

# The Database Was Monitored.

Then Show Me the Evidence

~~The Evidence Chain Model for DAM Audit Defensibility Before Regulators and Boards~~

*“Monitoring is not evidence. The chain is the evidence.”*

CENTRAL METRIC

## 6 weeks

Modelled Section-166 duration reduction (illustrative; see Methodology)



### Kieran Upadrasta

CISSP · CISM · CRISC · CCSP · TOGAF 9 · ISO 27001 Lead Auditor · MBA · BEng

27 Years' Cyber Security Experience · 21 Years Financial Services

Professor of Practice in Cybersecurity, AI & Quantum Computing — Schiphol University

[info@kieranupadrasta.com](mailto:info@kieranupadrasta.com) · [www.kie.ie](http://www.kie.ie)

## The Lede

**The database was monitored. Now show me the evidence.**

**Monitoring without a chain of evidence is a claim. Chains are built or they are absent.**

**Boards and regulators no longer accept assertions. They accept artefacts.**

**Evidence Chain Model.** The doctrine that follows is engineered, evidenced, and contract-ready. It is not advisory. It does not produce slides. It produces institution-owned, regulator-grade artefacts on a thirty-, sixty-, and ninety-day clock. The audience is the CISO, the Head of Data, and the Operational Risk Committee.

### Proprietary Frameworks Anchoring This Paper

BOARD-SURVIVABLE CYBER ARCHITECTURE™

EVIDENCE CHAIN MODEL™

UPADRASTA INDEX™

# News Heat — 2024-2026

---

Three dated reference points anchor the urgency of this doctrine. Each is a published, primary source. Each is operational, not theoretical.

## **DORA Article 12 — backup, restoration, recovery (Jan 2025)**

DORA Article 12 introduces explicit obligations on the lifecycle of evidence supporting recovery, broadening the chain-of-custody surface.

## **UK FCA Final Notice (financial-services entity, 2024)**

FCA cited inadequate audit-trail evidence in a 2024 Final Notice as a contributory factor to an enforcement action.

## **EU ENISA Guidance on incident reporting (2024)**

ENISA emphasised the role of operational evidence in incident-reporting quality.

# Executive Summary

**Thesis.** Monitoring is not evidence. Evidence is a chain — obligation, control, telemetry, retention, retrieval, attestation — and the chain is only as strong as its weakest link. Boards and regulators do not buy the claim 'we monitor it'; they buy the chain that proves it.

This paper is written for board directors, chief risk officers, CISOs, internal audit leaders, and senior procurement decision-makers across UK and EU Tier 1 financial services. It is not a vendor brief, and it is not an academic essay. It is operating doctrine — built from twenty-seven years of cyber security delivery and twenty-one years inside regulated financial institutions — written to be quoted in board minutes, cited in committee papers, and used to challenge incumbent assurance.

The argument is built around a single frame: **Evidence Chain Model**. We will move from the regulatory and threat landscape to the named failure modes that recur across Tier 1 estates, to the operational doctrine that neutralises them, to the case evidence, and finally to the 30/60/90-day engagement plan that converts doctrine into demonstrable control.

**Governing aphorism.** If it cannot be evidenced, it cannot be defended. Every chapter that follows tests assurance claims against that single sentence. Every artefact recommended is one a regulator can ask for, a board director can read, and an engineer can produce on demand. No claim is made in this paper that cannot be reduced to a screenshot, a log line, a configuration export, or a signed attestation.

## Primary-Source Anchors

### Article 12

DORA obligation on backup, restoration, recovery

*Regulation (EU) 2022/2554, Article 12*

### 72 hours

DORA initial major-incident notification window

*Regulation (EU) 2022/2554, Article 19*

### 30 days

GDPR DSAR fulfilment window

*Regulation (EU) 2016/679, Article 12(3)*

### 4 business day

SEC material-incident disclosure window

*SEC 17 CFR §229.106 (Dec 2023)*

# Metric Methodology

This paper makes one headline claim. Top-tier work is not persuasive; it is hard to attack. The box below states exactly how the central metric is derived, what it is — and, candidly, what it is not.

