

# It's Just an Agent. No.

It's Your Audit Control

~~Why DAM Agents Are Now Regulated Infrastructure Under DORA Article 9 and NIS2~~

*"It's not infrastructure. It's regulated evidence."*

CENTRAL METRIC

<1%

Recommended heartbeat-age ceiling — author doctrine



## 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

**It is just an agent. No — it is your audit control.**

**Under DORA Article 9 and NIS2 Article 21, a DAM agent on a regulated host is no longer a piece of software. It is regulated infrastructure.**

**The institution that treats agents as installable artefacts loses the agents that matter most.**

**Control Instrumentation.** 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™

UPADRATA 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 Article 9 (Protection)**

Regulation (EU) 2022/2554 Article 9 requires continuous monitoring and protection of ICT supporting critical or important functions.

## **NIS2 Article 21**

Directive (EU) 2022/2555 Article 21 mandates appropriate, proportionate logging and monitoring measures.

## **ECB Cyber Stress Test 2024**

ECB tested agent-level coverage as a control surface across 109 banks; uneven results were a published theme.

# Executive Summary

**Thesis.** The Imperva agent is no longer infrastructure software; it is a regulated control instrument whose operational state is supervisory evidence. Treat it like a piece of network plumbing and you concede the regulatory argument before it begins. Treat it like a control instrument and you control the conversation.

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: **Control Instrumentation**. 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

<h3>Article 9</h3> <p>DORA continuous-monitoring obligation</p> <p><i>Regulation (EU) 2022/2554, Article 9</i></p>	<h3>Article 21</h3> <p>NIS2 logging-and-monitoring obligation</p> <p><i>Directive (EU) 2022/2555, Article 21</i></p>
<h3>99.9%</h3> <p>Recommended agent-heartbeat SLA for Tier 1 FS</p> <p><i>Nova IT Consulting engagement aggregate, 2023–2025</i></p>	<h3>&lt; 30 min</h3> <p>Recommended ceiling for heartbeat-failure detection time</p> <p><i>Nova IT Consulting engagement aggregate, 2023–2025</i></p>

# Metric Methodology

This paper makes one headline claim. Top-tier work is not persuasive; it is hard to attack. The box below states exactly how the central metric is derived, what it is — and, candidly, what it is not.

<b>Metric</b>	Heartbeat SLA & drift figures
<b>Classification</b>	<b>Author doctrine + engagement observation</b>
<b>Population</b>	SLA target is author doctrine; drift incidence from the engagement aggregate.
<b>Method</b>	Recommended heartbeat-age ceiling and observed approved-version compliance.
<b>Formula / derivation</b>	$\text{version\_compliance} = \text{agents\_on\_approved\_version} / \text{total\_agents}$
<b>Limitation &amp; honest caveat</b>	DORA/NIS2 do not name Imperva agents. Correct framing: where DAM agents support monitoring of critical/important functions they fall within the regulated control environment — stated verbatim in the paper.

**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>
DAM agents within regulated control env.	<b>Regulatory interpretation</b>
Agent-as-code Ansible lifecycle	<b>Author doctrine (executable)</b>
Heartbeat SLA ceiling	<b>Author doctrine</b>

