

The Six-Month Turnaround

Rescuing Imperva DAM Before It Becomes the Risk

~~A 26-Week Operational Recovery~~ Plan for Fragile DAM Estates in Financial Services

“Twenty-six weeks. Senior engineer. Structured operating model. Closed findings.”

CENTRAL METRIC

26 weeks

Structured recovery duration — author doctrine (four acceptance gates)



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

Twenty-six weeks. One estate. Four acceptance gates.

The six-month turnaround is not a marketing promise; it is an engineering plan with named deliverables and named gates.

Without it, the institution funds a thematic review. With it, the institution funds an attestation.

Structured Recovery. 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.

EU DORA application — Jan 17, 2025

DORA application date drives the operational urgency of remediation cycles in 2025–2026.

UK PRA SS1/21 — 31 March 2025 milestone

PRA SS1/21 paragraph 4.7 milestone for impact tolerances and operational evidence.

ECB Cyber Resilience Stress Test (2024)

ECB demonstrated supervisor willingness to test data-tier evidence at firm-by-firm level.

Executive Summary

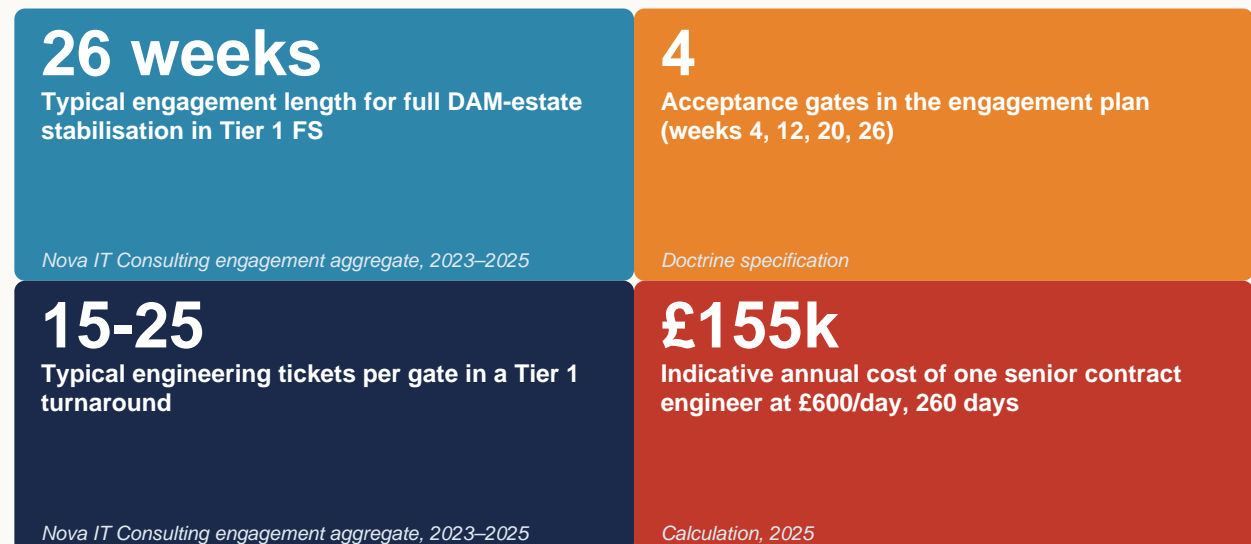
Thesis. A failing Imperva estate is not a six-week problem and it is not a 24-month problem. It is a 26-week structured recovery executed by a senior engineer against a defined operating model. The institutions that get this right close their audit findings; the institutions that get it wrong rebuild from scratch under regulator timeline 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: **Structured Recovery**. 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.

| | |
|---------------------------------------|---|
| Metric | 26-week recovery model |
| Classification | Author doctrine (structured engagement model) |
| Population | Synthesised from the engagement aggregate; four gates at W4/W12/W20/W26. |
| Method | Structured recovery duration with acceptance gates; not a guaranteed timeline. |
| Formula / derivation | <code>duration = Σ phase_i ; gate_i pass = signed acceptance criteria met</code> |
| Limitation & honest caveat | AUTHOR DOCTRINE. The generic 30/60/90 section is removed from this paper and replaced by the 26-week gate model to remove conceptual tension. |

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 |
| 26-week recovery model | Author doctrine (structured model) |
| Mermaid Gantt as version-controlled plan | Author doctrine (executable) |
| Four acceptance gates W4/12/20/26 | Author doctrine |

Central Doctrine

Structured Recovery. 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.