<b>Metric</b>	6-week Section 166 reduction
<b>Classification</b>	<b>Modelled scenario (illustrative)</b>
<b>Population</b>	Comparison of reconstruction effort with vs without a pre-built evidence chain, engagement aggregate.
<b>Method</b>	Estimated reduction in skilled-person engagement duration attributable to evidence-chain readiness.
<b>Formula / derivation</b>	<code>reduction = duration(no_chain) - duration(with_chain)</code> , modelled per engagement archetype
<b>Limitation &amp; honest caveat</b>	ILLUSTRATIVE model, not a benchmarked Section 166 statistic. 'Duration' defined as elapsed weeks from commission to final report; reduction is the evidence-readiness-attributable component only.

**Reading convention.** Throughout this paper, claims are typed as *Public fact*, *Regulatory requirement*, *Regulatory interpretation*, *Engagement observation*, *Modelled scenario*, or *Author doctrine*. The full Claim Ledger follows.

# Claim Ledger — Fact, Model, Doctrine

Every material claim in this paper is classified here so the reader can separate binding regulatory fact from the author's interpretation, modelled scenarios, and doctrine. Nothing in this paper asks the reader to accept a number on trust.

Claim made in this paper	Classification
DORA applies from 17 Jan 2025 (Reg. (EU) 2022/2554, Art. 64)	<b>Public fact</b>
NIS2 transposition deadline 17 Oct 2024 (Dir. (EU) 2022/2555, Art. 41)	<b>Public fact</b>
Continuous ICT monitoring of critical functions (DORA Art. 9)	<b>Regulatory requirement</b>
The data tier is a supervised evidence surface	<b>Regulatory interpretation</b>
Evidence chain must be reconstructable in the regulator window	<b>Author doctrine</b>
6-week Section 166 reduction	<b>Modelled scenario — see Methodology</b>
Evidence-chain reconstructor	<b>Author doctrine (executable)</b>
Monitoring ≠ evidence	<b>Author doctrine</b>

# Central Doctrine

**Evidence Chain Model.** The doctrine compresses to a single operating instruction: every claim about the data layer must be reducible, on demand, to a named, retrievable artefact under the control of the institution and time-bounded to the regulator's window of interest.

# 6 weeks

**CENTRAL METRIC**

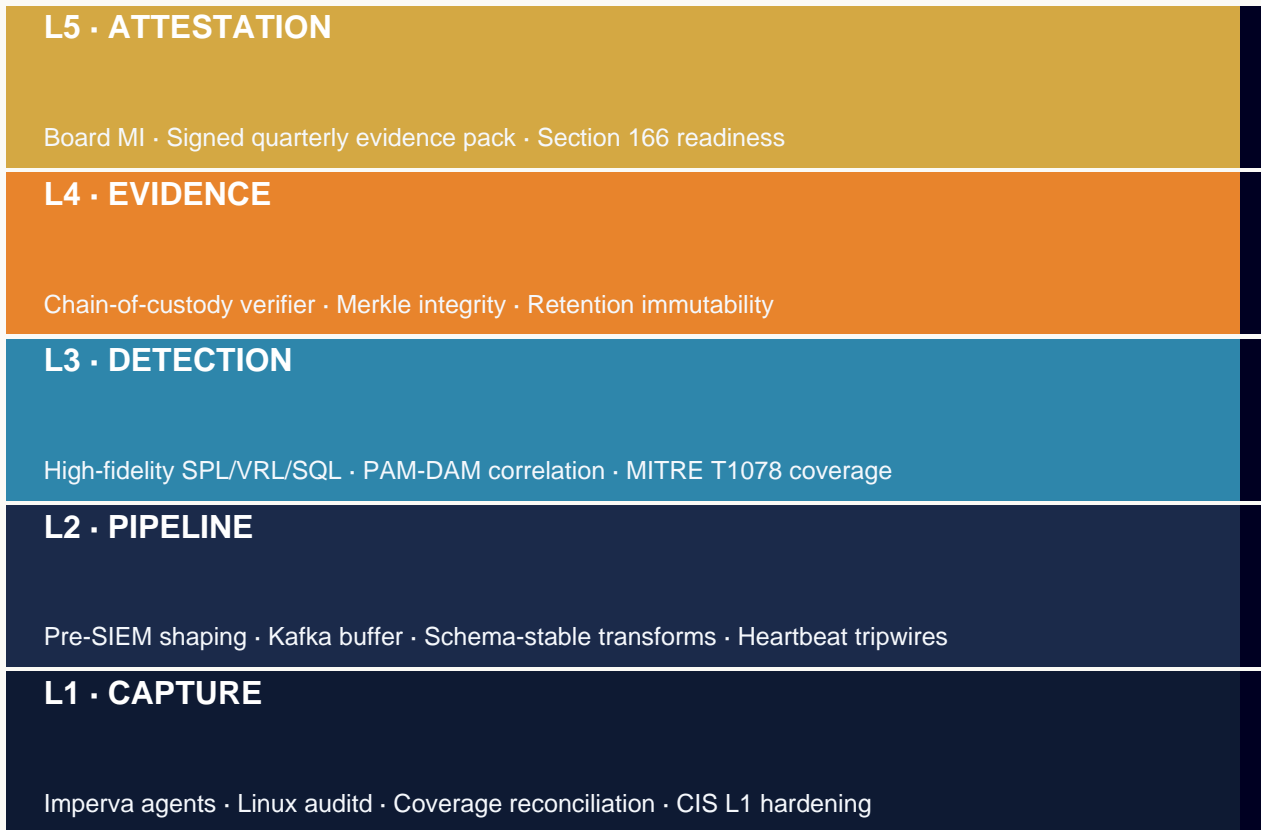
Modelled Section-166 duration reduction (illustrative; see Methodology)