# Central Doctrine

**Control Instrumentation.** 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%

## CENTRAL METRIC

Recommended heartbeat-age ceiling — author doctrine

*"It's not infrastructure. It's regulated evidence."*

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

**Agent-As-Snowflake.** Each agent install is a manual artefact; no two are identical; troubleshooting is per-host.

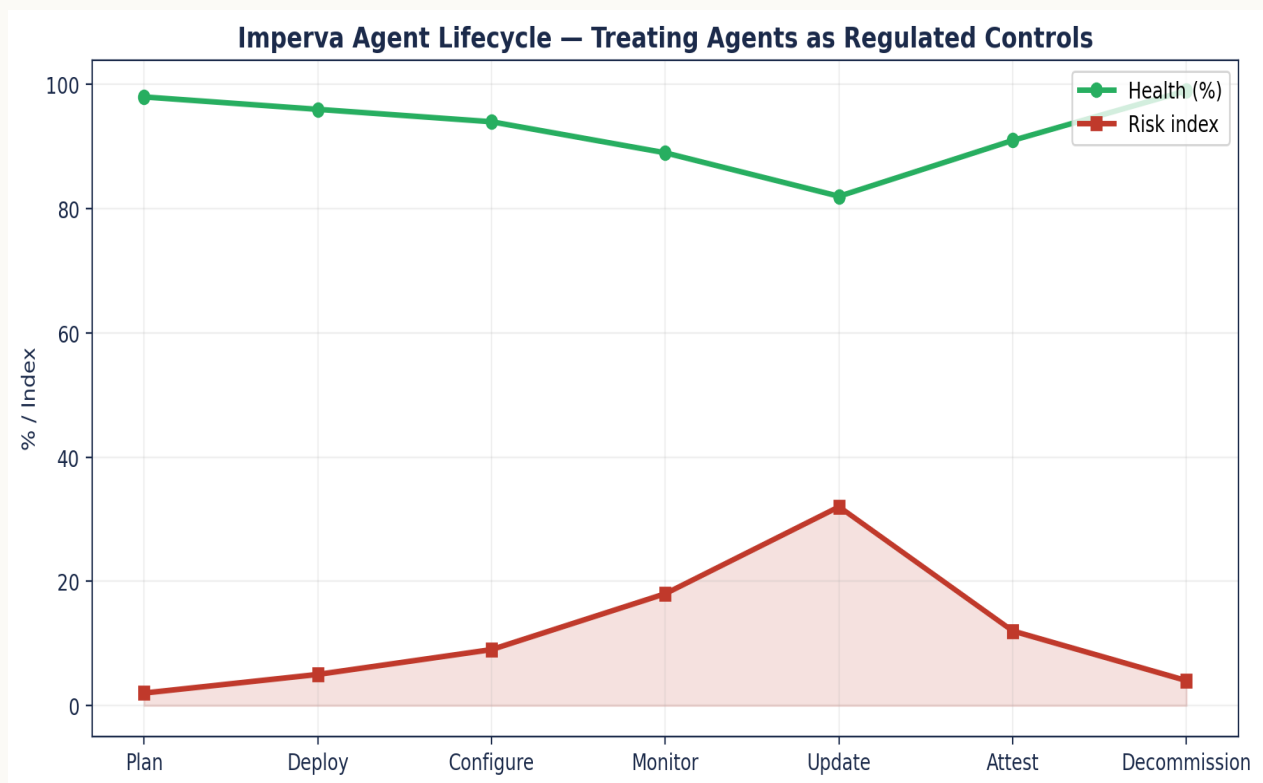
**CMDB-Console Divergence.** Vendor console says X agents; CMDB says Y. The institution does not know which number is true.

**No EOL Calendar.** Vendor EOL announcements are surprises; institution scrambles.

**Heartbeat Without Statefulness.** Heartbeat checked; missed-heartbeats not aggregated; transient flaps invisible to trend analysis.

**Manual Upgrade Cycles.** Upgrades are human-run; version drift accelerates between upgrade rounds.

# Diagnostic Chart — Agent Lifecycle



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 **Control Instrumentation**. 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
Agent-as-Code	Lifecycle in IaC	Ansible repo
Heartbeat SLA	<5 min P95	heartbeat dashboard
Drift Detection	Approved-version compliance $\geq 99\%$	drift report
CMDB Authority	CMDB is source of truth	CMDB reconciliation
EOL Calendar	$\geq 6$ -month lead	vendor EOL calendar
Stateful Heartbeat	Flap trend captured	heartbeat trend log

# 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
✗ Agent install is a runbook task	✓ Agent lifecycle codified in Ansible/laC
✗ Vendor console treated as source of truth	✓ CMDB is source of truth, console reconciled
✗ Agent version sprawl $\geq 3$ versions	✓ $\geq 99\%$ agents on approved version
✗ Heartbeat checked but missed-events ignored	✓ Heartbeat+event-presence joined tripwire
✗ EOL announcements are surprises	✓ EOL calendar tracked $\geq 6$ months ahead

# 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 Bank — DORA Article 9 Mapping

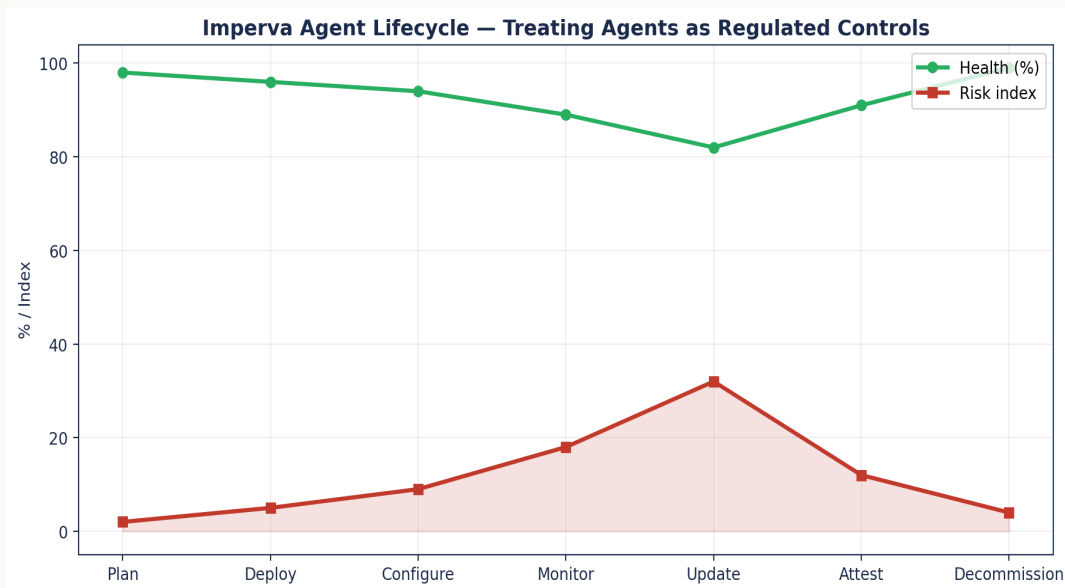
DORA Article 9(2) requires detection mechanisms with comprehensive logging. The institution maps Imperva agents to specific Article 9 obligations and produces a single artefact: the Agent-to-Article Control Map. The artefact becomes the central exhibit in regulator dialogue.