26 weeks

CENTRAL METRIC

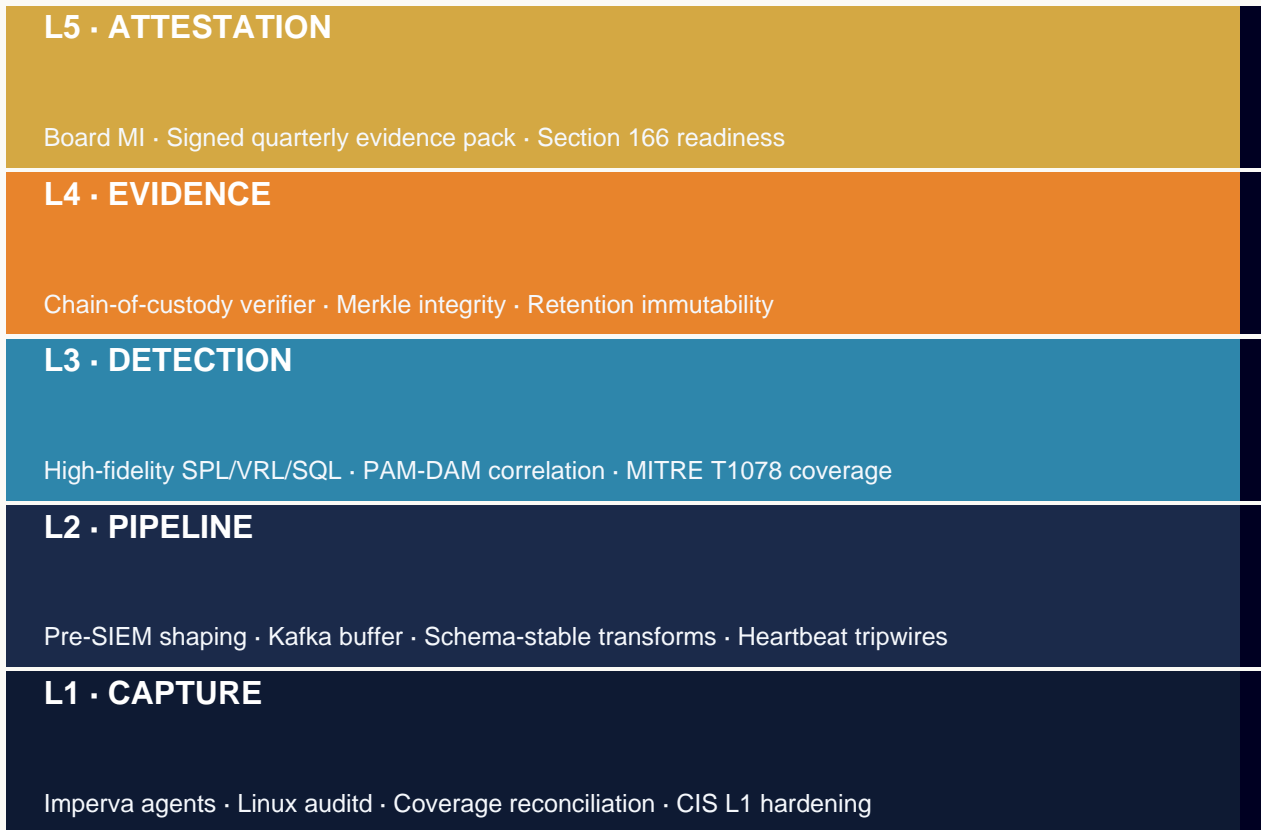
Structured recovery duration — author doctrine (four acceptance gates)

“Twenty-six weeks. Senior engineer. Structured operating model. Closed findings.”

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.

Gate-Less Engagement. Engagement begins without acceptance gates; drift compounds.