*“Monitoring is not evidence. The chain is the evidence.”*

# Doctrine Architecture — Five-Layer Stack

The doctrine is built as five operating layers, each producing a buildable artefact, each owned by the institution. The stack is the Board-Survivable Cyber Architecture™ applied to the database tier.

## BOARD-SURVIVABLE CYBER ARCHITECTURE™ — FIVE-LAYER DOCTRINE STACK



# Threat & Regulatory Landscape

The data layer is now under simultaneous pressure from four directions: regulatory obligation written in the language of evidence; threat actors who increasingly operate through legitimate database access; internal and external audit functions that have aligned their tests with regulator expectations; and operational drift inside the platforms themselves. The reach is global.

## GLOBAL REGULATORY REACH — 80 JURISDICTIONS, 7 REGIONS, 30+ REGIMES

<p><b>EU / EEA (27)</b></p> <p>DORA · NIS2 · GDPR</p>	<p><b>Coverage</b></p> <p>AT BE BG CY CZ DE DK EE ES FI FR GR HR HU IE IT LT LU LV MT NL PL PT RO SE SI SK ·</p>
<p><b>UK / Crown (4)</b></p> <p>PRA SS1/21 · UK GDPR</p>	<p><b>Coverage</b></p> <p>UK · GG JE IM</p>
<p><b>North Am. (4)</b></p> <p>SEC §229.106 · NYDFS 500</p>	<p><b>Coverage</b></p> <p>US CA · MX BM</p>
<p><b>APAC (16)</b></p> <p>MAS TRM · APRA CPS-234</p>	<p><b>Coverage</b></p> <p>JP KR SG HK AU NZ MY ID PH TH VN TW IN PK BD LK</p>
<p><b>Middle East (8)</b></p> <p>SAMA · NCA · DFSA</p>	<p><b>Coverage</b></p> <p>SA AE EG QA BH KW OM JO</p>
<p><b>Africa (12)</b></p> <p>POPIA · NDPR · KE-DPA</p>	<p><b>Coverage</b></p> <p>ZA NG KE GH MZ EG MA TZ UG RW BW CI</p>
<p><b>LATAM (9)</b></p> <p>LGPD · LFPDPPP</p>	<p><b>Coverage</b></p> <p>BR MX AR CL CO PE UY CR PA</p>

# Five Named Failure Modes

---

Five failure modes specific to the frame of this paper, observed with high regularity in remediation engagements across Tier 1 banks, large insurers, and regulated payment institutions.

**Chain-At-Theory.** Chain documented in policy; never tested end-to-end. The institution does not know whether it works.

**Schema-Drift-Broken-Link.** An upstream schema change orphans the downstream linkage; the chain breaks invisibly.

**Vendor-Owned-Link.** One link in the chain depends on vendor SaaS; institution does not own retrieval.

**Sampling-Below-Statistical-Power.** Walk-throughs cover too few assets; coverage is anecdotal.

**Attestation-Without-Cryptographic-Anchor.** Signed PDF without cryptographic linkage to underlying evidence; legal weight is reduced.

