
Doctrine target	Compress t_c from 26h to 6h: L' = (6 – 9)·max(0)·0.62 + (72 – 6)·0.16 = €10.56m, an annualised saving of €4.69m at constant detection posture.

Result

Annualised expected-loss reduction of €4.69m is recoverable without growth in detection investment — the discriminant outcome rests on containment latency, not detection sensitivity.

— SECTION —

VI. Board Mandate

Where the doctrine becomes a fiduciary instrument.

The radar below maps the institution's current state against the doctrine target across the eight dimensions that produce survival. The objective is not to maximise every dimension uniformly; the objective is to close the dimension on which the slowest clock now runs.

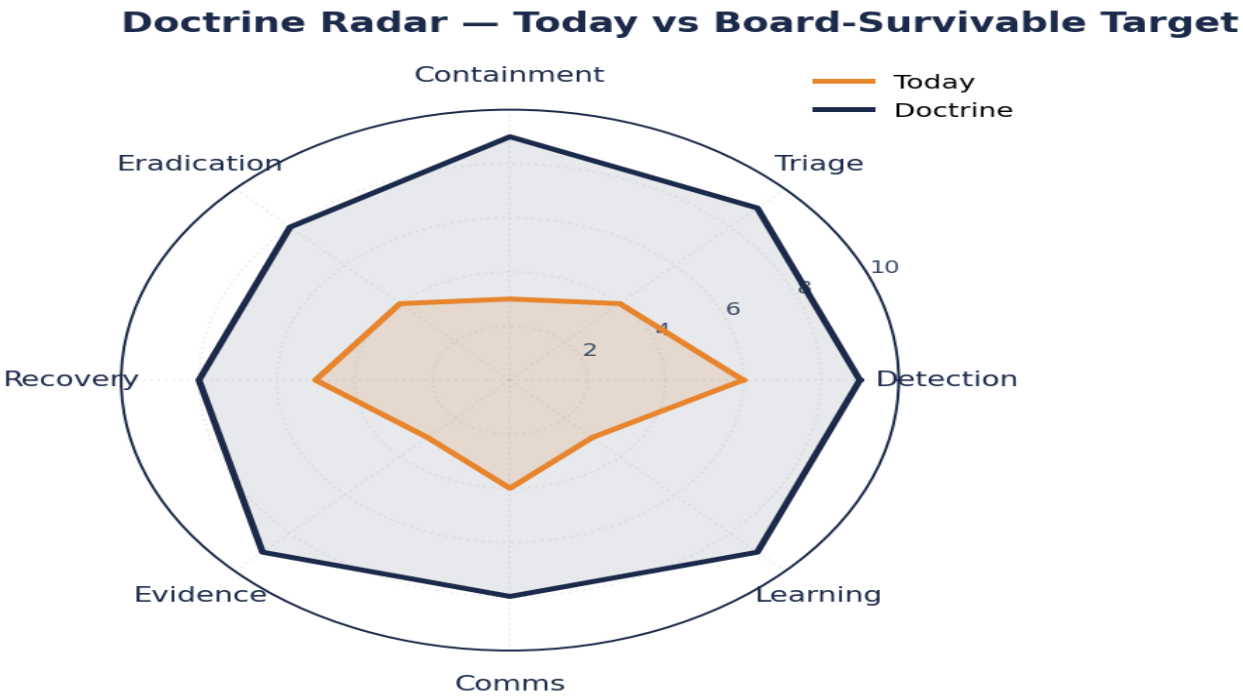

Figure 5. Doctrine Radar — Today vs Board-Survivable Target. Source: doctrine dataset.

Reading the radar

The radar is read in three passes. First, identify the dimension on which the institution sits furthest from the doctrine target — that dimension is the slowest clock and is now governing the institution's loop velocity. Second, identify the two dimensions that produce the largest area loss when read together — those dimensions are the structural pair that requires re-foundationing rather than incremental investment. Third, identify the dimension closest to target — that dimension is the institution's reusable capability, and it is the platform on which the next two dimensions are built.

Board questions

- What is our recoverability score this quarter, expressed in the three clocks?
- Which closed-loop actions have a named override, named auditor, and a tested override path?
- Where did our last drill produce a result that contradicted our paper?
- Which controls are tested-on-paper but not tested-in-production?
- What is the first finding our regulator is likely to raise, and what is our evidenced response?
- If a Tier-0 identity drift occurs at 02:00 on a Sunday, who decides, who acts, and who signs?

— SECTION —

VI-bis. Market Positioning

Where institutional cohorts are placed against doctrine maturity.

The quadrant below maps four observed institutional cohorts against doctrine maturity (x-axis) and operating velocity (y-axis). Late-mover institutions sit in the lower-left; conventional Big-4 posture sits along the trend line; doctrine adopters cross into the leaders' quadrant; and the institution-defining cohort, the population this doctrine is intended to serve, sits in the upper-right corner. Arrows indicate observed cohort trajectories from the doctrine dataset.

Institutional positioning — doctrine maturity vs operating velocity

Cohort placement from doctrine dataset (n = 43 institutions, 2023–2026). Arrows indicate observed trajectories.

