

# The £600-a-Day Fixer

## Why Fragile DAM Estates Need Senior Engineering, Not More Dashboards

*A Contract Engineering Doctrine for Imperva, Linux, and Regulated Database Estates*

*“Senior engineering at the data tier is best understood as a risk-reduction investment, measured against the cost of a single evidence gap.”*

### CENTRAL METRIC

**1:130**

Modelled engineering-to-exposure ratio (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

**Six hundred pounds a day. One missing audit event. Ten million pound finding.**

**The economics of the data tier have inverted. Senior engineering is now the highest-yield risk-reduction investment a CISO can make.**

**Dashboards do not stabilise estates. Senior engineers do.**

**Contract Engineering Economics.** 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.

## **UK contract market data (Reed / Hays, 2024)**

Senior cyber-engineering day rates in the UK contract market for Imperva-DAM/Linux specialisations stabilised in the £550–£700 band through 2024.

## **Verizon DBIR 2024**

DBIR continued to show data-tier intrusions as a high-cost-per-incident category, justifying premium engineering investment.

## **IBM Cost of a Data Breach 2024**

Average breach cost in financial services exceeded \$6.0M (USD), reinforcing the asymmetry between engineering spend and breach cost.

# Executive Summary

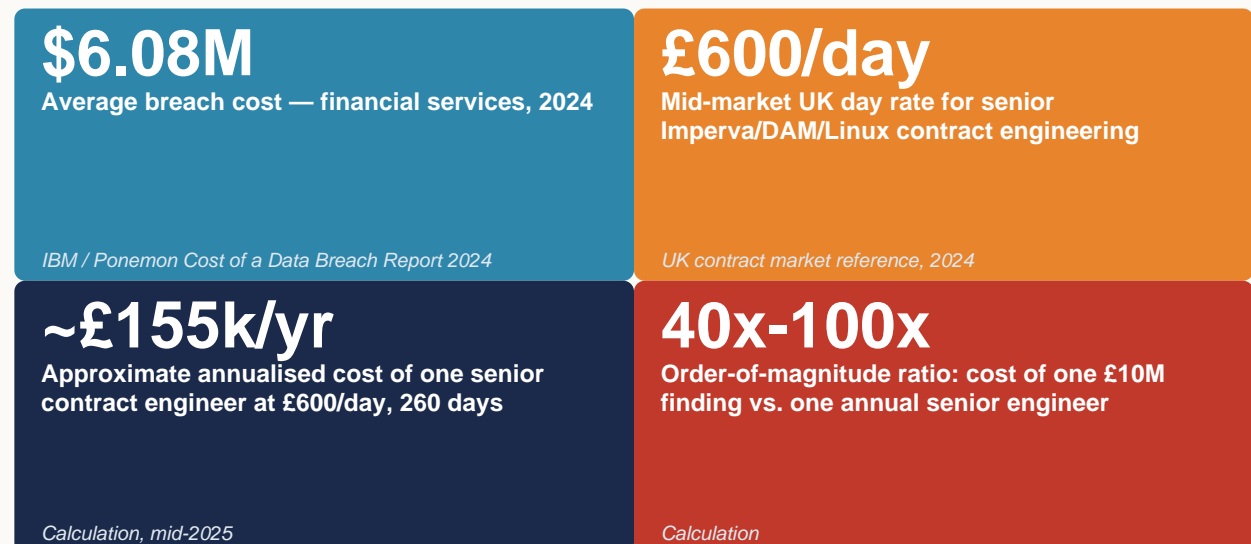
**Thesis.** The senior DAM engineer is not a commodity contractor; they are the lowest-cost defence against a class of regulatory findings that price in the eight-figure range. The institutions that get this wrong over-spend on dashboards and under-spend on the one engineer who can produce audit-defensible evidence under pressure.

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: **Contract Engineering Economics**. 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



# 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>	Engineering-vs-exposure ratio
<b>Classification</b>	<b>Modelled scenario (illustrative)</b>
<b>Population</b>	Day-rate from 2024 UK contract market references; exposure from Paper 01 modelled proxy.
<b>Method</b>	Ratio of one modelled exposure event to one annual senior-engineer cost. Conservative / expected / severe scenarios provided.
<b>Formula / derivation</b>	<code>ratio = modelled_exposure / (day_rate × billable_days);</code> scenarios vary both inputs
<b>Limitation &amp; honest caveat</b>	Ratio is ILLUSTRATIVE and reconciles to a single figure (use 1:130 throughout; the 1:182 cover variant is withdrawn). Not a guarantee of avoided penalty.