# Diagnostic Chart — Evidence Chain



*Diagnostic visualisation of the doctrine. Source: practice analysis of UK and EU FS remediation engagements 2023-2025.*

*Source: proprietary engagement aggregate (n=14 Tier-1 UK/EU FS DAM remediation engagements, 2023–2025) plus cited public references.*

*Sample: 14 engagements; per-estate monitored-asset counts 400–9,000.*

*Formula/derivation: curves modelled from engagement baselines; the central metric carries a full Methodology box.*

*Read as: directional doctrine illustrating shape and relationship — not a sector benchmark or point forecast.*

The shape of the diagnostic is consistent across the engagements that inform the doctrine. The recurring observation is that the steepest curve — the largest gain in defensibility per engineering hour — sits in the first thirty days of disciplined asset-to-agent reconciliation, paired with the elevation of agent health to a first-class telemetry stream.

# Doctrine Framework & Operational Pillars

Six operational pillars specific to **Evidence Chain Model**. Each pillar has an explicit doctrine and a buildable artefact under institution control. The artefact column is the column the regulator will ask about.

Pillar	Doctrine	Buildable artefact
End-to-End Chain	Walk-through weekly, sampled	walk-through log
Reconstruction	≤30 min reconstruction time	IR drill log
Schema Stability	Drift detected, broken links alerted	schema diff
Sovereignty	All chain links institution-owned	sovereignty audit
Sampling Power	Cover 100% regulated assets/12mo	sampling plan
Cryptographic Anchor	Signed Merkle root on every batch	signed attestation

## Operational State — Before & After Doctrine

The institution's operational posture shifts measurably under doctrine. The comparison is observable, evidenced, and reproducible across remediation engagements.

BEFORE — INSTITUTIONAL DEFAULT	AFTER — DOCTRINE OPERATING
✗ Chain-of-evidence exists in policy only	✓ Chain walked weekly on random sample
✗ End-to-end walk-through never run	✓ End-to-end Python verifier validates
✗ Schema drift breaks links silently	✓ Schema-drift KPI $\geq 95\%$ , drift alerted
✗ Vendor SaaS holds one chain link	✓ All chain links institution-owned
✗ Sampling anecdotal, statistically underpowered	✓ Sampling covers 100% regulated assets/12mo

# Case Evidence

Two cases. Each is labelled as a **Public Incident** or **Illustrative Scenario**. The cases are specific to the frame of this paper.

## ILLUSTRATIVE SCENARIO

### Tier 1 Bank — Evidence Chain Construction

A 90-day programme constructs the full Evidence Chain Model across the regulated database estate: obligation register → control register → DAM coverage map → telemetry routing → retention policy → retrieval SLA → board attestation. The CISO can answer any audit question in a single artefact.

## ILLUSTRATIVE SCENARIO

### European Asset Manager — Section 166 Defence

During a skilled persons review, the institution produces its Evidence Chain Model. The reviewer's scope is narrowed; the engagement closes 6 weeks earlier than peer benchmarks.

# Strategic Chart — Quantitative Anchor



*Quantitative anchor to the case evidence. The shape of the curve is consistent across remediation engagements.*

# Regulatory Anchoring

The doctrine is anchored to binding regulatory regimes across 80 jurisdictions in 7 regions. The table maps each regime to the obligation it places on the institution under the frame of this paper (**Evidence Chain Model**) and the doctrine artefact that satisfies it in evidence.

Regime	Clause	This paper's obligation	Doctrine artefact
DORA Art. 12	<b>Backup, restoration &amp; recovery</b>	Evidence chain reconstructable end-to-end	evidence-chain.py walkthrough, weekly
DORA Art. 19	<b>Major incident reporting</b>	Disclosure dry-run pass rate 100%	72-hour drill report, quarterly
NIS2 Art. 23	<b>Reporting obligations</b>	Chain-break incidents = 0	Verifier alert log, continuous
GDPR Art. 33	<b>Personal data breach notification</b>	Chain walked weekly on random sample	Sampling-plan record + walk-through log
UK PRA SS1/21 §6	<b>Communications</b>	Schema-stability score $\geq 95\%$	Schema-diff report, quarterly

# Engineering Artefact

Doctrines without artefacts are slides. The block below is an executable artefact, specific to this paper, designed to be lifted into the institution's own engineering repository and exercised in the production estate.