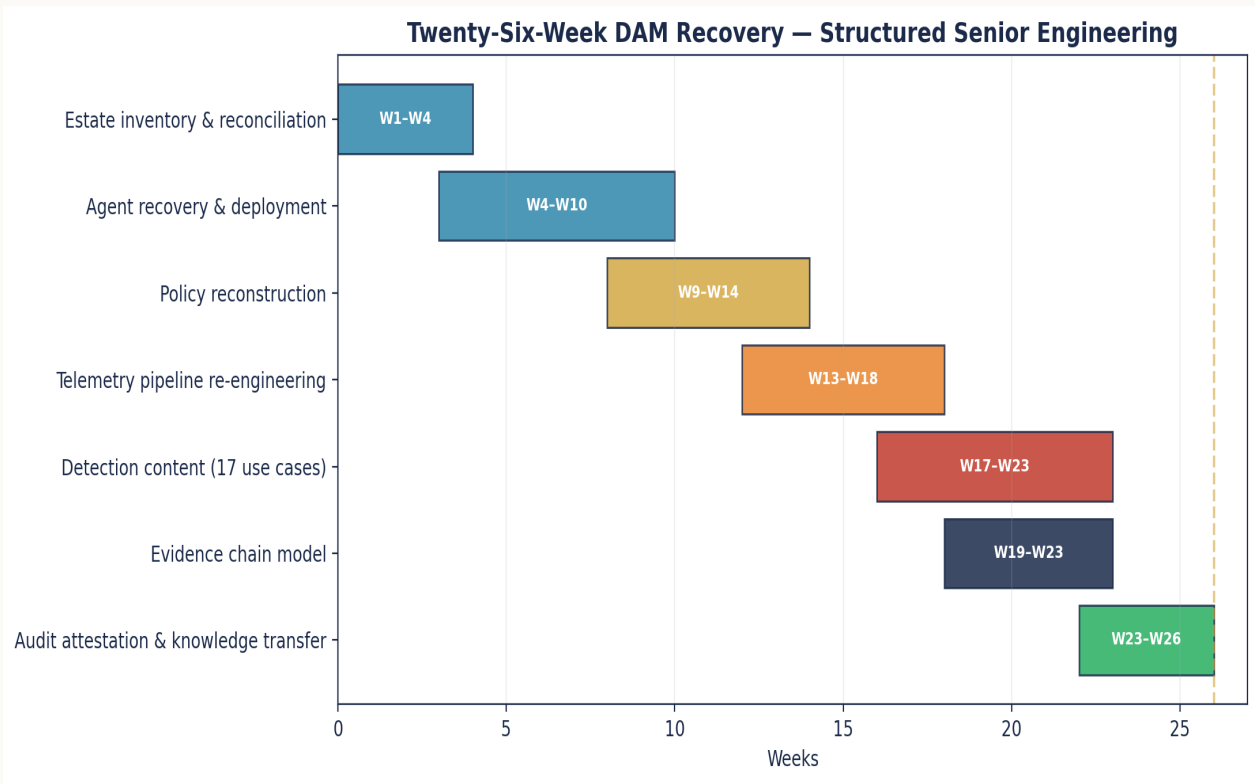
Plan-In-Slide-Deck. Plan exists as a slide; not version-controlled; weekly progress invisible.

No Named Successor. Engagement closes without permanent owner; doctrine reverts.

Backlog-Without-Risk-Ordering. Tickets attacked in arrival order; highest-risk items deferred to week 20.

Single-Engineer Lifeline. Single contractor; no bus factor; departure mid-engagement is catastrophic.

