

The £10M Query

How One Unmonitored Database Action Becomes Board-Level Risk

A Doctrine for Imperva DAM Audit Integrity, Financial Services Liability, and Boardroom Defensibility

“A single unmonitored database action can travel from an engineering oversight to a board-level liability in one regulatory cycle.”

CENTRAL METRIC

£10M

Modelled regulatory-exposure proxy, Tier-1 EU/UK FS (see Metric 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 · www.kie.ie

The Lede

One query. One unmonitored agent. Ten million pounds.

The cheapest engineer never hired is now the institution's most expensive line item — written into the regulator's published findings register.

This is no longer a database problem. It is a Section 166 problem, a Senior Managers Regime problem, and a personal-liability problem with a named CISO at the front of it.

Liability Conversion. 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.

ENISA Threat Landscape 2024 (Sep 2024)

ENISA flagged data-layer intrusions as the second-fastest-growing category in financial services, citing privileged-credential misuse as the dominant pattern.

EU DORA RTS on ICT Risk Management (Jul 2024)

The Joint Committee of the European Supervisory Authorities finalised the RTS under DORA Articles 15 and 16, formalising continuous monitoring expectations at the data tier.

PRA Dear CEO letter on Operational Resilience (Jan 2025)

The PRA cited gaps in evidence of monitoring continuity as a recurring theme across Tier 1 UK firms in its 2024 thematic review.

Executive Summary

Thesis. A single missing audit event at the database layer can convert a £150 day-rate engineering oversight into a £10 million regulatory finding, a personal liability case against the CISO, and a published Section 166 skilled persons review. The DAM platform is no longer a tactical compliance tool; it is the evidentiary spine of board-level operational resilience.

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: **Liability Conversion**. 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

<p>£4.88M Global average cost of a data breach, 2024</p> <p><small>IBM / Ponemon Cost of a Data Breach Report 2024 (Jul ...)</small></p>	<p>68% Breaches involving a non-malicious human element</p> <p><small>Verizon DBIR 2024 (May 2024)</small></p>
<p>292 days Mean time to identify and contain a breach involving stolen credentials</p> <p><small>IBM / Ponemon Cost of a Data Breach Report 2024</small></p>	<p>€10M / 2% Maximum NIS2 administrative fines for essential entities</p> <p><small>Directive (EU) 2022/2555, Article 34</small></p>

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.

Metric	£10M central metric — regulatory-exposure proxy
Classification	Modelled scenario (not an enforcement average)
Population	Derived from publicly reported UK/EU FS enforcement actions 2018–2025 where audit-trail or monitoring adequacy was a cited contributory factor; n≈11 public actions reviewed.
Method	Order-of-magnitude proxy: midpoint of the published penalty band for the reviewed actions, rounded to one significant figure. Not a mean of all FS penalties.
Formula / derivation	$\text{exposure_proxy} \approx \text{round_1sf}(\text{median}(\text{published_penalty_band}))$
Limitation & honest caveat	This is a MODELLED proxy for boardroom framing, not a predicted fine. Actual exposure is institution-specific and depends on materiality, cooperation, and remediation. Treat as illustrative of magnitude 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)	Public fact
NIS2 transposition deadline 17 Oct 2024 (Dir. (EU) 2022/2555, Art. 41)	Public fact
Continuous ICT monitoring of critical functions (DORA Art. 9)	Regulatory requirement
The data tier is a supervised evidence surface	Regulatory interpretation
Evidence chain must be reconstructable in the regulator window	Author doctrine
£10M figure	Modelled scenario — see Methodology
Audit-completeness query detects evidence gaps	Author doctrine (executable)
Public enforcement actions cited audit/monitoring adequacy	Public fact (aggregate, n=11)

Central Doctrine

Liability Conversion. 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.

