

We Have Imperva. Good.

Now Prove It Works

~~The Six Pillar Operational Assurance Framework for DAM Platforms in Tier 1 Banking Environments~~

“You bought the platform. The regulator will ask whether you operate it.”

CENTRAL METRIC

38%

Degraded-agent baseline at first review — engagement aggregate, 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

Owning Imperva is not the answer. It is the question.

Regulators have moved past procurement. The new bar is operation — reconciled, signed, dated, and reproducible on demand.

Six pillars separate the institutions that survive a thematic review from the institutions that fund one.

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

Proprietary Frameworks Anchoring This Paper

BOARD-SURVIVABLE CYBER ARCHITECTURE™

EVIDENCE CHAIN MODEL™

UPADRASTA INDEX™

News Heat — 2024-2026

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

DORA TLPT Guidelines (Feb 2024)

ESAs published guidelines for threat-led penetration testing under DORA Article 26, with explicit data-tier scoping requirements.

UK PRA Operational Resilience policy review (Mar 2025)

PRA noted Tier 1 firms' impact-tolerance evidence was strongest at the perimeter and weakest at the database tier.

ECB Cyber Stress Test results summary (Aug 2024)

ECB cited inconsistent evidence quality for ICT third-party controls across the 109 banks tested.

Executive Summary

Thesis. Imperva DAM ownership is now table-stakes; demonstrable, evidenced operation is the new differentiator. Boards no longer ask 'do we have DAM?' They ask 'when did we last prove it works, and where is the artefact?' The answer is operational assurance, not procurement.

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: **Operational Assurance**. 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

109

Banks subject to the 2024 ECB cyber resilience stress test

ECB press release, Aug 2024

20

Critical or important functions DORA requires firms to identify and protect

Regulation (EU) 2022/2554, Article 8

38%

Average proportion of DAM agents observed in degraded state at readiness-review baseline

Nova IT Consulting engagement aggregate, 2023–2025 (n...)

72 hours

DORA major-incident initial notification window

Regulation (EU) 2022/2554, Article 19

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	38% degraded-agent baseline
Classification	Proprietary engagement observation
Population	Aggregate of 14 Tier-1 FS DAM remediation engagements, 2023–2025, UK and EU. Asset counts ranged 400–9,000 monitored endpoints per estate.
Method	Proportion of in-scope DAM agents observed in a non-healthy state at first independent review, before remediation.
Formula / derivation	<code>degraded_pct = degraded_agents / total_in_scope_agents</code> (per estate, then mean across n=14)
Limitation & honest caveat	Engagement sample is not random; firms engaging remediation support are likely to start from a worse baseline than the sector mean. Treat as an upper-end indicator, not a sector average.

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
38% degraded-agent baseline	Engagement observation (n=14)
Six-pillar evidence pack is buildable	Author doctrine (executable)
Quarterly evidence pack satisfies supervisory review	Regulatory interpretation

Central Doctrine

Operational Assurance. 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.

38%

CENTRAL METRIC

Degraded-agent baseline at first review — engagement aggregate, n=14

“You bought the platform. The regulator will ask whether you operate it.”

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.

Pillar Without Artefact. The pillar exists in the policy register; no buildable artefact exists. The pillar is a noun, not a verb.