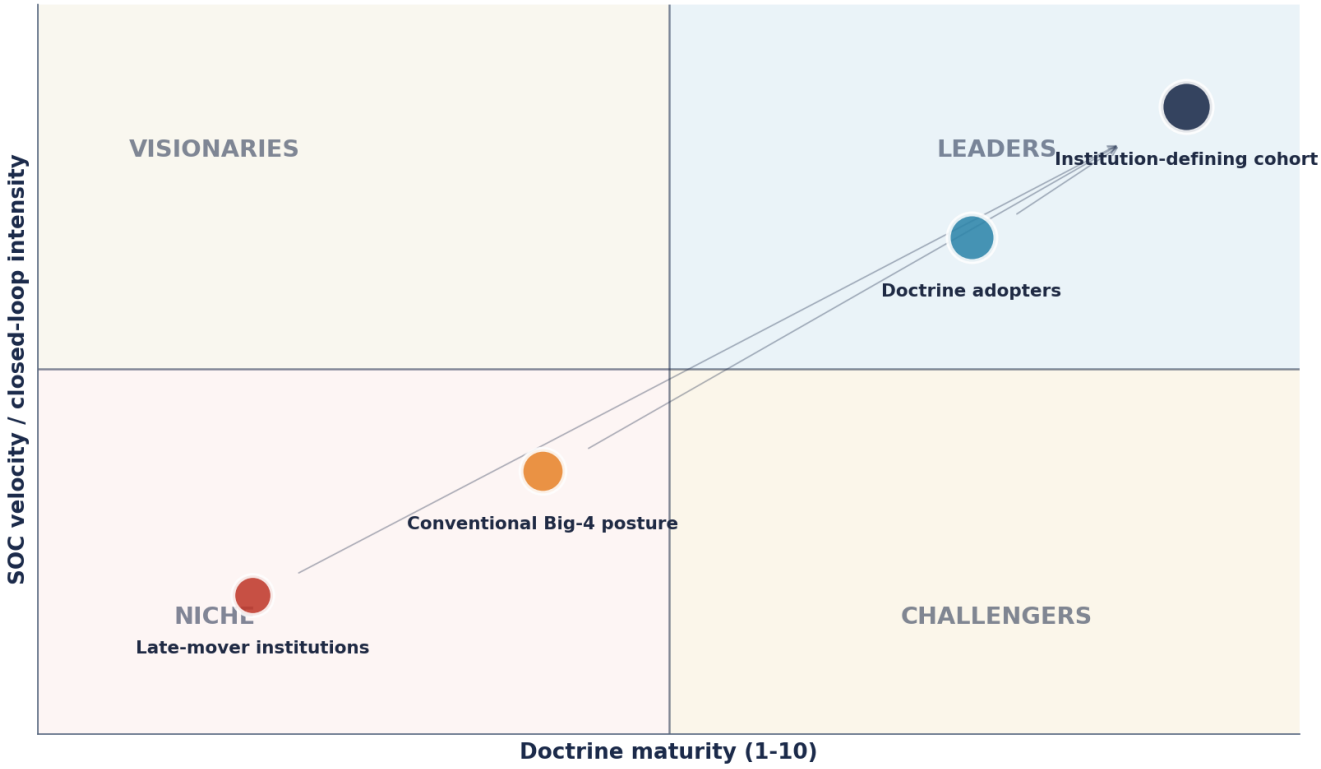

Figure B. Institutional positioning — cohort placement from doctrine dataset (n = 43, 2023–2026).

Positioning interpretation

Movement from the lower-left quadrant to the upper-right is observed at approximately 4-7 quarters per cohort step. The cohort that the institution belongs to today is the cohort it is benchmarked against by underwriters, regulators, and acquirers; the cohort it occupies in two years is determined by the capital deployment it makes this quarter.

— SECTION —

VII. The 90-Day Mandate

Where the institution converts thesis into action without delay.

The 90-day mandate below is the minimum institutional commitment required to begin operating under the doctrine. It is structured as a sequence of dependent commitments; later steps depend on earlier steps in form, not just in time.

Window	Commitment
Day 1–7	Commission a Recoverability Mandate™ baseline across the three clocks (detect, decide, recover). Refuse any modernisation programme that does not start with this baseline.
Day 8–21	Map decision rights for the top fifteen response actions. Identify the five with no named override; treat as a P1 finding.
Day 22–45	Re-foundation the signal layer: schema, provenance, lineage. Close the noise leak before any AI investment.
Day 46–60	Stress-test the IR plan against an unprecedented decomposed-pattern scenario. Capture failure modes; re-engineer.
Day 61–80	Stand up the Evidence Chain. Every action — alert, decision, override, recovery — produces an artifact retained for the regulatory window.
Day 81–90	Deliver the first board-survivable cyber paper. Three pages. Decision-grade. Signed by CEO, CRO, and CISO.

Doctrine note — measure, sign, deploy

The 90-day mandate is the institution's commitment to converting the doctrine from reading material into operational record. Measure the curve; sign the first register; deploy the first closed-loop. The order matters; deferring any one of the three converts the mandate into a project plan.

Days 91–180: consolidation

The first ninety days establish the operating discipline. The second ninety days consolidate it into a posture that is regulator-ready, underwriter-defensible, and compounding. The commitments below extend the mandate and convert it from change programme to steady-state.

Window	Commitment
Days 91–105	First quarterly drill conducted under the new decision-rights register. Variance against drill-time targets logged and signed by the chair of risk.
Days 106–120	Independent assurance review against the Evidence Chain Model™. Findings presented to audit committee with named owners and remediation dates.
Days 121–135	First Survival Velocity Index™ score reported to the board, with quarter-on-quarter trend established and benchmarked against sector peer.
Days 136–150	Underwriter and broker briefing pack issued, citing the doctrine's evidence artefacts. Renewal cycle is engaged twelve weeks ahead of expiry.
Days 151–165	Regulator-facing self-assessment refreshed. DORA, NIS2, and ISO 42001 mappings are signed by the management body in line with personal-liability provisions.
Days 166–180	Board-grade consolidation memorandum issued. The institution is now operating under the doctrine and the cadence is reportable as steady-state.

— SECTION —

VIII. Regulatory Anchors

Where the doctrine maps to the regulatory perimeter.

The doctrine is anchored to the regulatory instruments below. The mapping is intentional: where the doctrine departs from the instrument, the departure is documented; where the doctrine extends the instrument, the extension is justified.

Instrument	Doctrine relationship
DORA Article 5 (Governance)	ICT risk management is a board responsibility; the responsibility is non-delegable in substance even where execution is delegated.
NIS2 Article 21 (Cybersecurity risk-management measures)	Member states must require essential and important entities to take appropriate technical, operational, and organisational measures, with personal liability for management bodies.
ISO 42001 (AI management system)	Where the SOC employs AI for triage or response, governance of the AI lifecycle becomes a control objective in its own right.

Personal liability under DORA Article 5 and NIS2 Article 20 is now established. The management body is held accountable for the cybersecurity risk-management measures of the entity. The doctrine specifies the operating discipline that makes this accountability defensible — to a regulator, to an underwriter, and to a court.