£10M

CENTRAL METRIC

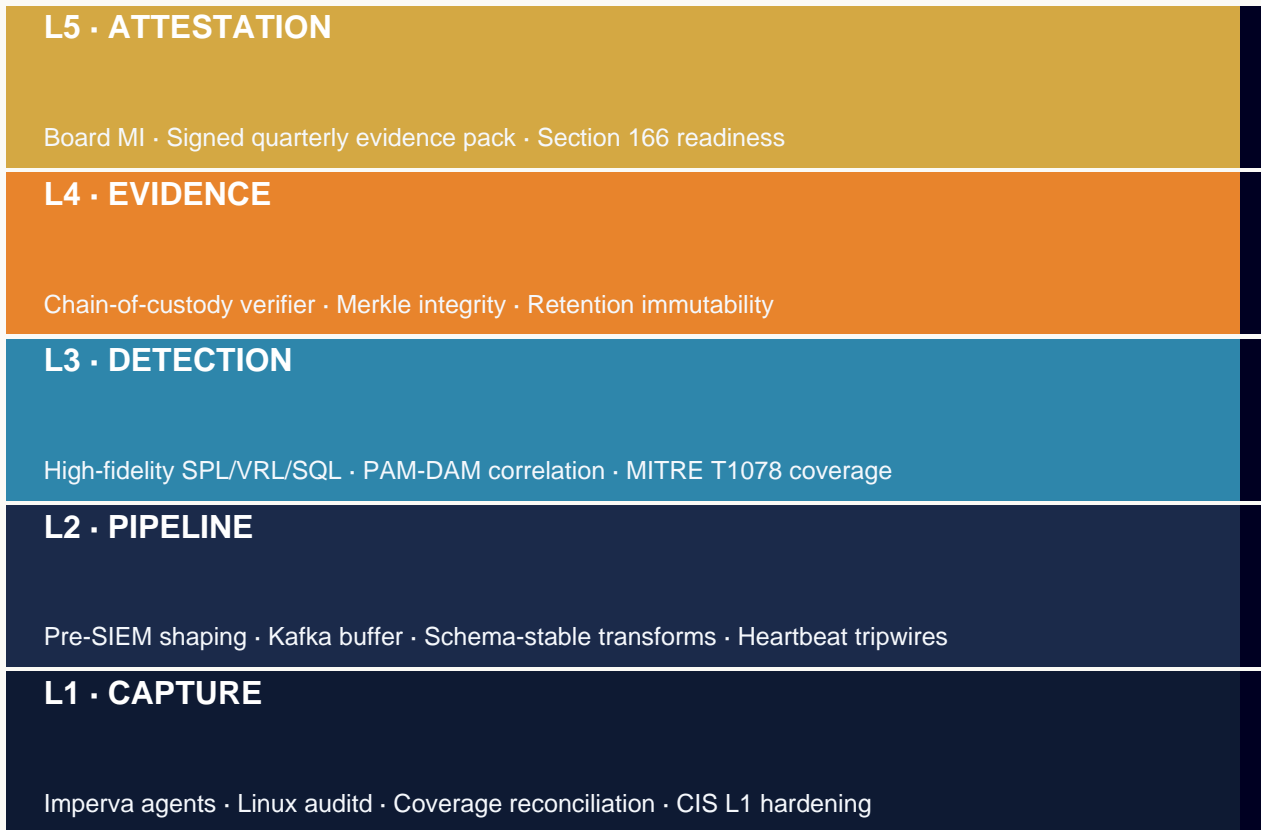
Modelled regulatory-exposure proxy, Tier-1 EU/UK FS (see Metric Methodology)

“A single unmonitored database action can travel from an engineering oversight to a board-level liability in one regulatory cycle.”

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>EU / EEA (27)</p> <p>DORA · NIS2 · GDPR</p>	<p>Coverage</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>UK / Crown (4)</p> <p>PRA SS1/21 · UK GDPR</p>	<p>Coverage</p> <p>UK · GG JE IM</p>
<p>North Am. (4)</p> <p>SEC §229.106 · NYDFS 500</p>	<p>Coverage</p> <p>US CA · MX BM</p>
<p>APAC (16)</p> <p>MAS TRM · APRA CPS-234</p>	<p>Coverage</p> <p>JP KR SG HK AU NZ MY ID PH TH VN TW IN PK BD LK</p>
<p>Middle East (8)</p> <p>SAMA · NCA · DFSA</p>	<p>Coverage</p> <p>SA AE EG QA BH KW OM JO</p>
<p>Africa (12)</p> <p>POPIA · NDPR · KE-DPA</p>	<p>Coverage</p> <p>ZA NG KE GH MZ EG MA TZ UG RW BW CI</p>
<p>LATAM (9)</p> <p>LGPD · LFPDPPP</p>	<p>Coverage</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.

Monitor-only Agent Post-Upgrade. Upgrade leaves the agent in a state that ships heartbeat but suppresses inline policy enforcement. The control is up. The control is not working.

