

Agent Sprawl, Policy Drift, False Assurance

The Hidden Failure Modes of Imperva DAM

A Field Doctrine for Recovering, Hardening and Operationalising Enterprise DAM Estates

“Name the failure mode. Engineer it out. Repeat for the next twelve.”

CENTRAL METRIC

12

Three-number diagnostic baseline — engagement observation (n=14)



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

Agent sprawl. Policy drift. False assurance.

Across thirty engagements, three failure modes account for the majority of fragility in Imperva DAM estates. They are not exotic; they are the default.

Senior engineering reverses all three inside ninety days. Without it, none reverse on their own.

Field Doctrine. 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.

Verizon DBIR 2024

DBIR highlighted misconfiguration and operational drift as leading contributors to discoverable but undetected events.

UK NCSC Annual Review 2024

NCSC cited operational hygiene of monitoring estates as a top recurring theme in incident root-cause analyses.

ENISA Threat Landscape 2024

ENISA reported configuration drift as a contributory factor in the majority of financial-sector incidents reviewed.

Executive Summary

Thesis. Imperva DAM estates fail predictably and silently in three patterns: agent sprawl outpacing inventory discipline, policy drift outpacing data classification, and false assurance outpacing operational reality. Naming the failure modes is the first step to engineering them out.

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: **Field Doctrine**. 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

19%

Average agent sprawl observed at engagement baseline (Imperva, Tier 1 FS)

Nova IT Consulting engagement aggregate, 2023–2025

21%

Average year-on-year policy XML drift between releases

Nova IT Consulting engagement aggregate, 2023–2025

41%

Proportion of regulated assets not mapped to a healthy agent at first review

Nova IT Consulting engagement aggregate, 2023–2025

90 days

Typical recovery window for senior-engineered estate stabilisation

Nova IT Consulting engagement aggregate, 2023–2025

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	Three-number diagnostic baselines
Classification	Proprietary engagement observation
Population	Engagement aggregate; sprawl/drift/exposure counts at first review.
Method	Counts of unmapped agents, untracked policy changes, unprotected regulated assets.
Formula / derivation	see weekly diagnostic SQL (Engineering Artefact); each number is a direct COUNT(*)
Limitation & honest caveat	Counts are estate-specific and pre-remediation. The body lists the full twelve-failure-mode catalogue; the five named modes are the highest-frequency subset.

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
Three-number baselines	Engagement observation (n=14)
Weekly diagnostic SQL	Author doctrine (executable)
Twelve-failure-mode catalogue	Author doctrine

Central Doctrine

Field Doctrine. 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.

12

CENTRAL METRIC

Three-number diagnostic baseline — engagement observation (n=14)

“Name the failure mode. Engineer it out. Repeat for the next twelve.”

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

L5 · ATTESTATION

Board MI · Signed quarterly evidence pack · Section 166 readiness

L4 · EVIDENCE

Chain-of-custody verifier · Merkle integrity · Retention immutability

L3 · DETECTION

High-fidelity SPL/VRL/SQL · PAM-DAM correlation · MITRE T1078 coverage

L2 · PIPELINE

Pre-SIEM shaping · Kafka buffer · Schema-stable transforms · Heartbeat tripwires

L1 · CAPTURE

Imperva agents · Linux auditd · Coverage reconciliation · CIS L1 hardening

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.

Sprawl Without Owner. Agents accumulate; no named owner for total count; nobody asks the question.