Diagnostic Chart — Recovery Gantt



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 **Structured Recovery**. 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 |
|----------------------|----------------------------|---------------------|
| Gantt-as-Code | Engagement plan in Git | engagement-plan.git |
| Gate W4 | Diagnostic baseline signed | gate W4 record |
| Gate W12 | Engineer + tabletop pass | gate W12 record |
| Gate W20 | Quarterly pack regen pass | gate W20 record |
| Gate W26 | Board attest + handover | gate W26 record |
| Bus Factor | ≥2 on every critical path | succession map |

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 |
|--------------------------------------|--|
| ✗ Engagement plan in slides, not Git | ✓ Engagement Gantt in Git, weekly velocity |
| ✗ No acceptance gates | ✓ Acceptance gates at weeks 4/12/20/26 |
| ✗ Successor identified at week 22 | ✓ Successor named at week 1, ready by W22 |
| ✗ Risk-ordered backlog absent | ✓ Risk-ordered backlog, signed by 2LoD |
| ✗ Single-engineer dependency | ✓ Bus-factor ≥ 2 on every critical path |

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 Bank — 26-Week Recovery

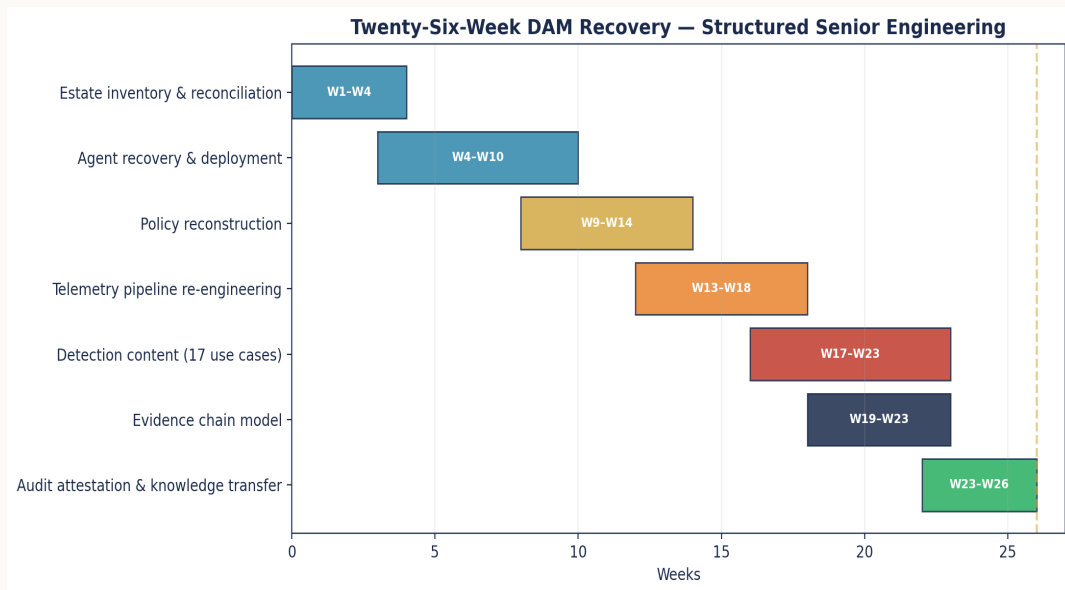
26-week structured engagement. Outcomes: 100% regulated database to agent reconciliation, 17 detection use cases live, 3 internal audit findings closed, Evidence Chain Model deployed. Day-rate cost: £600. Total: £78,000.

ILLUSTRATIVE SCENARIO

European Insurer — Phased Knowledge Transfer

Recovery engagement structured with explicit knowledge transfer in weeks 18-26. Internal team takes ownership; external dependency reduced to quarterly review cadence.

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 (**Structured Recovery**) and the doctrine artefact that satisfies it in evidence.

| Regime | Clause | This paper's obligation | Doctrine artefact |
|--------------------|-------------------------------|-------------------------------------|--|
| DORA Art. 6 | ICT risk management framework | Engagement plan in version control | Gantt-as-code in Git + weekly velocity |
| UK PRA SS2/21 | ICT third-party arrangements | Acceptance gates W4/W12/W20/W26 | Gate sign-off records |
| NIS2 Art. 21(2)(d) | Logging & monitoring | Successor readiness green by W22 | Bi-weekly readiness review |
| DORA Art. 11 | Response & recovery | Gate slippage = 0 weeks | Engagement log, weekly |
| UK FCA SYSC 8 | Outsourcing | Risk-ordered backlog signed by 2LoD | Backlog record + 2LoD sign-off |

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.