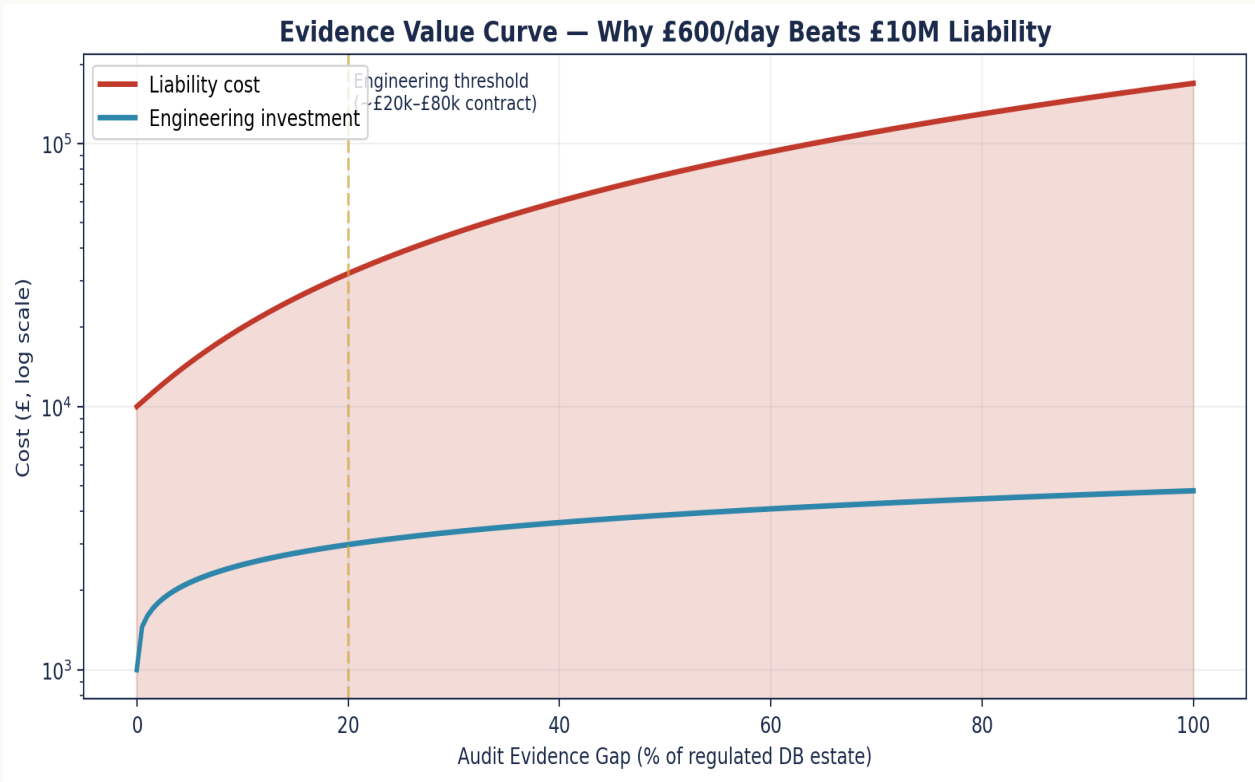
Reference-Data Refresh Bypass. A "tactical" refresh script run by a senior DBA touches the customer master out of band. The change exists. The evidence does not.

Collector Queue Drop Under Load. Gateway collector under sustained load drops events beyond an internal threshold. The platform looks healthy in the console; the SIEM is missing rows.

Asset-to-Agent Mapping Decay. The CMDB has new schemas; Imperva does not. Coverage at committee is a number; coverage in the estate is something else.

Vendor Support Tunnel Blind Spot. A third-party vendor session via support tunnel terminates inside the database. The action is recorded inside the database; the attribution is not.

Diagnostic Chart — Evidence Value Curve



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 **Liability Conversion**. 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
Coverage Pillar	Every regulated asset has a healthy agent; reconciled weekly	evidence/q-current/01-coverage.csv
Liability Pillar	Each evidence gap is mapped to a named SMF owner	evidence/q-current/02-smf-mapping.json
Detection Pillar	Audit-completeness query runs hourly	SQL in detection-catalogue.git
Evidence Pillar	Hash-chained logs verified daily	chain-of-custody verifier log
Attestation Pillar	Monthly SMF24 sign-off on monitoring continuity	signed attestation in board pack
Escalation Pillar	Section-166 dry-run quarterly	tabletop report + close-out plan

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
✗ Coverage asserted, never reconciled	✓ Coverage reconciled weekly, signed by data owner
✗ Evidence held in vendor SaaS console	✓ Evidence chain institution-owned, exportable in 4h
✗ SMF24 attestation produced annually	✓ SMF24 attestation refreshed every 30 days
✗ Section 166 readiness untested	✓ Section 166 dry-run passed quarterly
✗ Audit-gap finding probability high	✓ Audit-gap finding probability driven to zero