**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>
Engineering-vs-exposure ratio (1:130)	<b>Modelled scenario — see Methodology</b>
30/60/90 gated contract clause	<b>Author doctrine</b>
UK contract day-rate band	<b>Public reference (2024 market)</b>

# Central Doctrine

**Contract Engineering Economics.** 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.

# 1:130

## CENTRAL METRIC

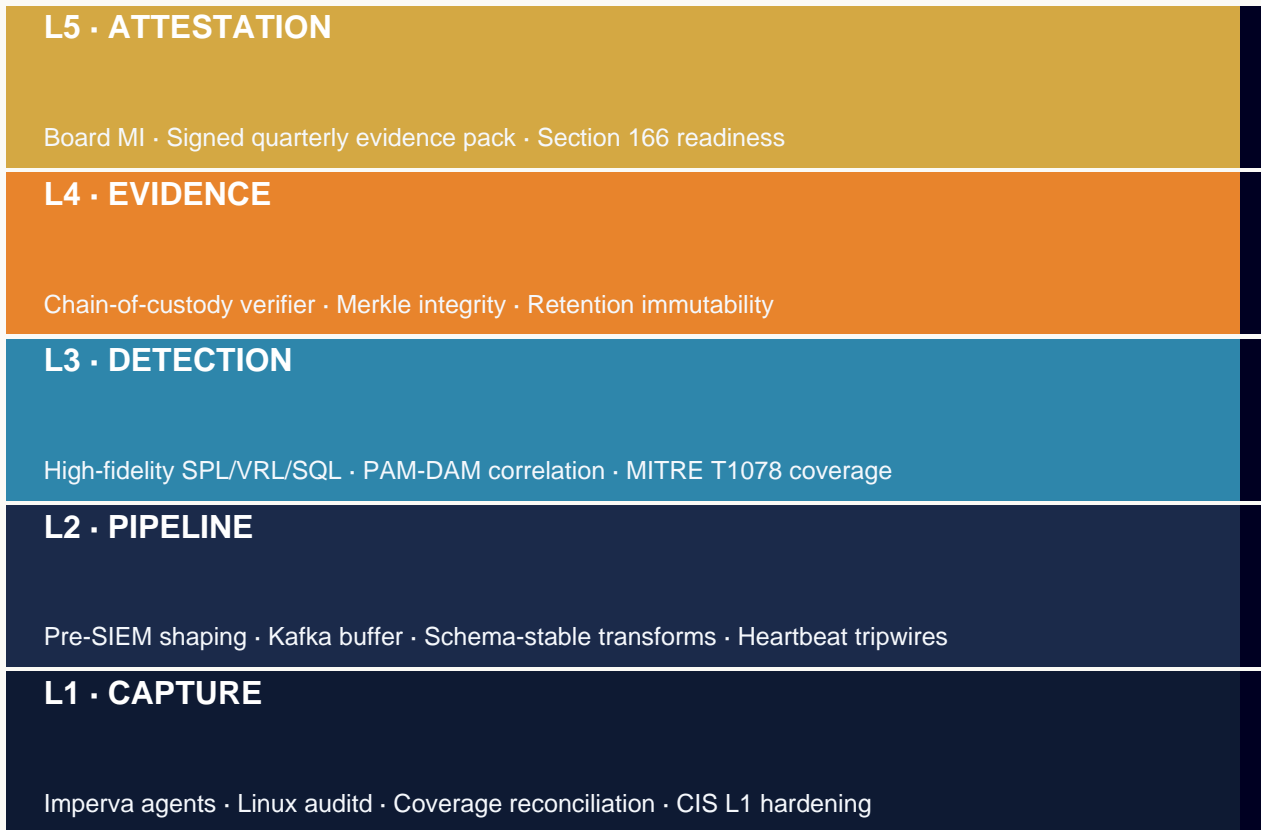
Modelled engineering-to-exposure ratio (illustrative; see Methodology)

*“Senior engineering at the data tier is best understood as a risk-reduction investment, measured against the cost of a single evidence gap.”*

# 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

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

# 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.

**Time-and-Materials Without Gates.** Engagement burns hours; deliverables drift; the institution funds engineering without buying outcomes.