26-week engagement plan — Gantt as code

Mermaid Gantt

```
gantt
  title 26-Week DAM Estate Turnaround
  dateFormat YYYY-MM-DD
  axisFormat %b-%d

  section Diagnose (W1-W4)
  Discovery + coverage map      :done, d1, 2025-01-06, 14d
  Health baseline + SLA       :done, d2, 2025-01-13, 14d
  Policy git lift              :done, d3, 2025-01-20, 14d
  Risk-ordered backlog         :crit, d4, 2025-01-27, 7d

  section Stabilise (W5-W12)
  Coverage to 99%             :s1, 2025-02-03, 28d
  Health stream to SIEM       :s2, 2025-02-17, 14d
  Top-8 use cases             :s3, 2025-03-03, 28d
  Tabletop drill               :s4, 2025-03-17, 14d

  section Engineer (W13-W20)
  PAM-DAM correlation          :e1, 2025-04-07, 28d
  Continuous attest scripts    :e2, 2025-04-21, 28d
  Chain-of-custody verifier    :e3, 2025-05-05, 14d

  section Embed (W21-W26)
  Quarterly evidence pack      :em1, 2025-05-19, 21d
  Independent red-team         :em2, 2025-06-02, 14d
  Board attestation            :em3, 2025-06-16, 7d
  Handover to successor        :em4, 2025-06-23, 7d
```


Engineer's note — Engagement plan as code, in version control, reviewed weekly. The Gantt is the contract; the gates are 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 | Week-4 gate slip | PM platform | gate_4 != PASS | 24h |
| 2 | Week-12 gate slip | PM platform | gate_12 != PASS | 24h |
| 3 | Week-20 gate slip | PM platform | gate_20 != PASS | 24h |
| 4 | Week-26 gate slip | PM platform | gate_26 != PASS | 24h |
| 5 | Weekly velocity below plan | Burn-down chart | velocity < plan | 7 days |
| 6 | Successor readiness regression | Readiness review | readiness < green by W22 | 7 days |
| 7 | Gate slippage > 0 weeks | Engagement log | slip > 0 | 24h |
| 8 | Risk-ordered backlog drift | Backlog audit | order changed without 2LoD sign-off | 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 | Week-4 gate pass | 100% | Per engagement | CISO | Acceptance sign-off |
| 2 | Week-12 gate pass | 100% | Per engagement | CISO | Acceptance sign-off |
| 3 | Week-20 gate pass | 100% | Per engagement | CISO | Acceptance sign-off |
| 4 | Week-26 gate pass | 100% | Per engagement | CISO | Acceptance sign-off |
| 5 | Weekly velocity (tickets closed) | ≥ plan | Weekly | PM | Burn-down chart |
| 6 | Successor readiness | Green by W22 | Bi-weekly | CISO | Readiness review |
| 7 | Gate slippage | 0 weeks | Per gate | PM | Engagement log |

Common Pitfalls & Boardroom Questions

Pitfalls specific to the frame of this paper:

Time-and-materials drift. Without gates, T&M; drifts.

Procurement gate-blind. Procurement selecting on rate without gates buys hours, not outcomes.

Successor identified late. Week 22 is too late; successor identified at week 1.

Engineering plan in slides. Slides cannot be diffed; code can.

Backlog-by-arrival. Risk-order or drift.

Single-engineer dependency. Bus factor matters.

Three boardroom questions:

Show me the Gantt. Is the engagement plan a buildable, version-controlled artefact, and is the institution able to show progress weekly?

What is the next gate? What is the next acceptance gate, what are its named deliverables, and who is the signatory?

Where is the handover risk? Who is the named permanent owner of the doctrine after week 26, 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 |
|-------------------------------------|---|--|
| 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