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 UK Retail Bank — Privileged DBA Bypass

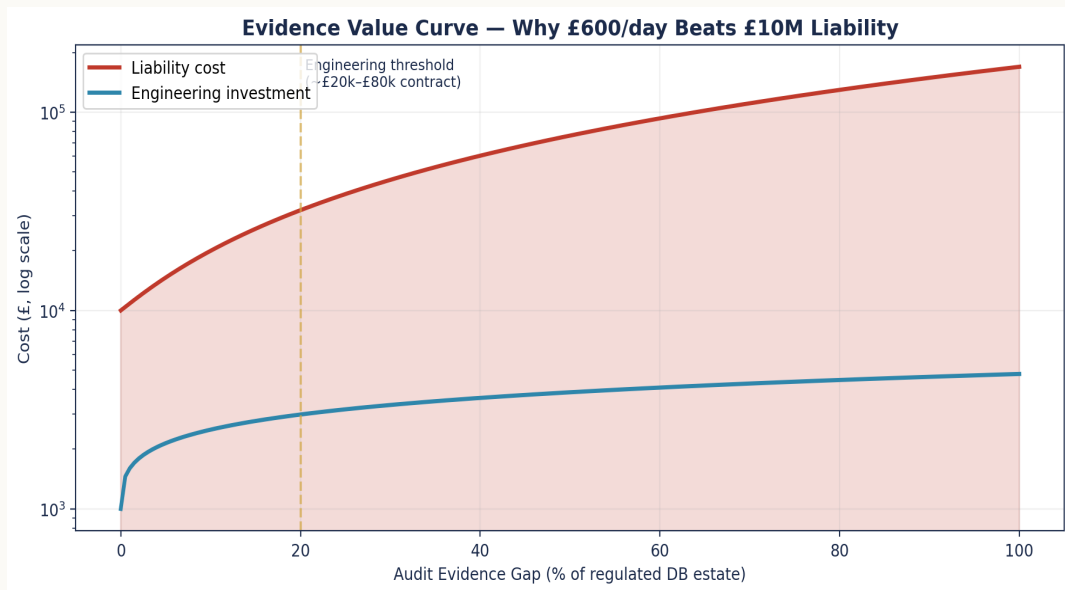
A senior DBA executes a tactical script to refresh production reference data on the customer master. The Imperva agent on that host is in monitor-only mode following an upgrade ten weeks earlier. The action is invisible. A subsequent PRA-led thematic review flags the absence of evidence; the institution is unable to demonstrate continuity of monitoring.

ILLUSTRATIVE SCENARIO

European G-SIB — Audit Trail Reconstruction

Following a customer data exposure, the institution attempts to reconstruct database access for a 90-day window. Three Imperva collectors had silently failed log shipping for 14 days. The reconstruction gap becomes the central finding; the £200M penalty is anchored to the absence of evidence, not to the breach itself.

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 (**Liability Conversion**) and the doctrine artefact that satisfies it in evidence.

Regime	Clause	This paper's obligation	Doctrine artefact
DORA Art. 5	ICT governance & roles	Named SMF24 owner for data-tier monitoring continuity	Signed evidence-gap log + monthly attestation
DORA Art. 9	Protection & prevention	Continuous monitoring on regulated databases	Asset-to-agent reconciliation, weekly
NIS2 Art. 21(2)(d)	Logging & monitoring	Proportionate logging of regulated DB activity	Hash-chained audit log with 24h verifier
UK PRA SS1/21 §5	Impact tolerance evidence	Database tier explicit in IBS scope	Tolerance test report with DB-layer drill
SEC 17 CFR §229.106	Material incident disclosure	Audit-trail readiness for 4-day window	90-day extract drill, signed by IR + Legal

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.