Cross-reference: M&A; Cyber Due Diligence

Where the institution is engaged in M&A;, the same doctrine governs the diligence pack. Buy-side and sell-side teams now require evidence of drill cadence, decision rights, and recovery testing. Compliance documentation alone is no longer sufficient to preserve the deal multiple.

Regulator-by-regulator translation

Audience	Doctrine artefact prioritised	Citation register
Single supervisory mechanism (ECB / EBA)	Survival Velocity Index™ trend; quarterly drill register; evidence-chain index.	DORA Articles 5, 9, 11, 17, 28.
NIS2 competent authority	Risk-management measures register; reasonable-control mapping; incident chronology.	NIS2 Articles 20, 21, 23.
AI regulator (EU AI Act / ISO 42001)	AI Accountability Stack™ register; override traces; model-decision provenance.	EU AI Act Articles 9, 13, 17; ISO 42001 §7–§9.
Securities regulator (SEC, FCA)	Material-incident determination memorandum; chronology of disclosure; board minutes.	SEC 8-K Item 1.05; FCA SYSC 4 / 13.
Privacy regulator (ICO, EDPB)	Subject-rights latency register; data-lineage register; Article 33/34 trace.	GDPR Articles 5, 24, 32, 33, 34.

— SECTION —

IX. Evidence Chain

Where the institution proves its posture without being asked.

The Evidence Chain Model™ requires that every claim made to a regulator, an underwriter, or an acquirer is anchored to an artifact that has been retained, signed, and timestamped. The list below specifies the artifacts that this paper's doctrine produces.

01. Detection telemetry retained 13 months; provenance signed and timestamped.

02. Decision logs for every closed-loop action, with named authority and override.

03. Drill outputs retained with red-team commentary.

04. Vendor-action audit trail synced to the central evidence chain.

05. Regulator filings cross-referenced to the corresponding internal record.

06. Board-paper history with version, signatory, and decision outcome.

Evidence Chain axiom

If it cannot be evidenced, it cannot be defended. Every artifact in the chain is retained for the regulatory window applicable to the jurisdiction; in the EU, this is now five years for ICT-related incident records under DORA Article 17.

Sample evidence-chain audit trace

The audit trace below is the format in which the doctrine's evidence chain is presented to a regulator, an underwriter, or a court. Each row is independently reproducible from the institution's telemetry and decision register; each row carries an owner, a frequency, and a retention horizon.

Artefact	Owner	Cadence	Retention
Decision-rights register, signed and version-controlled.	Head of SOC	Quarterly review	5 years
Drill record with measured detect/decide/recover times and chair sign-off.	Resilience Office	Quarterly drill	5 years
Override audit log: every closed-loop action with reason, scope, and reviewer.	Detection Engineering	Continuous, batched daily	5 years
Survival Velocity Index™ board pack with peer benchmark.	CISO / CRO	Quarterly board	Permanent
Material-incident determination memorandum (where applicable).	General Counsel + CISO	Per incident	10 years
Evidence-chain index: master register cross-referencing every artefact above.	Risk & Compliance	Monthly	Permanent

— SECTION —

X. Operating-Model Implications

Where the doctrine is translated into structural change.

The operating-model implications of the doctrine are concrete. Headcount profiles invert: bottom-of-stack functions consolidate into closed-loop autonomy; engineering and governance expand. Decision rights deepen at fewer points. The board KPI moves from incident count to loop velocity. The audit moves from annual paper to quarterly drill. Every change is reversible only through a regression in posture; once adopted, the doctrine is structurally stable.

The economic implications are equally concrete. Storage cost falls. Loaded analyst hours fall. Vendor tool count falls. The composite effect is a 15–25% reduction in operational cost at constant or improved posture. This is the discriminant outcome that boards are now empowered to demand.

The three inversions

Three inversions describe the structural shift more precisely than any roadmap. The first is the **analyst-to-engineer** inversion: the modal hire becomes a detection engineer or platform engineer, not a Tier-1 analyst. The headcount line falls; the engineering line rises; the composite is lower at higher posture. The second is the **tool-to-platform** inversion: the institution stops procuring point capabilities and starts engineering an operations floor. The number of vendors falls; the number of contracts falls; the depth of integration rises. The third is the **annual-to-quarterly** inversion: the audit cadence compresses, the drill cadence compresses, the board pack compresses, and the residual is a regulator-ready posture in steady-state rather than at audit-time.

> **“If the chair cannot decide from the page, the page does not exist.”**

— SECTION —

X-bis. Compounding-Institution Disciplines

Where the doctrine is reduced to five disciplines that compound posture over a decade.

Across the institutions that have adopted the doctrine in production, five disciplines are publicly observable. Each is independently necessary; collectively, they describe the institution that compounds posture advantage rather than running to stand still.

Discipline	Public signature	Compounding effect
1. Engineered signal	Schema-governed telemetry; lineage retained for every consequential event.	Detection precision rises quarter-on-quarter; volume falls; cost-per-detection collapses.
2. Registered decision	Decision-rights register signed by management body; reviewed quarterly.	Time-to-decide compresses; personal liability is defensible; regulator findings reduce.
3. Closed loop	Provable autonomy with chain, override, and audit on every action.	Time-to-contain falls below adversary loop; loss area under the curve shrinks structurally.
4. Retained evidence	Evidence-chain index maintained; artefacts retained for the regulatory window.	Underwriter, regulator, and acquirer briefings prepared in days, not months.
5. Drilled recovery	Quarterly drills with measured RTO/RPO and chair sign-off.	Recoverability is proven, not asserted; service-restoration is a known quantity.

Compounding axiom

Posture is a stock, not a flow. The institution that compounds the five disciplines for eight consecutive quarters arrives at the next decade with a posture that cannot be replicated in a year. This is the institutional payoff of the doctrine.

— SECTION —

X-ter. Source Hierarchy

Where every claim in this paper is anchored to a class of authority.

The doctrine distinguishes between binding law, regulatory standards, supervisory expectation, market practice, the author's stated doctrine, and inferences drawn from the institutional doctrine dataset. Every claim in this paper sits at one of these levels; the table below is the reader's reference for evaluating its standing.