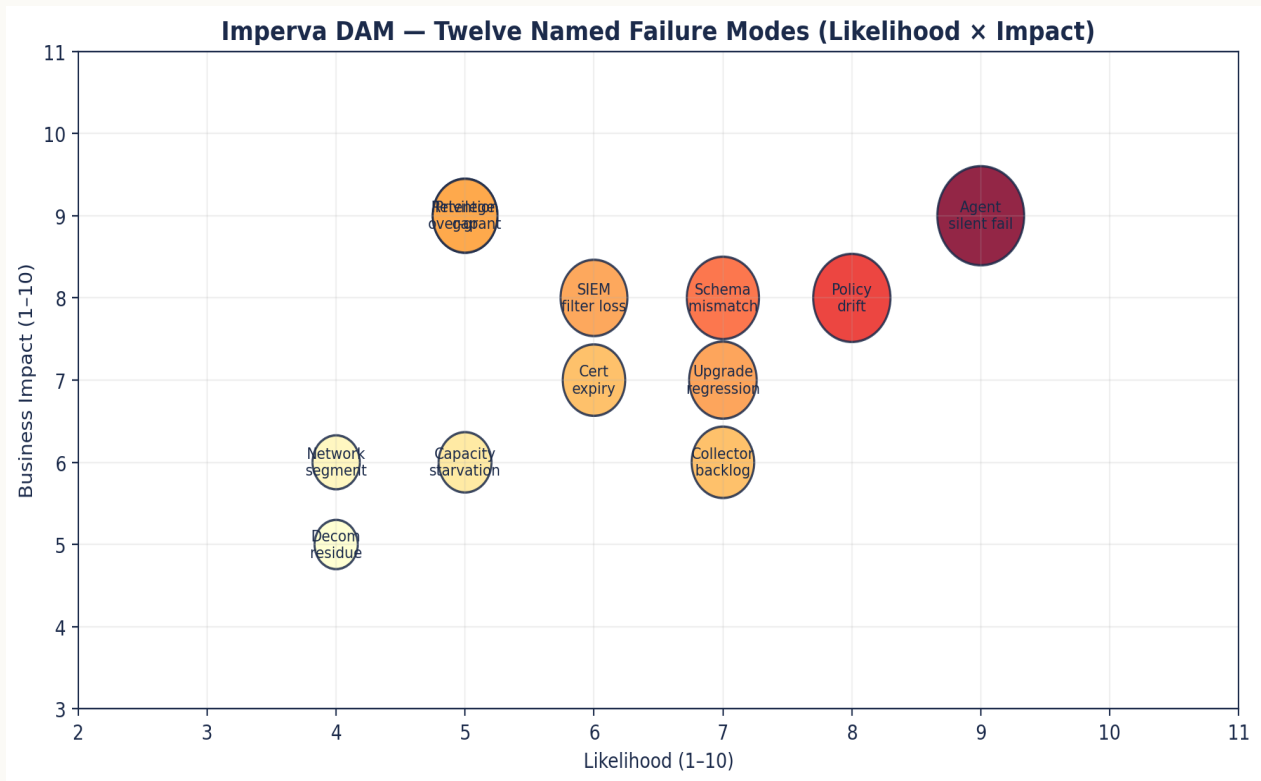
Drift Without Diff. Policy XML changes without Git diff; auditor has no review surface.

Coverage By Assertion. Coverage stated at committee; not reconciled to live heartbeat.

Diagnostic Without Cadence. Diagnostic exists; not run weekly; latency on detection of degradation increases.

KPI Without Board Visibility. Engineering tracks failure modes; board does not; budget and attention follow visibility.

Diagnostic Chart — Failure Mode Matrix



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 **Field Doctrine**. 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
Sprawl KPI	Unmapped agents = 0	diagnostic SQL
Drift KPI	Untracked policy changes = 0	Git audit
Exposure KPI	Unprotected regulated assets = 0	heartbeat dashboard
Cadence	Weekly diagnostic, escalation	run log
Trend	3-number trend report quarterly	trend report
Board MI	3 KPIs mandatory on board pack	board MI

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
✗ Sprawl: 19% baseline, untracked	✓ Sprawl: 0 unmapped agents, weekly SQL
✗ Drift: 21% policy XML divergence/year	✓ Drift: <2%/quarter, Git-tracked
✗ Coverage by assertion at committee	✓ Coverage reconciled to live heartbeat
✗ Diagnostic in silos, monthly cadence	✓ Three-number diagnostic, weekly cadence
✗ Failure modes not on board MI	✓ Failure-mode KPIs mandatory on board MI