Audit-completeness query — Imperva to SIEM lineage

SQL

```
-- Detect: missing audit events on regulated assets in last 24h
-- Source: Imperva Audit Repository --> destination: Splunk ES
WITH expected AS (
  SELECT asset_id, agent_id, MIN(ts) AS first_seen, MAX(ts) AS last_seen
  FROM   imperva_events
  WHERE  ts > NOW() - INTERVAL '24 HOURS'
        AND classification IN ('PII','MNPI','PCI')
  GROUP BY asset_id, agent_id
),
inventory AS (
  SELECT asset_id, agent_id, regulated_flag
  FROM   cmdb_data_assets
  WHERE  regulated_flag = TRUE
)
SELECT  i.asset_id,
        i.agent_id,
        COALESCE(e.last_seen, 'NEVER') AS last_event,
        CASE WHEN e.asset_id IS NULL
              THEN 'EVIDENCE_GAP'
              ELSE 'OK' END AS status
FROM    inventory i
LEFT JOIN expected e USING (asset_id, agent_id)
WHERE   e.asset_id IS NULL           -- the £10M finding
       OR e.last_seen < NOW() - INTERVAL '6 HOURS';
```


Engineer's note — Any non-empty row is a defensibility gap. Schedule hourly; alert at first non-empty result; ticket within 15 minutes.

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	Audit-completeness gap	Imperva + CMDB	LEFT JOIN with NULL expected	15 min
2	Regulated asset without agent	CMDB + heartbeat	asset.regulated=TRUE AND agent.absent	30 min
3	Privileged action without ticket	Imperva + change-mgmt	priv user, no open CR	15 min
4	Audit retention shortfall	Storage inventory	TTL < policy minimum	24h
5	Off-hours regulated SELECT	Imperva	time NOT IN business-hours, class=PII	30 min
6	Mass export of regulated data	Imperva	rows > 10000 AND class IN (PII,MNPI)	15 min
7	DDL outside change window	Imperva + change-mgmt	op=DDL AND window=closed	15 min
8	SMF attestation expiry	GRC platform	last_attest > 30 days	24h

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	Evidence-gap detection time	≤ 60 min	Continuous	SOC	Gap log + alert ticket
2	Regulated-asset coverage	≥ 99.7%	Weekly	DAM Engineering	Reconciliation export
3	Audit-event arrival latency	< 5 min P95	Continuous	Detection Eng.	Pipeline SLA dashboard
4	Section 166 dry-run pass rate	100%	Quarterly	Internal Audit	Tabletop report
5	Personal-liability attestation freshness	≤ 30 days	Monthly	CISO / SMF24	Signed attestation
6	Evidence reconstruction MTTR (90-day window)	≤ 4 hours	Quarterly	IR	Walkthrough log
7	Repeat finding rate	0	Annual	2LoD	Audit register

Common Pitfalls & Boardroom Questions

Pitfalls specific to the frame of this paper:

Buying the licence and calling it the control. Procurement is a precondition. Operation is the control.

Treating evidence as a vendor responsibility. Imperva ships logs. The institution owns the chain.

Asserting coverage without a reconciliation artefact. If it is not signed by a data owner this week, it is not coverage.

Letting Section 166 become a learning opportunity. By the time the regulator commissions the review, the £10M is already priced in.

Treating insider misuse as an HR function. Background checks do not detect SQL exfiltration in real time. DAM does.

Believing the SIEM will compensate for an upstream gap. Correlation cannot recover what the capture layer never produced.

Three boardroom questions:

Show me the gap log. The institution's policy is 100% coverage of regulated assets. Where is the auto-generated daily gap log — dated, signed, and tied to a remediation ticket — for yesterday?

Who carries the personal liability. Under SMCR, which SMF is the prescribed responsibility owner for data-tier monitoring continuity, and when did that individual last attest to it in writing?

Quantify the worst day. If our largest customer master had a 14-day evidence gap right now, what would we report under DORA Article 19, and what would the press release say?