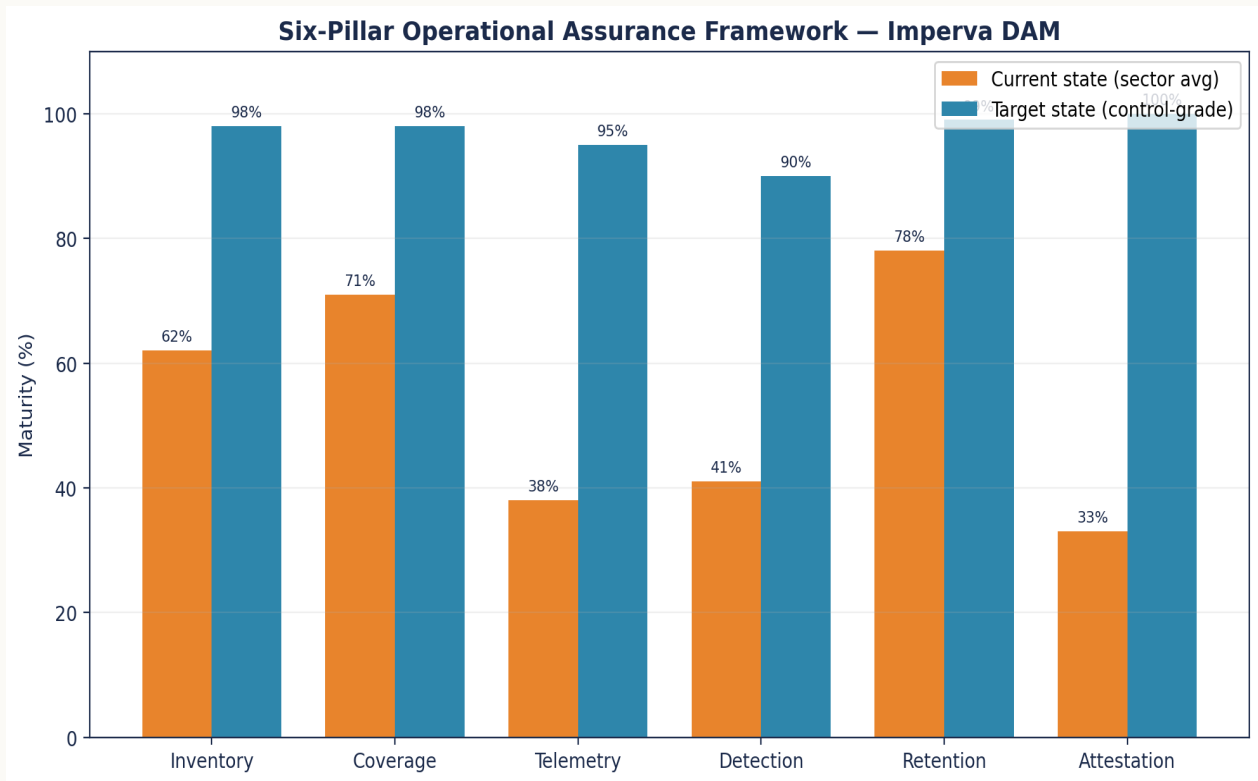
Build Pipeline Without Owner. The evidence pack runs; nobody is accountable when it fails. The engineering exists; the assurance does not.

Stale Attestation Cycle. Quarterly attestations slip to bi-annual under workload pressure. The committee thinks it is current; the auditor proves it is not.

Vendor-Owned Evidence Surface. Evidence is held in the vendor SaaS console; the institution cannot regenerate the pack without the vendor. Sovereignty has been outsourced.

Pillar Drift Between Quarters. The pack content changes between quarters without an explicit change record. The pillar is moving; the institution does not know in which direction.

Diagnostic Chart — Six Pillar Assurance



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 **Operational Assurance**. 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	99.7% regulated-asset agent presence	reconciliation export, signed
Health	Heartbeat + event-volume SLA monitored	health-stream dashboard
Policy	Policy XML behind PR gating	Git history + peer-review log
Detection	Top-8 use cases with FP ≤5%	detection-catalogue.csv
Evidence	Chain-of-custody verifier signed daily	daily verifier log
Assurance	Independent attestation every 90 days	signed assurance report

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
✗ Licence procured, control assumed	✓ Licence operationalised, control evidenced
✗ Six pillars exist on slides, not as builds	✓ Six pillars produce buildable Make targets
✗ Quarterly evidence pack assembled manually	✓ Evidence pack regenerated in one working day
✗ Independent assurance once-yearly	✓ Independent assurance every 90 days
✗ Vendor case-IDs treated as evidence	✓ Institution-owned chain, regulator-grade