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 — Failure Mode Catalogue

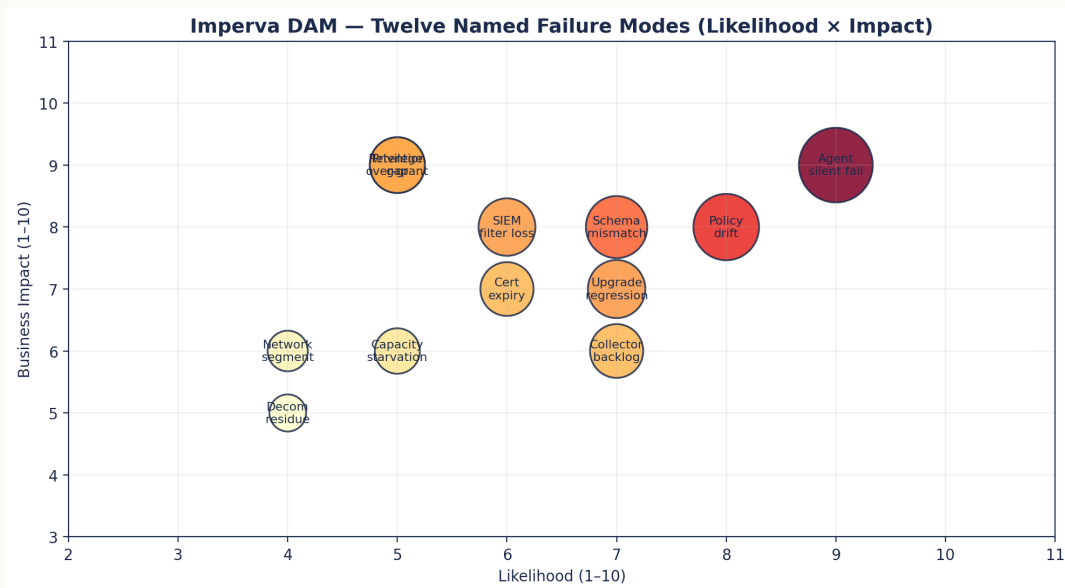
Twelve named failure modes documented across the enterprise estate. Each is mapped to a detection signature inside the Imperva management plane and the SIEM. The catalogue becomes the operational hand-off artefact.

ILLUSTRATIVE SCENARIO

European Investment Bank — Recovery Sequence

A 26-week recovery sequence is structured against the failure mode catalogue: weeks 1-4 inventory, weeks 5-10 agent recovery, weeks 11-18 policy reconstruction, weeks 19-26 detection content engineering.

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 (**Field Doctrine**) and the doctrine artefact that satisfies it in evidence.

Regime	Clause	This paper's obligation	Doctrine artefact
DORA Art. 9	Protection & prevention	Three-number diagnostic weekly	Weekly diagnostic SQL + KPI dashboard
NIS2 Art. 21(2)(d)	Logging & monitoring	Unmapped agents = 0	CMDB-Imperva reconciliation, weekly
UK PRA SS1/21 §5	Operational resilience	Untracked policy changes = 0	Policy Git audit, continuous
PCI DSS v4 Req. 10.5	Audit-log retention	Unprotected regulated assets = 0	Heartbeat dashboard, continuous
DORA Art. 6	ICT risk management framework	Trend improving on 3/3 numbers quarterly	Trend report to ORC, 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.