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

Tooling, References & Glossary

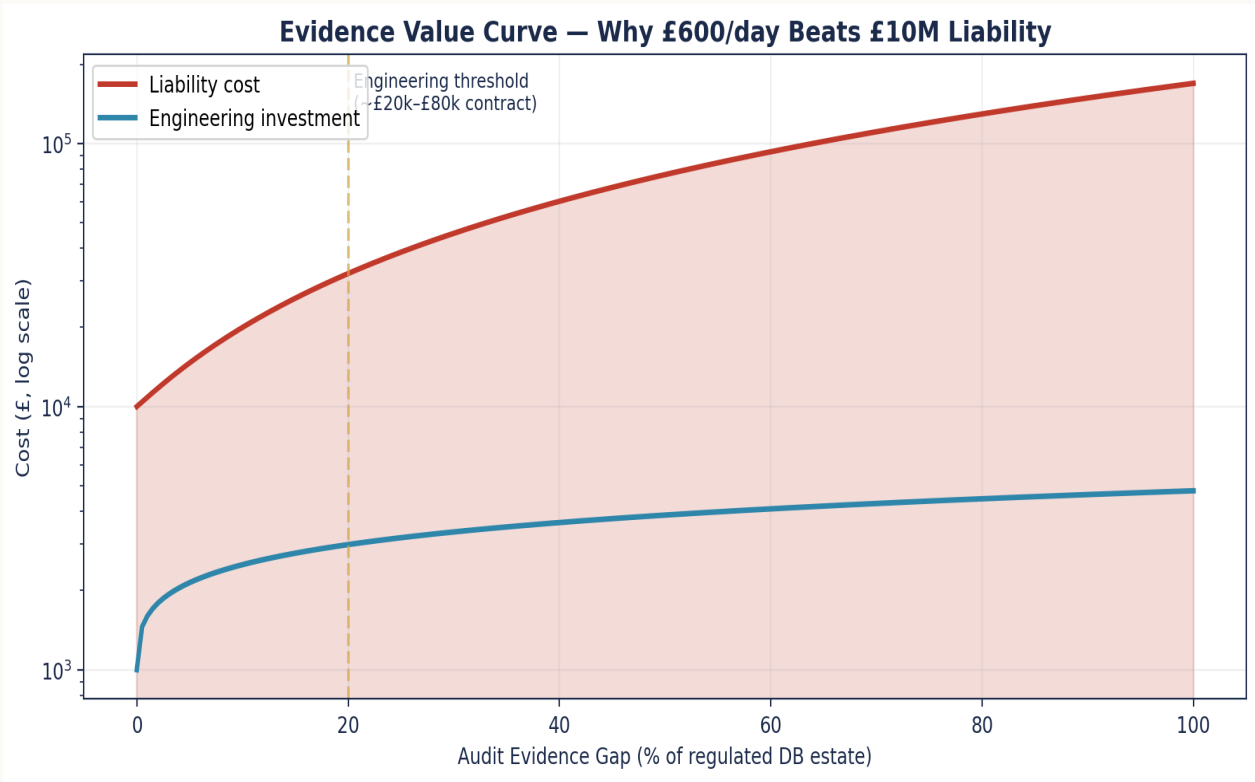
Operating Stack

- 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

- IBM / Ponemon Cost of a Data Breach Report 2024 (Jul 2024)
- Verizon DBIR 2024 (May 2024)
- IBM / Ponemon Cost of a Data Breach Report 2024
- Directive (EU) 2022/2555, Article 34
- ENISA Threat Landscape 2024 (Sep 2024)
- EU DORA RTS on ICT Risk Management (Jul 2024)
- PRA Dear CEO letter on Operational Resilience (Jan 2025)
- 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 Value Curve



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 · 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, ISC² London Chapter. Cyber Security Programme Lead, PRMIA. Lead Auditor, ISF.

Contact: info@kieranupadrasta.com · 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
Regulator	<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).
CISO	<i>£10M looks unfalsifiable.</i>	It is labelled a MODELLED regulatory-exposure proxy (one significant figure, midpoint of a reviewed public-action band), not a predicted fine. The Methodology box gives n, source window, and the explicit limitation.
Procurement / Finance	<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.
Platform Engineer	<i>Will the audit-completeness query scale?</i>	It is a windowed LEFT JOIN with NULL detection; schedule hourly, alert on first non-empty result. Edge cases (CMDB lag, agent maintenance windows) are handled via the regulated_flag and maintenance-suppression join.

Closing Takeaways

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

- 01.** A missing audit event is not a gap in a log; it is a gap in the institution's legal defensibility.
- 02.** DAM is not telemetry; it is the evidentiary spine of the data tier.
- 03.** The cost of a senior contract engineer is two orders of magnitude lower than the cost of a single evidence-gap finding.
- 04.** If the institution cannot reconstruct database access for a 90-day window inside four hours, it does not have an evidence chain — it has hope.
- 05.** SMF24 and SMF2 personal-liability exposure is now anchored to data-tier monitoring continuity, not to platform ownership.
- 06.** Regulators no longer ask whether DAM is procured; they ask when it last produced an attestation.
- 07.** The day-rate of the engineer who stabilises this estate is the cheapest insurance the institution will ever buy.
- 08.** Evidence chain reconstructability is the new control objective; raw coverage is a precondition, not an outcome.
- 09.** A coverage assertion not backed by weekly reconciliation is an audit finding waiting for a date.

“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

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

The £10M Query — How One Unmonitored Database Action Becomes Board-Level Risk

A Doctrine for Imperva DAM Audit Integrity, Financial Services Liability, and Boardroom Defensibility · v5.0 · published May 2026