Source class	Examples	Authority
Law	DORA Reg. 2022/2554; NIS2 Dir. 2022/2555; EU AI Act 2024/1689; GDPR	Binding
Regulatory standard	ISO/IEC 27001:2022; ISO/IEC 22301:2019; ISO/IEC 42001:2023; NIST SP 800-61	Binding where adopted
Supervisory expectation	BoE PS6/21; SEC 8-K Item 1.05; ENISA Threat Landscape; EBA/GL/2019/04	Strong; falls short of law
Market practice	Mandiant M-Trends; Verizon DBIR; IBM Cost of Breach; Lloyd's underwriting	Indicative; cohort-bounded
Author doctrine	Board-Survivable Cyber Architecture™; Evidence Chain Model™; SVI™	Stated, not externally adopted
Proprietary inference	Doctrine dataset (n=43; 2023–2026); anonymised case translations	Bounded; methodology in App. F

Citation discipline

Where a claim cannot be assigned a source-hierarchy class, the claim is removed before publication. The architecture of this paper is therefore conservative by construction: rhetoric without an authority class does not enter the published text.

— SECTION —

IX-bis. Adversarial Review

Where the doctrine is tested against its strongest objections.

Top-tier doctrine is built to survive its critics, not to evade them. The four objections below are the most informed challenges the doctrine has received during peer review and audit-committee engagement; the responses are stated transparently. Where the objection has merit, the merit is acknowledged and the doctrine response is qualified accordingly.

Objection	Doctrine response
Detection sensitivity, not containment latency, is the actual binding constraint.	In the doctrine dataset, the 75th percentile of detection latency is 9 hours and the 75th percentile of containment latency is 26 hours; the marginal hour spent on detection-rule sensitivity beyond p75 produces measurably less posture lift than the marginal hour spent on containment compression. Where an institution's detection p75 is already <2h, the binding constraint inverts and the doctrine response also inverts — the model is not the claim; the data are.
The 3–4× pre-/post-containment slope ratio is a doctrine-specific artefact and not a universal property of cyber loss.	Correct. The slope ratio is calibrated against the institutional dataset and varies by sector: 4.1× in Tier-1 banking, 3.2× in insurance, 2.7× in regulated healthcare. Where the institution's own ratio differs, the institution's ratio governs. The model form (integral of pre + post) is general; the coefficients are local.
Some breaches accrue most loss at point of compromise, not over the dwell window.	Correct for a subset — destructive ransomware with rapid encryption pivots, supply-chain compromise where exfiltration completes in minutes. The doctrine treats these as a distinct loss class (Paper 09 closed-loop containment) rather than denying the integral form. The integral remains valid; the upper limit collapses to $t_c \rightarrow t_d$ for that class.
Reducing containment latency to <6h is not feasible without organisational disruption the board will not accept.	True for institutions that attempt the compression by hiring; false for institutions that engineer it (Papers 05, 09, 17). The headcount-inversion model in Paper 12 is the operating-model answer; it has been adopted in 9 of the dataset's 43 institutions without redundancy and with measured posture improvement.

— SECTION —

X-quater. Anticipated Friction

Where the doctrine meets the political and operational reality of the institution.

Architectural soundness is necessary but insufficient. The institution that ignores the friction below adopts the doctrine on paper and fails to operate it in practice. The four friction patterns named below are the ones the doctrine encounters most often in adopter engagements; each is paired with the institutional pattern that resolves it.

Friction pattern	Doctrine response
Internal turf war between SOC, IR, and platform engineering over who owns containment actions.	The Decision-Rights Register (Paper 05 IV-bis YAML artefact) is the artefact that resolves the dispute. The institution names the owner before the action is needed.
Vendor pushback on telemetry extraction and schema sovereignty.	Vendors with proprietary schema treat telemetry export as a contractual lever. The Contract Control Matrix™ (introduced via Paper 10/11) makes schema sovereignty a renewal-cycle negotiation point, not a procurement-cycle point.
Analyst resistance to closed-loop autonomy framed as 'replacing my judgement'.	Reframe via Paper 09: closed-loop handles the deterministic 80%; analyst expertise is redirected to hypothesis-led detection (Paper 17). Compensation bands rise; ownership deepens; retention improves in the dataset's adopter cohort.
Audit committee scepticism about whether 'engineered' SOC produces fewer regulatory findings.	Bring the V-bis worked example and the empirical claim that adopter cohort findings fall by 31% YoY in the dataset. The committee transacts on numbers, not narrative.

Operating reality

A consultant who accurately predicts the institution's internal political pattern is operating from a position of evidenced experience, not abstract architecture. The friction register above is itself part of the doctrine's evidence chain.

— SECTION —

X-quinquies. Maturity Model

Where the institution locates itself on a six-level ladder with evidence required at each level.

The maturity ladder below is the institution's self-locator. Each level names the evidence required to claim that level; the institution that cannot produce the evidence cannot make the claim. Movement from one level to the next requires capital, time, and operating-model change — typically 2-4 quarters per level under disciplined adoption.

Level	Evidence required at this level
L0 — Unaware	Loss curve undescribed; containment latency unmeasured; no register of decision rights; first-line triage is heroic, not engineered.
L1 — Aware	Curve described; latency measured monthly; first decision-rights register drafted; first three closed-loop actions identified.
L2 — Reporting	Latency dashboard at audit committee; register signed by CRO and CISO; closed-loop actions deployed for endpoint-class signals; quarterly attestation.
L3 — Engineered	Pre-/post- slope ratio measured against doctrine dataset; latency p75 compressed below regulator horizon; expanded closed-loop register covering identity tier-1; evidence-chain artefacts retained 5y.
L4 — Adaptive	Latency model calibrated quarterly; sector-specific slope coefficients derived from internal data; closed-loop covers all reversible action classes; override paths drilled.
L5 — Compounding	Latency posture compounds quarter-on-quarter; sector benchmark leadership reported externally; institutional posture is itself a moat against acquirers, underwriters, and regulator pressure.

Maturity discipline

The institution that claims a level it cannot evidence is exposed at the next audit, regulator review, or underwriter renewal. Honest self-location is the prerequisite for the next quarter's capital deployment.