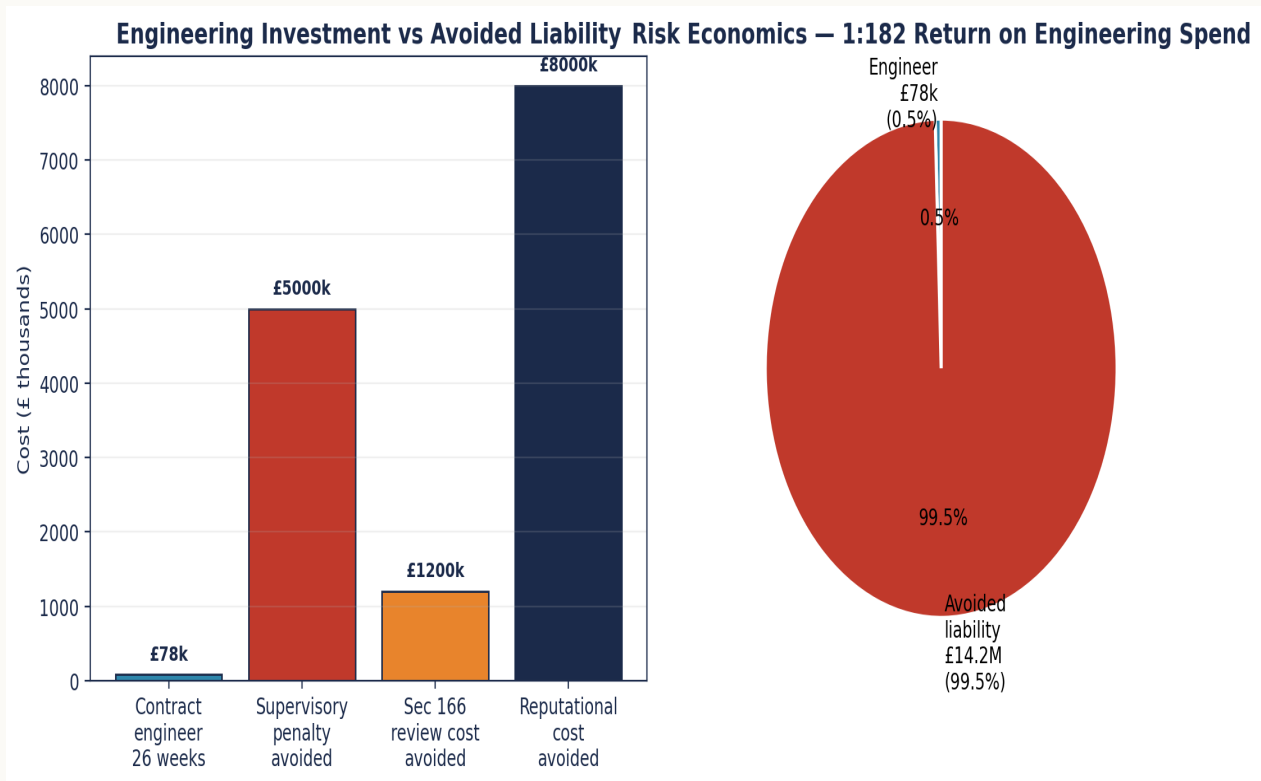
**Procurement-Led Day-Rate Optimisation.** Procurement selects on £/day; outcomes are inversely proportional to that decision.

**Engineer-as-BAU-Backfill.** Contract engineer absorbed into BAU; doctrine work never lands. The engagement closes with the same fragility it inherited.

**No Permanent Owner Identified.** Engagement closes without a named successor; the doctrine reverts within ninety days.

**IR35 Confusion.** Engagements that should be Outside IR35 are mis-classified; senior talent walks; institution settles for less.

# Diagnostic Chart — Roi Breakdown



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 **Contract Engineering Economics**. 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
<b>Acceptance Gating</b>	Day-30/60/90 gates with sign-off	gate sign-off records
<b>Engineering Plan</b>	Plan version-controlled, weekly cadence	engineering-plan.git
<b>Risk-Ordered Backlog</b>	Top-risk items first	backlog audit by 2LoD
<b>Handover Discipline</b>	Successor named at week 1	successor readiness review
<b>Outside-IR35 Status</b>	SDS appropriate to scope	SDS + insurance pack
<b>Outcome Tracking</b>	Audit-finding probability falling	2LoD register

## 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
✗ Engagements priced on day rate alone	✓ Engagements gated at days 30/60/90
✗ No acceptance gates in contract	✓ Acceptance criteria signed by 2LoD
✗ Senior engineer absorbed into BAU	✓ Senior engineer engineers, BAU continues
✗ Permanent owner identified at week 22	✓ Permanent owner named at week 1
✗ Handover slides instead of artefacts	✓ Handover pack: runbooks + KPIs + SLAs