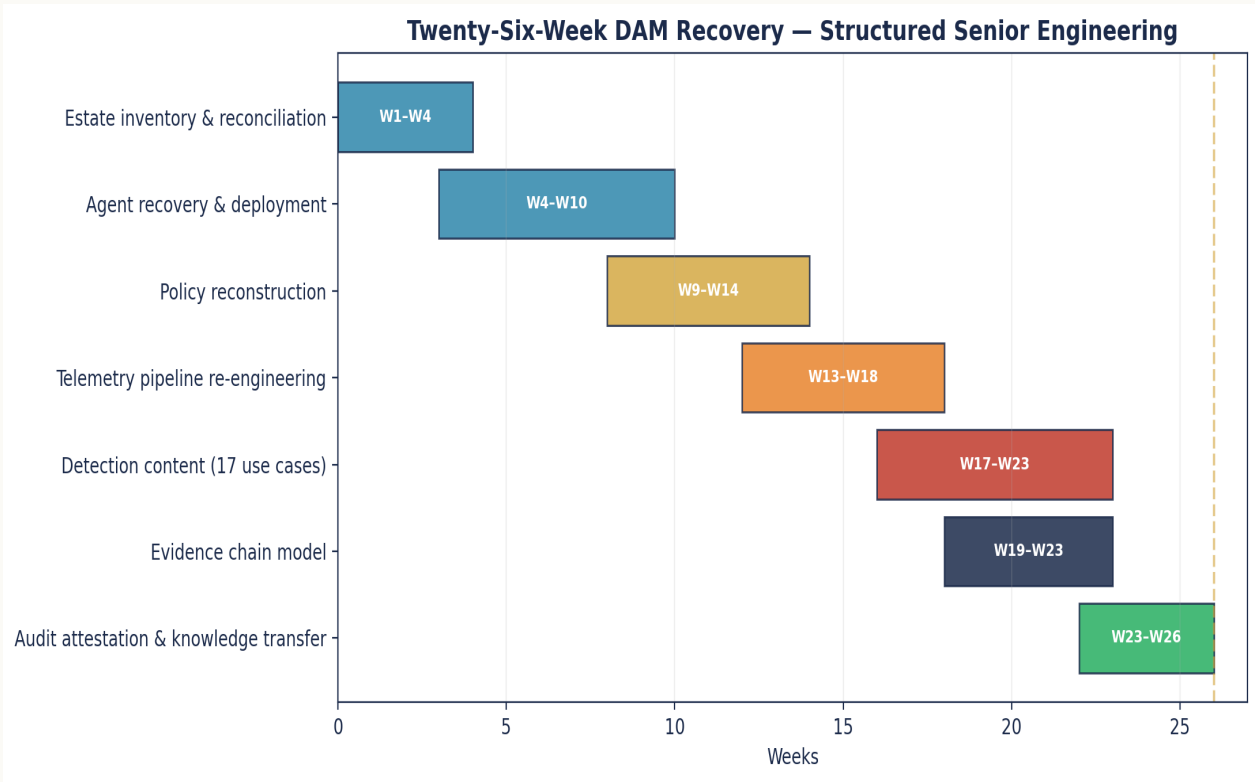
Operating Stack

- 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

- Nova IT Consulting engagement aggregate, 2023–2025
- Doctrine specification
- Calculation, 2025
- EU DORA application — Jan 17, 2025
- UK PRA SS1/21 — 31 March 2025 milestone
- ECB Cyber Resilience Stress Test (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 — Recovery Gantt



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>Why both 26-week and 30/60/90?</i> | Resolved: the generic 30/60/90 section is removed from this paper; only the 26-week four-gate model remains, with acceptance criteria for W4/W12/W20/W26. |
| 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>Is the Gantt usable?</i> | It is Mermaid (version-controllable); a sample weekly burn-down and a risk-ordered backlog example are included. |

Closing Takeaways

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

01. Twenty-six weeks is a doctrine, not a sprint.
02. Acceptance gates are the discipline; the plan is the artefact.
03. Engineering plans belong in version control.
04. The successor is identified at week 1, not week 24.
05. Drift between gates is the leading indicator of engagement failure.
06. Senior engineering compresses 12-month roadmaps into 6 months.
07. Boards should ask for the next gate, not the platform roadmap.
08. Handover is the engagement, not its afterthought.
09. If the engagement does not close with a permanent owner, the doctrine reverts within ninety days.

“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 Six-Month Turnaround — Rescuing Imperva DAM Before It Becomes the Risk

A 26-Week Operational Recovery Plan for Fragile DAM Estates in Financial Services · v5.0 · published May 2026