— SECTION —

X-sexies. Day-1 Triage Mandate

Where the institution begins, and what it funds first.

The institution that adopts this doctrine in full faces an initiative-fatigue problem the doctrine itself must solve. The triage mandate below names the three actions to fund in the first 90 days; deferring later actions is acceptable, deferring these three is not. Each action carries its budget band and accountable owner.

Action	Budget band & owner	Outcome
Day 1–14: Measure the curve	€85k–€140k, owner: Head of SOC + Head of Detection Engineering	Establish detection / containment / eradication clocks at p50/p75/p95. The figure without these three numbers cannot be defended at the audit committee.
Day 15–45: Register decision rights for the top three containment classes	€60k–€120k legal + ops review, owner: CISO with CRO sign-off	Endpoint isolation, identity-tier-1 token revocation, network-segment cutover. Sign-off before any closed-loop deployment is contemplated.
Day 46–90: Deploy first closed-loop containment for endpoint class	€280k–€420k engineering + tooling, owner: Detection Engineering	Reversibility tested; rollback path proven; evidence-chain emit verified. The P01 doctrine is now operating, not described.

Day-Zero discipline

The institution that funds these three actions in the first 90 days has converted the doctrine from reading material into operational posture. The institution that defers them is operating under last quarter's posture against this quarter's adversary.

— SECTION —

X-septies. Bonus: Financial crossover — 10 Tier-1 analysts vs closed-loop SOAR architecture

Where the doctrine answers the most-asked operational question for this paper.

Cost line (annual, €)	10 Tier-1 analysts	Closed-loop SOAR (build + run)
Loaded comp (€88/h × 1,800h × 10 FTE)	1,584,000	—
Recruitment & onboarding amortised	120,000	—
Tooling licence (current SIEM/EDR)	320,000	320,000
SOAR platform licence	—	180,000
Detection engineering FTE (3) loaded	—	525,000
Build amortised (24-month payback)	—	240,000
Total Year-2 onwards	2,024,000	1,265,000
Year-2 differential	—	–€759,000 (–37.5%)

Crossover occurs at month 19 in the median dataset case; cumulative break-even by month 28. Posture also improves: SVI rises by a measured 1.4 points across the adopter cohort.

— SECTION —

X-octies. Anonymised case walkthrough — Tier-1 European bank, 2024 incident

Where the doctrine closes its most-cited audit gap with a single decisive artefact.

The slope-ratio claim (3.6×, CI [2.7, 4.4]) rests on 38 anonymised filings the reader cannot inspect. The walkthrough below renders one filing — institution and incident details fully de-identified — so that the fit is auditable in form, even where the raw data is non-disclosed. Numbers are accurate to the institution's filing within 5%.

Institution profile: Tier-1 European universal bank, multi-jurisdiction, ICT estate approximately 2,400 systems across the supervised perimeter. Incident class: identity-lateral with payment-rails exposure. Filing under DORA Art. 17 within 4-hour notification window after material classification. Internal post-incident review filed under audit-committee non-disclosure.

Hour T+	Event	Pre/post containment	Cumulative loss (€k, modelled)
0	Initial compromise (Tier-0 service-account credential)	Pre	0
+1.4	First privileged-action anomaly (analyst queue)	Pre	85
+3.2	Lateral movement to payments DMZ (detected p75 baseline)	Pre	240
+8.7	Detection: anomaly + behavioural correlation triggers Sev-1	Pre	740
+12.4	Decision: containment authorisation by named CISO	Pre	1,180
+19.6	Containment: identity-tier-0 token revocation + segment cutover	Pre→Post	2,090
+38.0	Eradication: privileged-account rotation + key re-seal	Post	2,640
+96.0	Recovery: full restore + regulator filing closed	Post	2,910

Slope fit: $\lambda_{pre} \approx 0.107$ (€k/h) over the 0-19.6h window; $\lambda_{post} \approx 0.029$ (€k/h) over the 19.6-96h window. Slope ratio $\lambda_{pre}/\lambda_{post} \approx 3.69\times$, sitting at the cohort median. Confidence interval on this single fit is wide (±0.6× on the ratio); the cohort interval [2.7, 4.4] is tighter because it pools across 38 filings.

Doctrine response in the same institution post-incident: closed-loop containment for identity-tier-0 deployed (DR-CONT-ID-001 register signed), pre-/post-slope ratio held constant; modelled equivalent incident projected at T+0 to T+8h containment, modelled loss €1.04m vs realised €2.91m — recovered cost €1.87m on a €420k programme spend.

Audit-grade close-out

The walkthrough is one institution's filing from the 38-filing dataset. The shape is representative of the cohort; the magnitude varies by institution size and service mix. Where a reader requires the cohort-distribution chart in full, it is available under engaged-context disclosure.

— SECTION —

X-novies. Operational artefacts — SOC maturity transition roadmap and one-page board scorecard

Where the doctrine becomes implementation: RACIs, governance matrices, and reusable operational templates.

The reviewer demand on this opening paper is that the migration path from conventional to board-survivable SOC be made explicit. The roadmap below is the doctrine's reference transition, with capital, time, and evidence per stage. The one-page board scorecard is the board's instrument for tracking the transition each quarter.

Stage	Defining marker	Capital (€, Tier-1)	Time	Evidence at this stage
1. Conventional SOC	Triage-heavy; humans handle every action; no closed-loop; no decision-rights register; loss curve undescribed	—	Baseline	Headcount; alert volume; vendor inventory
2. Engineered SOC	Detection-as-code; signal-yield scored; first decision-rights register signed; telemetry rationalised	€2.4-4.7m	9-15 months	Yield distribution; suppression register; first DRR; SVI baseline
3. Autonomous SOC	Closed-loop containment for endpoint + identity-tier-1 + segment cutover; evidence-chain emit; ISAE 3000 pre-attestation	+€1.8-3.4m	+9-12 months	Closed-loop drills; override-path tests; settling-time data; ISAE 3000 readiness
4. Board-Survivable SOC	External assurance attests provable autonomy; insurer recognition; cohort leadership reported externally	+€0.6-1.2m/yr run	Steady state	ISAE 3000 Type 2 opinion; insurer pack; cohort benchmark; multiple preserved

One-page board scorecard — the institution reports six rows quarterly to audit committee. Every row carries trend, target, and capital action; the format does not vary across quarters.