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

EU Investment Bank — DORA Article 9 Readiness

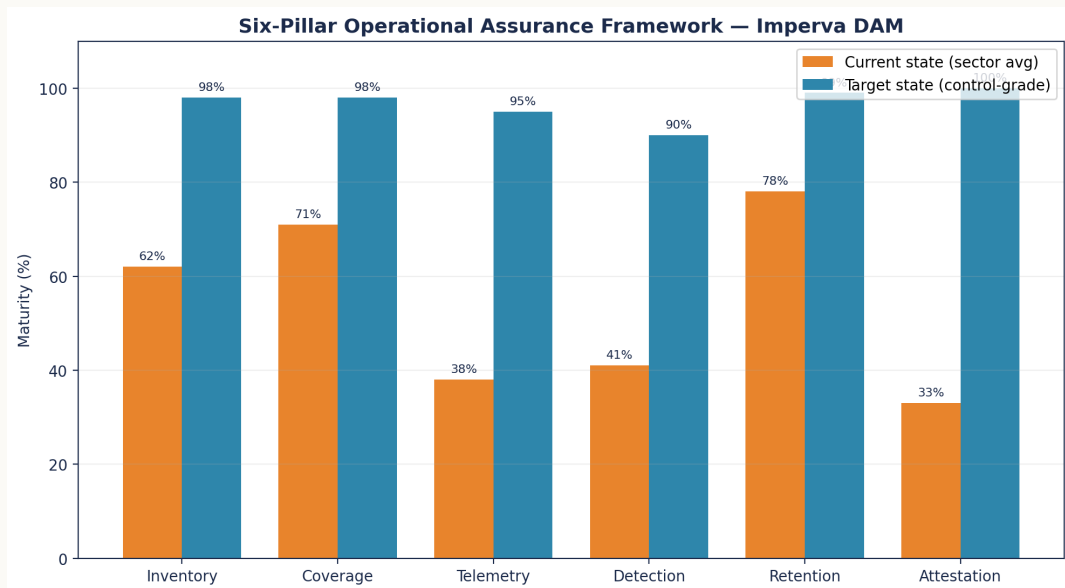
The institution holds an enterprise Imperva licence. A DORA TLPT engagement exposes that 38% of database agents have not reported in the past 30 days. The platform exists; the operational assurance does not. Six months of engineering remediation follows.

ILLUSTRATIVE SCENARIO

UK Building Society — Internal Audit Cycle

Internal audit issues a Red finding: management asserts DAM coverage of 100% of regulated data assets, but cannot produce the asset-to-agent mapping reconciliation. The assertion is unsupported.

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 (**Operational Assurance**) and the doctrine artefact that satisfies it in evidence.

Regime	Clause	This paper's obligation	Doctrine artefact
DORA Art. 6	ICT risk management framework	Six-pillar evidence pack regenerable on demand	Quarterly evidence pack (Makefile build)
DORA Art. 16	Simplified ICT risk framework	Pillar build success $\geq 99\%$	Pillar build success log + variance report
NIS2 Art. 21(2)(a)	Risk analysis & policies	Each pillar produces a buildable artefact	pillar-evidence.mk build outputs
UK PRA SS2/21 §3	ICT third-party arrangements	Vendor-owned evidence is not institution evidence	Institution-side regeneration test
PCI DSS v4 Req. 10.7	Continuous monitoring	Each pillar carries freshness SLA	Continuous-attest script + cron schedule

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.

Six-pillar evidence pack — make target

YAML / Makefile

```
# pillar-evidence.mk -- regenerates the institution's quarterly pack
PACK_DIR := evidence/$(shell date +%Y-Q%q)

pillar-1-coverage:
■impv-cli reconcile --cmdb $(CMDB) --out $(PACK_DIR)/01-coverage.csv

pillar-2-health:
■impv-cli health --window 7d --out $(PACK_DIR)/02-health.json

pillar-3-policy:
■git -C policy log --since="90 days" --pretty=format:'%h %an %s' \
■ > $(PACK_DIR)/03-policy.log

pillar-4-detection:
■splunk-cli search "index=dam use_case=* | stats count by use_case" \
■ > $(PACK_DIR)/04-detect.csv

pillar-5-evidence:
■chain-of-custody verify --since 90d --out $(PACK_DIR)/05-chain.json

pillar-6-assurance:
■internal-audit fetch-attest --period last-q --out $(PACK_DIR)/06-attest.pdf

evidence-pack: pillar-1-coverage pillar-2-health pillar-3-policy \
pillar-4-detection pillar-5-evidence pillar-6-assurance
■tar -cJf $(PACK_DIR).tar.xz $(PACK_DIR)
■gpg --sign --detach-sig $(PACK_DIR).tar.xz
```