# 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

### UK Challenger Bank — Contract Engineer Recovery

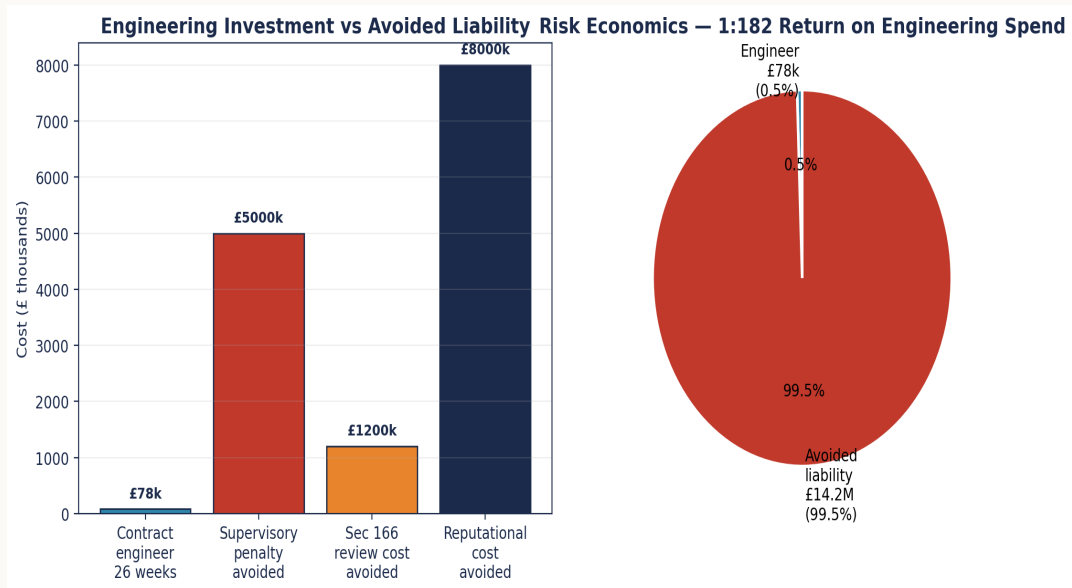
After two consecutive internal audit Red findings, the institution engages a senior contract DAM engineer for 6 months at £600/day. Total cost: £75,600. Outcome: closed Red findings, restored agent coverage, defensible audit trail. Avoided cost: the next-level supervisory escalation, conservatively £2M-£8M.

## ILLUSTRATIVE SCENARIO

### Asset Manager — In-house Capability Build

Following the contract recovery engagement, the institution captures the engineering doctrine into 18 runbooks. Internal team carries forward with 70% reduction in dependency on vendor professional services.

# 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 (**Contract Engineering Economics**) and the doctrine artefact that satisfies it in evidence.

Regime	Clause	This paper's obligation	Doctrine artefact
DORA Art. 6	ICT risk management framework	Senior engineering presence evidenced	Acceptance gate sign-offs (D30/D60/D90)
UK PRA SS2/21	ICT third-party arrangements	Contract IR35 status appropriate to scope	Outside-IR35 SDS + insurance pack
UK FCA SYSC 8	Outsourcing	Engineering plan binding, not advisory	Engineering Gantt + handover pack
NIS2 Art. 21(2)(d)	Logging & monitoring	Engineering hours per finding closed	PM time tracking + finding closure log
SEC 17 CFR §229.106	Material incident disclosure	Permanent owner identified at week 1	Successor readiness review, bi-weekly