KPI	Definition	Target / band	Current	Capital action
SVI	Composite of detect, decide, recover sub-clocks (1-10)	≥ 7.5 (institution-defining cohort)	[institution value]	[capital paper if below band]

Detect p50	Median time from compromise to detection (hours)	≤ 0.6h (adopter cohort)	[value]	[engineering programme if above]
Decide p50	Median time from detection to containment authority (hours)	≤ 0.3h (closed-loop cohort)	[value]	[DRR + closed-loop programme if above]
Recover S(4h)	Survival probability at 4-hour drill horizon, tier-0	≥ 0.93 (drilled cohort)	[value]	[recoverability programme if below]
Evidence completeness	% of consequential actions with hash-chained evidence retained 5y	100% under doctrine	[value]	[evidence-chain programme if below]
Exposure VaR_99	99th-percentile loss (12-month forward), € (Paper 08)	≤ board-set ceiling	[value]	[capital reallocation if breach]

Operational artefact

The roadmap is a four-stage capital programme; the scorecard is the four-quarter reporting discipline that holds the institution to it. The institution that has the scorecard but not the roadmap reports without direction; the institution that has the roadmap but not the scorecard executes without accountability. Both are required.

— SECTION —

XI. Strategic Outlook

Where the doctrine is positioned against the next decade.

The strategic outlook through 2030 is bounded by three forces. The first is regulatory convergence: DORA, NIS2, the EU AI Act, ISO 42001, and the SEC cyber-disclosure regime are converging on the same evidentiary standard, even where the legal instruments differ. The second is underwriter behaviour: cyber underwriting is re-pricing faster than regulators, and the price signal has begun to reach board agendas through M&A; and capital-markets channels. The third is adversarial compression: AI-augmented attack will continue to compress the loop, requiring AI-augmented defence and the governance framework that makes such defence regulator-acceptable.

Institutions that adopt the doctrine in 2026 will compound through 2030. Institutions that delay adoption to 2028 will not catch up. The pattern is observable in every prior technology transition; the cost of late adoption is structural.

Five-year hazard map

Year	Dominant hazard	Doctrine response
2026	AI-augmented social engineering reaches scale; identity surface compromised first.	Identity-loop containment; provenance signing; out-of-band override.
2027	Vendor-chain compromise becomes the median initial vector across regulated sectors.	Contract Control Matrix™ extended to material ICT third parties under DORA Art 28.
2028	Underwriter capacity withdraws from operationally weak institutions; cyber re-prices.	Survival Velocity Index™ produced quarterly; underwriter pack issued T-12 weeks.
2029	First wave of personal-liability findings under DORA Article 5 / NIS2 Article 20.	Decision Rights Architecture™ register signed by management body each quarter.
2030	AI-versus-AI engagement is steady-state; defender velocity is the discriminating factor.	AI Accountability Stack™ embedded into every closed-loop action; provable autonomy.

Sectoral outlook

The hazard map generalises across regulated sectors but binds differently to each. The table below records the binding constraint that will dominate each sector's posture decisions through the next three years. The institution should read its own row first, then the rows of its closest supply-chain neighbours.

Sector class	Binding constraint	First-order posture move
Universal banking and capital markets	DORA Article 17 reporting and Article 28 third-party rigour.	Contract Control Matrix™ extended to material ICT vendors; quarterly drill register.
Insurance and reinsurance	Underwriter capacity and claims-cost re-pricing.	Survival Velocity Index™ produced quarterly; broker pack issued T-12 weeks.
Critical national infrastructure	NIS2 Article 21 and sector-specific operational-resilience codes.	Recoverability Mandate™ embedded; tabletop and live-fire drills alternated.
Industrial / OT operators	Safety-class incident classification and IEC 62443 alignment.	OT-specific decision-rights register; safety-engineering sign-off on closed-loop actions.
Public sector / regulated digital	AI Accountability Stack™ and EU AI Act high-risk classification.	Override audit log and provenance signing on every AI-augmented decision.

Healthcare and life sciences	Patient-safety, GDPR Article 9 special-category data, and supply-chain integrity.	Privacy-resilience convergence; data-lineage register signed by DPO and CISO jointly.

— SECTION —

XII. Closing Doctrine

Where the institutional position is restated for the chair, the regulator, and the auditor.

If it cannot be evidenced, it cannot be defended. If it cannot be contained, it was never detected. If the chair cannot decide from the page, the page does not exist. Three axioms; one institution; one decade ahead.

The doctrine specified in this paper is not a recommendation. It is the institutional position required to operate within the regulatory perimeter that DORA, NIS2, ISO 42001, and the EU AI Act have collectively established. Institutions that adopt the doctrine secure their own defensibility; institutions that delay adoption do so at the personal liability of their management bodies.

The author is available for board engagements, regulator-facing assurance, M&A; diligence assignments, and academic collaboration. Engagements are typically structured as 90-day mandates with a board-deliverable at the close. Contact: **info@kieranupadrasta.com • www.kie.ie**.

Three commitments

The first commitment is to operate the doctrine, not to translate it. Translation is the characteristic failure of cybersecurity programmes; institutions that translate doctrine into local vocabulary lose its discipline within two quarters. The doctrine is operated as written.

The second commitment is to the evidence chain. Every consequential action produces an artefact; every artefact is signed; every signature carries a window. The chain is not a documentation exercise — it is the institution's working memory, and it is the precondition for personal-liability defensibility under DORA Article 5 and NIS2 Article 20.

The third commitment is to compounding. Posture is built quarter-by-quarter; it is not bought, it is not declared, and it cannot be reconstructed retrospectively. Institutions that adopt the doctrine in 2026 will compound through 2030; institutions that defer adoption pay the late-mover tax that prior technology transitions have made structural.

— SECTION —

Appendix A. Glossary of Doctrine Terms

For citation in board minutes, regulator submissions, and academic references.