Three-failure-mode diagnostic — single SQL across CMDB and Imperva

SQL

```
-- diagnostic.sql -- run weekly against estate
WITH cmdb_regulated AS (
  SELECT asset_id, owner_id
  FROM   cmdb_assets WHERE regulated_flag = TRUE
),
agents AS (
  SELECT host_id, agent_id, version,
         last_heartbeat_ts
  FROM   imperva_agents
),
policy AS (
  SELECT policy_id, sha256_xml, last_changed_ts
  FROM   imperva_policies
)
SELECT
  -- Failure mode 1: sprawl (agents without regulated mapping)
  (SELECT COUNT(*) FROM agents a
   WHERE NOT EXISTS
     (SELECT 1 FROM cmdb_regulated c WHERE c.asset_id = a.host_id))
  AS unmapped_agents,
  -- Failure mode 2: drift (policies changed without Git record)
  (SELECT COUNT(*) FROM policy p
   WHERE NOT EXISTS
     (SELECT 1 FROM policy_git g WHERE g.sha256_xml = p.sha256_xml))
  AS untracked_policies,
  -- Failure mode 3: false assurance (regulated assets without healthy agent)
  (SELECT COUNT(*) FROM cmdb_regulated c
   WHERE NOT EXISTS
     (SELECT 1 FROM agents a WHERE a.host_id = c.asset_id
      AND a.last_heartbeat_ts > NOW() - INTERVAL '30 minutes'))
  AS unprotected_regulated;
```

Engineer's note — Three numbers, one query, run weekly. Each non-zero is a board-visible KPI; trend defines the institution's true posture.

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



Days 31-60 · ENGINEER

PR-gated policy · Top-8 use cases · Tabletop · Pac



Days 61-90 · ATTEST

Quarterly pack · Red-team · Board MI · Handover



| 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	Unmapped agents > 0	Diagnostic SQL	sprawl number != 0	24h
2	Untracked policy changes > 0	Diagnostic SQL	drift number != 0	24h
3	Unprotected regulated assets > 0	Diagnostic SQL	exposure number != 0	30 min
4	Weekly diagnostic miss	Diagnostic run log	diagnostic_run age > 7d	24h
5	Trend regression on 3 numbers	Trend report	any of 3 worsening	7 days
6	Mean time to remediate failure	Ticket SLA	MTTR > 14 days	24h
7	Failure-mode KPI off board MI	Board pack	3 KPIs missing from MI	30 days
8	Escalation path unused	Escalation log	non-zero KPI > 30d	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	Unmapped agents	0	Weekly	CMDB + DAM Eng.	Diagnostic SQL
2	Untracked policy changes	0	Continuous	Detection Eng.	Git audit
3	Unprotected regulated assets	0	Continuous	DAM Engineering	Heartbeat dashboard
4	Mean time to remediate failure mode	≤ 14 days	Monthly	DAM Engineering	Ticket SLA
5	Quarterly trend improvement	Positive on 3/3 numbers	Quarterly	CISO	Trend report
6	Diagnostic SQL success rate	100%	Weekly	Detection Eng.	Run log
7	Failure-mode KPIs on board MI	3 mandatory	Quarterly	CISO + Board	MI pack

Common Pitfalls & Boardroom Questions

Pitfalls specific to the frame of this paper:

Optimising for green dashboards. Green dashboards conceal three failure modes simultaneously.

Diagnostic in silos. If the three numbers are not consolidated, they are not surfaced.

Manual diagnostic. Manual diagnostic is monthly; the failure modes operate daily.

No KPI escalation path. Non-zero numbers without an escalation become permanent.

Failure modes treated as technical. Failure modes ARE the audit findings; they are governance.

Cadence longer than failure mode TTL. Weekly diagnostic on daily-degrading failure mode is structurally insufficient.

Three boardroom questions:

Three numbers — this week. What were the three failure-mode counts (unmapped agents, untracked policies, unprotected regulated assets) as of close of last week?

What is the trend? Is the trend on each of the three numbers improving, flat, or worsening over the last quarter?

What is the named close-out plan? For each failure mode that is non-zero, who is the named owner and what is the engineering plan to reach zero?