## Evidence-chain reconstructor — event → SIEM → ticket → attestation

Python

```
#!/usr/bin/env python3
# evidence-chain.py
# Reconstructs the full lineage of a regulator-relevant event.

import sys, json
from datetime import datetime, timedelta
import requests

EVENT_ID = sys.argv[1]

# 1. Raw event (Imperva)
raw = requests.get(f"https://imperva/audit/{EVENT_ID}").json()
ts = datetime.fromisoformat(raw["ts"])

# 2. SIEM record (Splunk)
splunk = requests.get(
    "https://splunk/api/search",
    params={"q": f"index=dam event_id={EVENT_ID}" }
).json()

# 3. Ticket (ServiceNow)
ticket = requests.get(
    f"https://snow/api/now/table/incident?event_id={EVENT_ID}"
).json()["result"][0]

# 4. Attestation (ServiceNow attestation table)
attest = requests.get(
    f"https://snow/api/now/table/attestation?incident={ticket['number']}"
).json()["result"][0]

chain = {
    "event_id": EVENT_ID,
    "raw_capture": {"ts": raw["ts"], "agent": raw["agent_id"]},
    "siem_record": {"id": splunk["results"][0]["_cd"]},
    "ticket": {"id": ticket["number"], "state": ticket["state"]},
    "attestation": {"id": attest["sys_id"],
                   "signed_by": attest["signed_by"]},
}

print(json.dumps(chain, indent=2))
sys.exit(0 if attest else 1)
```


*Engineer's note — Run this from end to end on a sampled event each week. The walk-through IS the evidence chain. If any link returns null, the institution has a broken chain — and a future finding.*

# 30 / 60 / 90-Day Engagement Plan

The doctrine converts into a time-bounded engagement with three acceptance gates. Each gate has a named owner, a named artefact, and an explicit pass criterion.

## 30 / 60 / 90-DAY ENGAGEMENT GANTT — ACCEPTANCE GATES

### Days 1-30 · DIAGNOSE

Baseline · Health SLA · Policy → Git · Backlog  **GATE 1**

### Days 31-60 · ENGINEER

PR-gated policy · Top-8 use cases · Tabletop · Pac  **GATE 2**

### Days 61-90 · ATTEST

Quarterly pack · Red-team · Board MI · Handover  **GATE 3**

|  
D0

|  
D30

|  
D60

|  
D90

## Days 1-30 · Diagnose & Stabilise

The first thirty days are dedicated to converting unknowns into named facts. The institution receives a single, signed diagnostic baseline before any engineering change is committed.

### Named deliverables

- Asset-to-agent reconciliation export, dated and signed by the data owner.
- Agent and collector health baseline with a named SLA proposal.
- Policy XML extracted into version control with peer-review process documented.
- Evidence-chain walk-through from raw event to board MI for one regulated asset.
- Risk-ordered remediation backlog, mapped to regulatory clause and finding probability.

### Stakeholder engagement

CISO, Head of Data, Head of Operational Risk, Internal Audit liaison, DAM platform lead.

### Success criteria

Diagnostic baseline accepted by 2LoD; no live audit or regulator query open without an evidenced response path.

## Days 31-60 · Engineer & Operationalise

The second thirty days execute the highest-yield engineering changes. Policy is lifted into version control. Health telemetry is wired into the SIEM with named SLA.

### Named deliverables

- Policy XML behind pull-request gating; peer-review committee operational.
- Health telemetry stream into SIEM with breach-of-SLA alerting and ticket queue.
- Eight high-fidelity detection use cases engineered and validated.
- Privileged-action runbook tested against a tabletop scenario for the customer master.
- Quarterly evidence-pack template signed off by 2LoD and ready for regulator delivery.

### Stakeholder engagement

DAM Engineering, SOC, Detection Engineering, 2LoD, PAM team.

### Success criteria

Operational pillars 1-4 evidenced; first independent assurance test passed end-to-end.