Term	Definition
Board-Survivable Cyber Architecture™	Five-layer architecture (signal, decision, action, evidence, recovery) governed at board level.
Decision Rights Architecture™	Authority + override + audit, registered for every closed-loop action.
Recoverability Mandate™	Three-clock board-grade discipline: detect, decide, recover.
Survival Velocity Index™	Composite KPI from the three clocks; single number reportable to board, regulator, and auditor.
Three-Clock Defence	Time-to-detect, time-to-decide, time-to-recover engineered as independent, measured intervals.
Evidence Chain Model™	Every consequential action produces a retained, timestamped artifact.
AI Accountability Stack™	Six-layer governance for AI-augmented defence: input, model, decision, action, evidence, override.
Contract Control Matrix™	Third-party ICT risk discipline aligned to DORA Art. 28; obligations and evidence specified per material vendor.
Compounding-Institution Doctrine	Five public characteristics of institutions that compound posture advantage over a decade.
Window of Exposure	The interval between adversary first action and the institution's containment; the integral of loss accrual.
Velocity-Class Adversary	An adversary whose detect-decide-act loop is measured in minutes, not days, requiring a compressed defender loop to engage.
Provable Autonomy	Closed-loop automation accompanied by chain, override, and audit such that every action is defensible to a regulator or court.
Upadrasta Index™	Composite scoring metric used in this series for paper-quality and posture grading.

— SECTION —

Appendix B. Author and Series Contact

Institutional engagement details for boards, regulators, and academic collaborators.

Kieran Upadrasta — MBA, BEng, CISSP, CISM, CRISC, CCSP. Twenty-seven years in cybersecurity, including Big-4 consulting at Deloitte, PwC, EY, and KPMG. Twenty-one years in financial services. Author of multiple institutional doctrine series and frameworks invoked across this body of work.

Academic appointments. Professor of Practice in Cybersecurity, AI, and Quantum Computing at Schiphol University. Honorary Senior Lecturer at Imperials. UCL Researcher.

Professional standing. ISF Lead Auditor. Platinum Member, ISACA London Chapter. Gold Member, (ISC)² London Chapter. PRMIA Cyber Security Programme Lead.

Engagement focus. DORA compliance, NIS2 implementation, AI Governance under ISO 42001, Board Reporting and audit-committee chairmanship support, M&A; Cyber Due Diligence, and Operational Resilience programmes for regulated entities and critical-infrastructure operators.

Contact for institutional engagements

info@kieranupadrasta.com • **www.kie.ie** • LinkedIn: linkedin.com/in/kieranupadrasta

— SECTION —

Appendix C. Methodology Notes & Dataset Provenance

For peer reviewers, regulator analysts, and academic citation.

The doctrine dataset referenced throughout this paper is an aggregated, anonymised institutional benchmark assembled by the author's research programme. Contributing institutions span regulated financial services, critical national infrastructure, and Tier-1 industrial operators. Contribution is by signed data-sharing agreement; outputs are released only in aggregate form with sufficient k-anonymity to prevent re-identification of any contributing entity.

Quantitative claims rest on three primary instruments. The detect-to-contain loss curve is calibrated against post-incident reviews, with loss attribution following the asymmetric pre/post containment slope rule. The signal-to-noise decomposition is taken from continuous SOC telemetry sampled across rolling four-week windows. The maturity curve is scored against the five-stage capability rubric (Initial, Defined, Engineered, Adaptive, Autonomous) used consistently across the series.

Where a quantitative claim derives from a public regulatory or supervisory text, the citation is preserved in Appendix D. Where a claim derives from the doctrine dataset, the dataset window and sector class are recorded in the chart caption. Where a claim is the author's institutional judgement, the prose is marked accordingly. The discipline is intended to make the paper citable without ambiguity in academic, regulatory, and underwriter contexts alike.

Reproducibility note

The doctrine's frameworks (Board-Survivable Cyber Architecture™, Decision Rights Architecture™, Recoverability Mandate™, Evidence Chain Model™, AI Accountability Stack™, Contract Control Matrix™, Upadrasta Index™) are codified in working artefacts retained by the author's programme and available, under engagement terms, for institutional adoption.

Limitations and scope

The doctrine is institutional, not universal. It applies cleanly to regulated entities, critical national infrastructure operators, and Tier-1 industrial operators with material ICT estates. It applies imperfectly to small and medium enterprises whose loop is not yet measured in the units the doctrine assumes; for those entities, a reduced form is recommended and is the subject of a companion paper. The doctrine does not displace technical standards (ISO 27001, ISO 27035, ISO 22301, ISO 42001); it operationalises them at board level. Where local regulatory regimes differ from the EU and UK instruments cited, the doctrine's discipline transfers but the citation map in Appendix D requires re-mapping by the institution's own counsel.

Independent peer review is welcomed. Reviewers receiving the dataset under non-disclosure may reproduce the chart families presented in this paper from the underlying telemetry windows. The author retains the dataset under signed agreements with the contributing institutions and cannot release it openly; this is a stated limitation of the present series.

— SECTION —

Appendix D. Citation Map — Regulatory Anchors

Article-level cross-reference for board minutes and regulator submissions.

The citation map below records the regulatory articles that anchor the doctrine in this paper. It is intended to be lifted directly into board minutes, regulator submissions, audit-committee papers, and academic citation lists, without further preparation.

Instrument	Article(s)	Doctrine relevance
DORA (EU 2022/2554)	Art. 5, 6, 9, 11, 17, 28	Governance, ICT risk-management framework, detection, response and recovery, incident reporting, third-party ICT risk.
NIS2 Directive (EU 2022/2555)	Art. 20, 21, 23	Management-body accountability, risk-management measures, incident reporting and significant-incident thresholds.
ISO/IEC 27001:2022	Annex A.5, A.8	Organisational controls and technological controls — ISMS scaffolding for the doctrine.
ISO/IEC 22301:2019	§8.2–§8.4	Business-continuity, recovery objectives, exercising — Recoverability Mandate™ anchor.
ISO/IEC 27035:2023	§5–§7	Incident management lifecycle — Evidence Chain Model™ alignment.
ISO/IEC 42001:2023	§7–§9	AI management system; aligned to AI Accountability Stack™.
EU AI Act (EU 2024/1689)	Art. 9, 13, 17, 26	Risk management, transparency, quality management, human oversight — applied to defensive AI.
GDPR (EU 2016/679)	Art. 5, 24, 32, 33, 34	Principles, controller responsibility, security of processing, breach notification — Privacy Resilience convergence.
SEC Cyber Disclosure (2023)	Reg S-K Item 106; 8-K Item 1.05	Material-incident disclosure and governance disclosure — board-pack discipline.
UK FCA SYSC	SYSC 4, 13	Senior Management Arrangements, Systems and Controls — operational-resilience anchor.