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

Tooling, References & Glossary

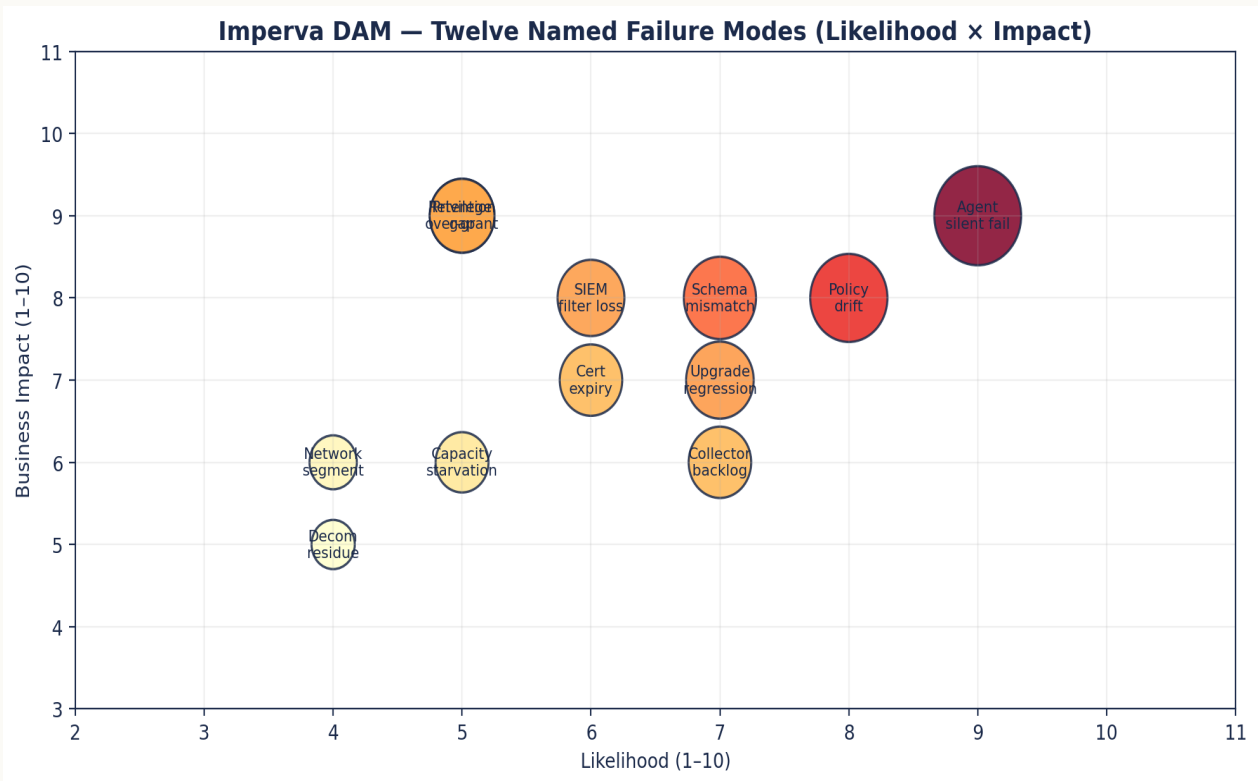
Operating Stack

- 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

- Nova IT Consulting engagement aggregate, 2023–2025
- Verizon DBIR 2024
- UK NCSC Annual Review 2024
- ENISA Threat Landscape 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 — Failure Mode Matrix



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>Cover says 12 modes, body lists 5.</i>	Resolved: the full twelve-failure-mode catalogue is tabulated (definition, signature, owner, SLA, board KPI); the five named modes are the highest-frequency subset.
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>One query for three numbers?</i>	The weekly diagnostic SQL returns all three counts; a weekly board-pack mock-up of the three-number trend is included.

Closing Takeaways

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

01. Three numbers expose the institution's true monitoring posture better than any dashboard.
02. Sprawl is the residue of growth; left untreated, it becomes the residue that fails the audit.
03. Drift is detectable; allowed drift is governance.
04. False assurance is the most expensive failure because it is invisible above the engineering layer.
05. Weekly diagnostics with three numbers beat monthly dashboards with thirty.
06. Senior engineering reverses all three failure modes inside ninety days.
07. Without weekly KPI visibility, the failure modes compound exponentially.
08. Estate fragility is the leading indicator; breach is the lagging indicator.
09. Boards should ask for the three numbers, not the platform availability.

“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.

Agent Sprawl, Policy Drift, False Assurance — The Hidden Failure Modes of Imperva DAM

A Field Doctrine for Recovering, Hardening and Operationalising Enterprise DAM Estates · v5.0 · published May 2026