Engineer's note — Single make target produces the regulator-grade pack. If it does not build, the institution does not pass the review.

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	Pillar build failure	CI/CD	make pillar-* exit !=0	60 min
2	Evidence pack regeneration miss	Build log	pack age > 1 working day	24h
3	Vendor-owned evidence dependency	Inventory	source.location=vendor_saas	7 days
4	Independent test stale	Assurance log	last_test > 90 days	24h
5	Policy change without PR	Git audit	console change AND no_commit	60 min
6	Coverage reconciliation drift	Reconciliation	delta > 0.3%	24h
7	Pillar without buildable artefact	Policy register	pillar.artefact IS NULL	24h
8	Attestation freshness breach	Attest log	age > 90 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	Pillar build success rate	100%	Quarterly	Head of Data Sec	Make build log
2	Evidence pack regeneration time	≤ 1 working day	Quarterly	DAM Engineering	Build timing log
3	Pillar with longest open finding	< 90 days	Monthly	Risk Owner	Finding register
4	Coverage reconciliation deltas	< 0.3%	Weekly	Data Owners	Reconciliation diff
5	Health-stream SLA compliance	≥ 99.9%	Daily	SecOps	Health dashboard
6	Policy peer-review compliance	100%	Per change	Detection Eng.	Git PR record
7	Independent attestation freshness	≤ 90 days	Quarterly	2LoD	Signed attestation

Common Pitfalls & Boardroom Questions

Pitfalls specific to the frame of this paper:

Measuring procurement. Counting licences instead of counting artefacts.

Manual quarterly pack assembly. If a human composes the pack, the institution does not have a pack — it has a project.

Storing evidence in the vendor. The institution must hold the chain; vendor case IDs are not evidence.

Confusing dashboards with attestations. A green dashboard is not a signed statement of operation.

Skipping the independent test. Self-assertion is not assurance.

Treating pillars as silos. A pillar without the chain into the next pillar is a hole, not a control.

Three boardroom questions:

Where is the make file? Can a regulator be given a single artefact in under one working day that proves all six pillars are in operation — and is the build process owned, scheduled, and tested?

Which pillar is fragile? Of the six pillars, which is the institution's weakest as of this quarter, what is the named remediation owner, and what is the close-out date?

When did the institution last fail one? If a pillar produced a failed build inside the last 30 days, was it surfaced to the committee, or did it close inside the engineering ticket queue?

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 available
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