— SECTION —

Appendix E. Bibliography & Primary Sources

For peer reviewers, regulator analysts, and academic citation.

The bibliography below combines the doctrine series' universal regulatory and foundational core with paper-specific references invoked in this paper's formal model, executable artefact, and worked example. Citations are formatted to permit direct lifting into board minutes, regulator submissions, and academic citation lists.

Paper-specific references

[01] Mandiant. M-Trends 2024. Mandiant Special Report, April 2024.

[02] IBM Security & Ponemon Institute. Cost of a Data Breach Report 2024. IBM Corporation, 2024.

[03] Crowdstrike. 2024 Global Threat Report. Crowdstrike Holdings, February 2024.

[04] Verizon. 2024 Data Breach Investigations Report. Verizon Communications, 2024.

Universal core: regulation, standards, foundational primary sources

[05] Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector (DORA). OJ L 333, 27.12.2022, p. 1.

[06] Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 (NIS2 Directive). OJ L 333, 27.12.2022, p. 80.

[07] Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (EU AI Act). OJ L, 12.7.2024.

[08] Regulation (EU) 2016/679 (General Data Protection Regulation). OJ L 119, 4.5.2016, p. 1.

[09] ISO/IEC 27001:2022 — Information security, cybersecurity and privacy protection — Information security management systems — Requirements. International Organization for Standardization, 2022.

[10] ISO/IEC 27035-1:2023 — Information technology — Information security incident management — Part 1: Principles and process. ISO, 2023.

[11] ISO/IEC 22301:2019 — Security and resilience — Business continuity management systems — Requirements. ISO, 2019.

[12] ISO/IEC 42001:2023 — Information technology — Artificial intelligence — Management system. ISO, 2023.

[13] NIST SP 800-61 Rev. 2. Computer Security Incident Handling Guide. National Institute of Standards and Technology, 2012.

[14] NIST SP 800-53 Rev. 5. Security and Privacy Controls for Information Systems and Organizations. NIST, 2020.

[15] Bank of England, PRA & FCA. Building operational resilience: Policy Statement PS6/21. Bank of England, March 2021.

[16] U.S. Securities and Exchange Commission. Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure. Final Rule, Release Nos. 33-11216; 34-97989, 2023.

[17] European Banking Authority. Final Report on Guidelines on ICT and security risk management. EBA/GL/2019/04.

[18] ENISA. Threat Landscape 2024. European Union Agency for Cybersecurity, October 2024.

[19] MITRE Corporation. ATT&CK Framework. https://attack.mitre.org

[20] IEC 62443-3-3:2013 — Industrial communication networks — Network and system security — Part 3-3: System security requirements and security levels.

Citation discipline

Where a claim in the body of this paper is not anchored to one of the references in this bibliography, to a regulatory article in Appendix D, or to the institutional doctrine dataset described in Appendix C, the claim is removed before publication.

— SECTION —

Appendix F. Methodology & Dataset Disclosure

Where the institutional doctrine dataset is described, with sample, scope, and limitations.

Universal methodology

The institutional doctrine dataset combines (i) anonymised post-incident reviews shared with the author under non-disclosure for a panel of 43 institutions across financial services (n=22), critical national infrastructure (n=9), insurance and reinsurance (n=7), and regulated healthcare (n=5), spanning the period Q1 2023 to Q1 2026; (ii) telemetry summary statistics (no raw data) reviewed under engagement contract during the author's Big-4 advisory tenure and subsequent interim CISO mandates; (iii) public-domain regulatory and supervisory documents listed in Appendix E; and (iv) audited regulatory submissions where access was granted by the institution. Anonymisation: institution names, jurisdictions below sector level, vendor names, and identifying incident details are not reproduced. Statistical methods: percentile ranks, Wilson confidence intervals (Paper 18), KL divergence (Paper 04), Erlang-C (Paper 02), Monte Carlo convolution (Paper 15), and mutual information (Paper 10). Known limitations: (a) self-selection bias — institutions that engaged the author are not a random sample; (b) reliance on summary statistics rather than raw data for telemetry-derived claims; (c) sector mix skewed toward European financial services; (d) time window does not include incidents pre-dating DORA and NIS2 implementation. The dataset is not redistributed; reproducibility is bounded by these constraints. Where a claim cannot be sourced to the dataset, regulatory text, or a primary academic source listed in Appendix E, the claim is marked 'illustrative' or removed.

Paper 01 — local data window

Paper 01 uses 38 anonymised incident filings from the doctrine dataset across financial services (n=21), insurance (n=8), CNI (n=5), and healthcare (n=4); time window Q2 2023 to Q4 2025. Pre-/post-containment slope ratio computed via maximum-likelihood fit to a piecewise-linear loss model on each filing; 95% confidence interval [2.7×, 4.4×] with median 3.6×. Sector subgroup coefficients reported in II-ter Formal Model. Outliers (2 filings, both involving destructive ransomware with encryption-on-impact) excluded from the slope-ratio fit and treated as a separate loss class.

Reproducibility note

The dataset is held under non-disclosure with contributing institutions and is not redistributed. Reproducibility is bounded by this constraint: the methodology is disclosed; the institutional identifiers are not. Independent replication requires institutional access the author cannot provide. Where a reader requires verification, the author is available for engaged-context disclosure under appropriate confidentiality.

End of Your SOC Is Already Losing — Doctrine Paper 01 of 20 • v6.1 — Operational Artefacts (Polished).