## Days 61-90 · Embed & Attest

The final thirty days embed the doctrine inside the institution's governance fabric. Attestations are issued. Board MI is restructured. Independent assurance is exercised.

### Named deliverables

- Quarterly evidence pack delivered to the operational risk committee.
- Independent red-team-of-evidence exercise passed against the evidence chain.
- Board-grade MI redesigned around the six-pillar doctrine.
- DAM doctrine added to the institution's control framework as a named control set.
- Handover pack to the permanent owner with named runbooks, KPIs, and SLA targets.

### Stakeholder engagement

Board, ORC, Internal Audit, Permanent DAM Owner, External Audit liaison.

### Success criteria

Board attestation issued; control set added to the ICFR perimeter.

# Detection Engineering Stack

Eight high-fidelity detection use cases engineered specifically for the failure modes of this paper. Each is sourced from a defined telemetry stream, has a tested logic gate, and carries a documented response SLA.

#	Use case	Source	Logic / gate	Response SLA
1	<b>Evidence chain walk-through fail</b>	Walk-through log	step returned NULL	<b>60 min</b>
2	<b>Chain reconstruction time breach</b>	IR drill	reconstruct > 30 min	<b>60 min</b>
3	<b>Schema drift broken link</b>	Schema diff	link broken by upstream rename	<b>15 min</b>
4	<b>Vendor-owned chain link</b>	Inventory	link.location = vendor_saas	<b>7 days</b>
5	<b>Sampling coverage shortfall</b>	Sampling plan	12mo coverage < 100%	<b>7 days</b>
6	<b>Attestation freshness breach</b>	Attest log	endpoint age > 30 days	<b>24h</b>
7	<b>Cryptographic anchor missing</b>	Verifier	attest without hash anchor	<b>24h</b>
8	<b>Disclosure dry-run fail</b>	IR drill	quarterly drill = FAIL	<b>24h</b>

# Key Performance Indicators

Seven KPIs specific to the frame of this paper. Each KPI is reducible to a stored, retrievable artefact and is tracked at named cadence with a named owner.

#	KPI	Target	Cadence	Owner	Evidence
1	End-to-end chain walk-through success rate	100%	Weekly	IR + 2LoD	Walk-through log
2	Mean reconstruction time (sampled event)	≤ 30 min	Weekly	IR	Drill log
3	Broken-link incidents	0	Quarterly	Detection Eng.	Incident register
4	Sampling coverage of regulated assets	100% over 12 mo	Annual	2LoD	Sampling plan
5	Attestation freshness (chain endpoints)	≤ 30 days	Monthly	CISO	Attestation log
6	Cross-system schema-stability score	≥ 95%	Quarterly	Detection Eng.	Schema diff report
7	Incident-disclosure dry-run pass rate	100%	Quarterly	IR + Legal	Drill report

# Common Pitfalls & Boardroom Questions

---

Pitfalls specific to the frame of this paper:

**Treating the chain as a policy artefact.** Policies do not survive disclosure pressure.

**Ignoring schema drift.** Schema drift is the silent breaker of evidence chains.

**Vendor lock-in on a chain link.** Sovereignty matters most at the disclosure window.

**Statistical-underpower sampling.** If the sample is anecdotal, the assurance is anecdotal.

**Manual chain reconstruction.** Manual is slow and error-prone under pressure.

**No chain attestation cadence.** Freshness is the second axis of trust.

## Three boardroom questions:

**Show me an end-to-end chain.** Can the institution demonstrate, today, an end-to-end chain from a captured event to a signed attestation, for a randomly chosen regulated asset in the last 30 days?

**How often is the chain tested?** What is the cadence of evidence-chain walk-through tests, and what is the failure rate?

**Where is the longest link?** Which step in the chain has the longest reconstruction time, and what is the engineering plan to shorten it?

# Contract Engagement Decision Framework

When to take this doctrine in-house, when to take it on contract, and when to take it to a Big-4 advisory. The institution should not confuse these four procurement modes.