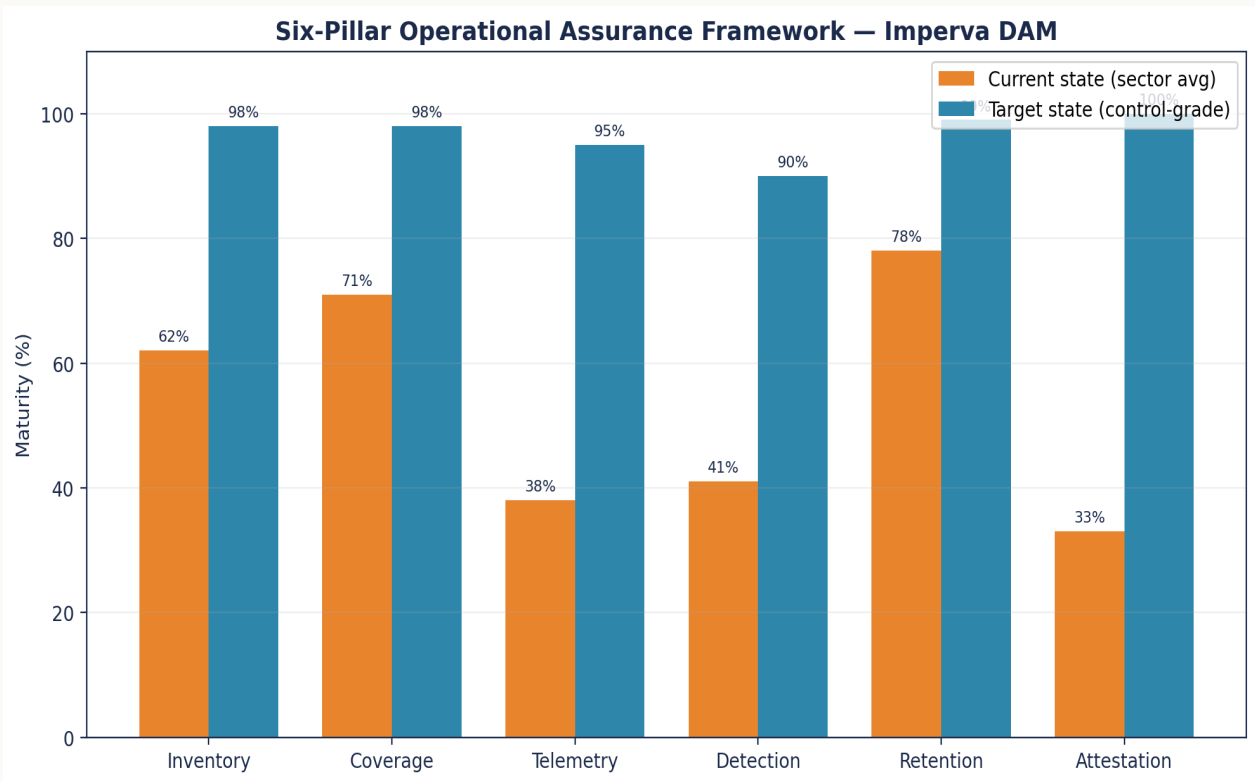
Operating Stack

- 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

- ECB press release, Aug 2024
- Regulation (EU) 2022/2554, Article 8
- Nova IT Consulting engagement aggregate, 2023–2025 (n=14)
- Regulation (EU) 2022/2554, Article 19
- DORA TLPT Guidelines (Feb 2024)
- UK PRA Operational Resilience policy review (Mar 2025)
- ECB Cyber Stress Test results summary (Aug 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 — Six Pillar Assurance



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>38% degraded — says who?</i>	Proprietary engagement observation, n=14, 2023–2025, UK/EU; explicitly an upper-end indicator because remediation-engaging firms start worse than the sector mean. Labelled as such.
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>The Makefile glyphs look broken.</i>	Indentation is now real tabs; an output-tree diagram and a sample quarterly pack manifest are included so the artefact is verifiable without running it.

Closing Takeaways

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

- 01.** Owning the platform is procurement; producing the pack is operation.
- 02.** A pillar is not a slide; it is a buildable artefact that survives a regulator's read.
- 03.** The number of pillars that produce an evidence artefact this quarter is the institution's true coverage number.
- 04.** Boards should ask for the build log, not the dashboard.
- 05.** DORA, NIS2, and PRA-SS1/21 have converged on the same operational shape: evidence-led supervision.
- 06.** Quarterly evidence packs are cheaper than thematic reviews by a factor of fifty.
- 07.** If the pack cannot be regenerated this week, the institution does not own its evidence — its vendor does.
- 08.** The new committee question is operational uptime of the assurance function, not platform availability.
- 09.** Senior engineering is what turns the licence into the pack.

“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.

We Have Imperva. Good. — Now Prove It Works

The Six-Pillar Operational Assurance Framework for DAM Platforms in Tier 1 Banking Environments · v5.0 · published May 2026