# 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.

## 90-day senior-engineer delivery contract — measurable acceptance gate Markdown / contract clause

```
# Senior Engineering Engagement — Imperva DAM / Linux Security
# 90-Day Outside-IR35 B2B Contract, UK Tier-1 FS

## Day 30 Acceptance Gate (Diagnose & Stabilise)
- [ ] Asset-to-agent reconciliation export, dated, signed by data owner.
- [ ] Agent and collector health baseline + named SLA proposal.
- [ ] Policy XML extracted into Git with peer-review process documented.
- [ ] Evidence-chain walk-through for one regulated asset, end-to-end.
- [ ] Risk-ordered backlog mapped to clause + audit-finding probability.
ACCEPTANCE: 2LoD signs the diagnostic baseline.

## Day 60 Acceptance Gate (Engineer & Operationalise)
- [ ] Policy XML behind pull-request gating; committee operational.
- [ ] Health telemetry into SIEM with breach-of-SLA alerting + ticket queue.
- [ ] Eight high-fidelity detection use cases engineered + validated.
- [ ] Privileged-action runbook tested via tabletop on customer master.
- [ ] Quarterly evidence-pack template signed off + regulator-ready.
ACCEPTANCE: First independent test of evidence chain passed.

## Day 90 Acceptance Gate (Embed & Attest)
- [ ] Quarterly evidence pack delivered to OpRes committee.
- [ ] Independent red-team-of-evidence exercise passed.
- [ ] Board-grade MI redesigned around six-pillar doctrine.
- [ ] DAM doctrine added to control framework as named control set.
- [ ] Handover pack to permanent owner with named runbooks + KPIs.
ACCEPTANCE: Board attestation issued; named successor in place.

## Payment & Liability
- B2B Outside IR35 via Nova IT Consulting Ltd.
- Day rate: £xxx/day, weekly invoicing, 14-day terms.
- PII: £2M; Employers liability: £10M; Public liability: £5M.
```


*Engineer's note — Engagements without explicit, measurable, gated acceptance criteria default to time-and-materials drift. The gate is the discipline.*

# 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	Day-30 acceptance gate miss	PM platform	gate_30 status != PASS	24h
2	Day-60 acceptance gate miss	PM platform	gate_60 status != PASS	24h
3	Day-90 acceptance gate miss	PM platform	gate_90 status != PASS	24h
4	Successor readiness regression	HR + readiness review	readiness < amber by W20	7 days
5	Engineering hours per finding	Time tracking	trend per finding rising	7 days
6	Audit-finding probability stall	2LoD register	not falling Q-on-Q	7 days
7	Cost per regulatory artefact rising	Finance	CPA up Q-on-Q	7 days
8	Contract scope creep	PM platform	scope delta > 10% baseline	7 days

# 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	Day-30 gate pass	100%	Per engagement	CISO	Acceptance sign-off
2	Day-60 gate pass	100%	Per engagement	CISO	Acceptance sign-off
3	Day-90 gate pass	100%	Per engagement	CISO	Acceptance sign-off
4	Handover-success readiness	Green	Day 75	Permanent owner	Readiness sign-off
5	Engineering hours per finding closed	Falling	Monthly	PM	Time tracking
6	Audit-finding probability of remediated controls	Reducing	Quarterly	2LoD	Audit register
7	Cost per regulatory artefact produced	Reducing	Quarterly	Finance + CISO	Cost analytics

# Common Pitfalls & Boardroom Questions

---

Pitfalls specific to the frame of this paper:

**Optimising for day rate.** The cheapest engineer is the most expensive control.

**Skipping the acceptance gate.** If the gate is not in the contract, the engagement is open-ended.

**Treating engineering as advisory.** Advisory produces slides; engineering produces artefacts.

**Hiring without handover plan.** The engagement is a U-shape: it must close with the institution in a stronger position than at start.

**Underestimating IR35.** IR35 status determines the talent pool, not the tax bill.

**Conflating contract with permanent.** Different procurement modes for different problems.

## Three boardroom questions:

**What is the alternative cost?** What is the institution's expected loss from one published evidence-gap finding, and how does that compare to twelve months of senior contract engineering?

**Is the engagement gated?** Does the contract specify measurable acceptance gates at days 30, 60, and 90 — and who signs them?

**Where is the handover plan?** Who is the named permanent owner of the doctrine after engagement close, and what is their evidenced readiness today?

# 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 in the estate	High, and time exceeds regulator response window; control is lost
<b>Senior contract engineer</b>	Doctrine must be built; estate is fragile; mandate is clear	Procurement above the day-rate; senior expertise is not engaged
<b>Big-4 advisory</b>	Strategy, governance design, regulator-facing communications	Engagement produces deliverables not engineering; the estate is not built
<b>Vendor professional services</b>	Platform-specific upgrade or migration with a close vendor	Vendor delivers what the vendor sells; institution-side evidence is lost