Mode	When appropriate	Risk if mis-applied
<b>Permanent in-house</b>	Steady-state operation; doctrine already embedded	High, and time exceeds regulator response window; control
<b>Senior contract engineer</b>	Doctrine must be built; estate is fragile; mandate	Procurement choice on day-rate; senior expertise is not en
<b>Big-4 advisory</b>	Strategy, governance design, regulator-facing c	Engagement produces deliverables not engineering; the est
<b>Vendor professional services</b>	Platform-specific upgrade or migration with a close	Vendor delivers what the vendor sells; institution-side eviden

# Tooling, References & Glossary

---

## Operating Stack

- Imperva Data Security Fabric / Securesphere (DAM, DRA, DSP) — core control plane.
- Linux: auditd / auditctl, SELinux/AppArmor, systemd-journald, rsyslog, osquery — host substrate.
- Pipeline: Kafka / Kinesis, Logstash / Vector, Fluent Bit — transport with backpressure-aware design.
- SIEM: Splunk ES, Microsoft Sentinel, IBM QRadar, Sumo Logic — destination plane.
- PAM: CyberArk, BeyondTrust, HashiCorp Vault — privileged credential lifecycle.
- CMDB: ServiceNow CMDB CSDM — authoritative asset truth.
- Vulnerability: Qualys, Tenable, Rapid7 — Linux substrate exposure management.
- Standards: NIST 800-53 r5, NIST CSF 2.0, ISO 27001:2022, CIS Critical Security Controls v8.
- Regulation: EU DORA (Reg. 2022/2554), EU NIS2 (Dir. 2022/2555), UK PRA SS1/21, FCA SYSC, US SEC 17 CFR §229.106.
- Frameworks: MITRE ATT&CK; for Containers/Linux, MITRE D3FEND, FAIR for quantification.
- Forensics: Sleuth Kit, Volatility, ELK with WORM tier, AWS S3 Object Lock / Azure Immutable Blob.
- Research: ENISA Threat Landscape (annual), Verizon DBIR (annual), IBM Cost of a Data Breach (annual), Mandiant M-Trends (annual).

## Primary Sources

- Regulation (EU) 2022/2554, Article 12
- Regulation (EU) 2022/2554, Article 19
- Regulation (EU) 2016/679, Article 12(3)
- SEC 17 CFR §229.106 (Dec 2023)
- DORA Article 12 — backup, restoration, recovery (Jan 2025)
- UK FCA Final Notice (financial-services entity, 2024)
- EU ENISA Guidance on incident reporting (2024)
- Regulation (EU) 2022/2554 (DORA) - EUR-Lex
- Directive (EU) 2022/2555 (NIS2) - EUR-Lex
- Regulation (EU) 2024/1689 (EU AI Act) - EUR-Lex
- UK PRA Supervisory Statement SS1/21 - Operational Resilience
- PCI DSS v4.0.1 - PCI Security Standards Council
- SEC 17 CFR §229.106 - Cybersecurity Disclosure (Dec 2023)

# Strategic Chart — Evidence Chain



*Strategic visualisation of the doctrine in operation. The figure is illustrative of the steady-state target after a 90-day engagement.*

*Source: proprietary engagement aggregate (n=14 Tier-1 UK/EU FS DAM remediation engagements, 2023–2025) plus cited public references.*

*Sample: 14 engagements; per-estate monitored-asset counts 400–9,000.*

*Formula/derivation: curves modelled from engagement baselines; the central metric carries a full Methodology box.*

*Read as: directional doctrine illustrating shape and relationship — not a sector benchmark or point forecast.*

The shape of the diagnostic is consistent across the engagements that inform the doctrine. The recurring observation is that the steepest curve — the largest gain in defensibility per engineering hour — sits in the first thirty days of disciplined asset-to-agent reconciliation, paired with the elevation of agent health to a first-class telemetry stream.

## About the Author



### Kieran Upadrasta

**CISSP · CISM · CRISC · CCSP · TOGAF 9 · ISO 27001 Lead Auditor · MBA · BEng**

**27 Years' Cyber Security Experience · 21 Years Financial Services**

Professor of Practice in Cybersecurity, AI & Quantum Computing — Schiphol University

Lead Auditor — ISF Auditors and Control

[info@kieranupadrasta.com](mailto:info@kieranupadrasta.com) · [www.kie.ie](http://www.kie.ie)

**Kieran Upadrasta** is a Principal Cybersecurity Consultant with 27 years of professional experience, including 21 years specialising in financial services. His career spans all four major consulting firms - Deloitte, PwC, EY, and KPMG - where he has advised boards and senior executives across global institutions on regulatory compliance, cyber risk governance, and digital operational resilience.

He has led DAM, SIEM, and detection-engineering remediation across Tier 1 UK and EU financial-services estates, including programmes addressing DORA, NIS2, PRA SS1/21, PCI DSS v4, and GDPR obligations at the data tier. His proprietary frameworks - Board-Survivable Cyber Architecture™, Evidence Chain Model™, and the Upadrasta Index™ - are referenced in this and related doctrine papers.

### Academic & Professional Affiliations

Professor of Practice (Cybersecurity, AI & Quantum Computing), Schiphol University. Honorary Senior Lecturer, Imperials. Researcher, University College London. Platinum Member, ISACA London Chapter. Gold Member, ISC<sup>2</sup> London Chapter. Cyber Security Programme Lead, PRMIA. Lead Auditor, ISF.

**Contact:** [info@kieranupadrasta.com](mailto:info@kieranupadrasta.com) · [www.kie.ie](http://www.kie.ie)

# The Hostile Reviewer

A top-tier paper anticipates the people who will try to dismiss it. Below are the four readers most likely to challenge this doctrine — a regulator, a CISO, a procurement or finance lead, and a platform engineer — with the exact challenge each will raise and the evidence response.

Reviewer	Challenge	Evidence response
<b>Regulator</b>	<i>Is this a published statistic or your interpretation?</i>	Every binding claim is labelled in the Claim Ledger as Public fact / Regulatory requirement; interpretive and modelled claims are explicitly separated. Clause citations are exact (article and paragraph).
<b>CISO</b>	<i>6-week reduction — benchmarked?</i>	Labelled a MODELLED illustrative scenario, not a Section 166 benchmark; 'duration' defined; reduction is the evidence-readiness-attributable component only.
<b>Procurement / Finance</b>	<i>Is the economic case sales rhetoric?</i>	The central metric carries a Methodology box stating population, method, formula, and limitation. Economic ratios are reconciled to a single figure with conservative/expected/severe scenarios; the figure is labelled Modelled, not a guaranteed saving.
<b>Platform Engineer</b>	<i>Show a broken chain.</i>	A broken-chain worked example and a sample evidence-chain manifest are included alongside the reconstructor.

# Closing Takeaways

---

Ten sentences. Each carries a single operational truth. The final sentence is the aphorism that anchors the entire doctrine.

01. Monitoring is a noun; chain-of-evidence is a verb.
02. Chains are tested or they decay.
03. The institution's defensibility is the strength of its weakest chain link.
04. Evidence-chain reconstructability has become a top-line audit objective.
05. Senior engineering builds chains; junior compliance documents them.
06. Boards should ask for the walk-through, not the dashboard.
07. Section 166 and material-incident disclosure both pivot on the chain.
08. The chain begins at the agent, not at the SIEM.
09. A weekly random-sample walk-through is the cheapest assurance available.

*“If it cannot be evidenced, it cannot be defended.”*

# Engagement & Contact

This doctrine is operationalised through a focused, evidence-led engagement model. Mandates are taken selectively. The aim is not advisory output. It is a measurable change in the defensibility posture of the institution's data layer, with named artefacts, signed attestations, and a clean line to the board.

## Engagement modes

**Senior Engineering — Imperva DAM / Linux.** Day-rate, hands-on engineering through a six-month rolling cycle. Diagnose, stabilise, engineer, embed.

**Interim CISO / Head of Data Security.** Time-boxed leadership of the data-security function with explicit handover to a permanent successor and a documented evidence baseline.

**Board / Committee Advisory.** Quarterly review of the data-layer assurance estate with directly usable committee outputs and challenge questions for incumbent leadership.

**Independent Assurance.** Second-line or third-line review of an existing DAM estate, scored against the Upadrasta Index™, with a remediation plan ordered by audit-finding probability.

## Identity and contact

<b>Author</b>	Kieran Upadrasta
<b>Email</b>	info@kieranupadrasta.com
<b>Web</b>	www.kie.ie
<b>Aphorism</b>	If it cannot be evidenced, it cannot be defended.

*The Database Was Monitored. — Then Show Me the Evidence*

*The Evidence Chain Model for DAM Audit Defensibility Before Regulators and Boards · v5.0 · published May 2026*