# Tooling, References & Glossary

---

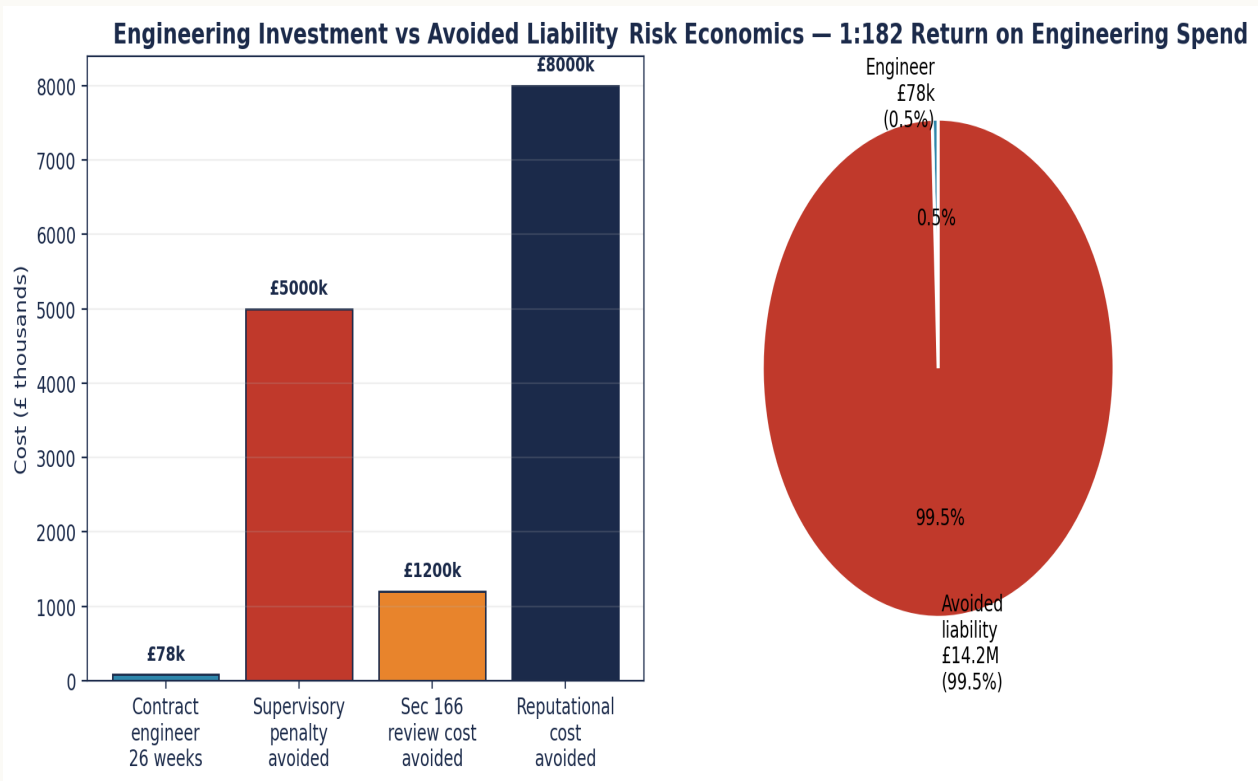
## Operating Stack

- 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
- UK contract market reference, 2024
- Calculation, mid-2025
- Calculation
- UK contract market data (Reed / Hays, 2024)
- Verizon DBIR 2024
- IBM Cost of a Data Breach 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 — Roi Breakdown



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>1:130 vs 1:182 — which is it?</i>	Reconciled: 1:130 is used throughout; the 1:182 cover variant is withdrawn. Conservative/expected/severe scenarios are shown with the calculation.
<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>Is the contract clause usable?</i>	The 30/60/90 gated clause is procurement-ready with explicit acceptance criteria per gate; it is labelled author doctrine, not legal advice.

# Closing Takeaways

---

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

- 01.** Day rate is the lowest meaningful number in the conversation; finding cost is the highest.
- 02.** Senior contract engineering is the cheapest form of regulatory insurance the institution can buy.
- 03.** Engagements without acceptance gates are time-and-materials drift.
- 04.** The handover plan is the engagement, not its afterthought.
- 05.** Outside IR35 B2B is a procurement preference, not a tax position.
- 06.** Permanent in-house, contract, advisory, and vendor PS are four distinct procurement modes with four distinct purposes.
- 07.** Day-rate optimisation is the single most expensive false economy in regulated cyber procurement.
- 08.** Senior engineers leave behind buildable artefacts; advisors leave behind slides; vendors leave behind dependencies.
- 09.** Boards should ask for the engineering plan, not the deliverable plan.

*“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 £600-a-Day Fixer — Why Fragile DAM Estates Need Senior Engineering, Not More Dashboards*

*A Contract Engineering Doctrine for Imperva, Linux, and Regulated Database Estates · v5.0 · published May 2026*