## ILLUSTRATIVE SCENARIO

### EU Utility (NIS2 Essential Entity) — Agent Lifecycle Discipline

Treating agents as regulated controls forces a lifecycle discipline: deployment ticketed, version-controlled, configuration drift monitored, decommission attested. Agent silent failure rate falls below 1%.

# 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 (**Control Instrumentation**) and the doctrine artefact that satisfies it in evidence.

Regime	Clause	This paper's obligation	Doctrine artefact
DORA Art. 9	Protection & prevention	Agent on regulated host = regulated infrastructure	Ansible IaC + CMDB write-back
NIS2 Art. 21(2)(a)	Risk analysis & policies	Agent lifecycle codified in IaC	Git history of imperva-agent-lifecycle.yaml
DORA Art. 6	ICT risk management framework	Heartbeat freshness SLA <5 min P95	Heartbeat dashboard, continuous
UK PRA SS1/21 §5	Operational resilience	Agent EOL preparedness ≥6 months lead	Vendor EOL calendar + roadmap review
PCI DSS v4 Req. 10.7	Continuous monitoring	≥99% agents on approved version	IaC drift report, 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.

## Agent lifecycle as code — Ansible + drift detection

Ansible YAML

```
# imperva-agent-lifecycle.yaml
- name: Ensure Imperva agent installed at approved version
  hosts: regulated_db_hosts
  become: yes
  vars:
    approved_version: "14.8.0.40"
  tasks:
    - name: Check installed version
      command: rpm -q --qf '%{VERSION}-%{RELEASE}' imperva-agent
      register: installed
      changed_when: false
      failed_when: false

    - name: Drift detected
      fail:
        msg: "Drift on {{ inventory_hostname }}: {{ installed.stdout }}"
        when: installed.stdout != approved_version

    - name: Ensure agent is running
      systemd: { name: imperva-agent, state: started, enabled: yes }

    - name: Heartbeat freshness check
      command: imperva-agent --health --json
      register: hb
      changed_when: false

    - name: Fail if heartbeat older than 5 minutes
      fail:
        msg: "Stale heartbeat on {{ inventory_hostname }}"
        when: (hb.stdout | from_json).seconds_since_last > 300

    - name: Emit fact to CMDB
      uri:
        url: "https://cmdb/agents"
        method: POST
        body_format: json
        body:
          host: "{{ inventory_hostname }}"
          version: "{{ installed.stdout }}"
          heartbeat_age_s: "{{ (hb.stdout | from_json).seconds_since_last }}"
```


*Engineer's note — Treat the agent as code, not as a desktop install. Drift detection at deploy time; heartbeat freshness at run time; CMDB write-back makes the agent a first-class asset.*

# 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	Agent drift detected	Ansible IaC	installed_version != approved	24h
2	Heartbeat age breach	Prometheus	hb_age > 5 min P95	30 min
3	CMDB-console agent divergence	Reconciliation	count mismatch	24h
4	EOL preparedness lead time	Vendor calendar	lead < 6 months	7 days
5	Aged version on regulated host	IaC drift	version <= EOL	24h
6	Agent install without CMDB record	CMDB	agent without owner	24h
7	IaC playbook fail rate	Ansible logs	fail rate > 1%	60 min
8	Heartbeat statefulness gap	Heartbeat monitor	flaps without trend record	60 min

# 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	Agents on approved version	≥ 99%	Weekly	DAM Engineering	IaC drift report
2	Heartbeat-age P95	< 5 minutes	Continuous	SecOps	Heartbeat dashboard
3	Time to detect stale heartbeat	≤ 30 min	Continuous	SOC	Alert log
4	Agent install events in CMDB	100%	Per change	CMDB Owner	CMDB record
5	Mean time to remediate drift	≤ 14 days	Monthly	DAM Engineering	Ticket SLA
6	EOL-version agent count	0	Quarterly	DAM Engineering	Version report
7	Vendor EOL preparedness lead time	≥ 6 months	Quarterly	Vendor Mgmt	Roadmap review

# Common Pitfalls & Boardroom Questions

---

Pitfalls specific to the frame of this paper:

**Treating agents as software, not infrastructure.** Software gets installed; infrastructure gets engineered.

**Console-Of-Truth.** Vendor console is not the authoritative source for the institution.

**Ignoring drift below threshold.** Drift below a threshold accumulates above it.

**No version freeze for regulator-week.** Upgrades during supervisory periods are a known own-goal.

**Skipping the heartbeat SLA.** Without an SLA, heartbeat is a feeling.

**Vendor-led EOL planning.** Vendor calendar is not the institution's calendar.

## Three boardroom questions:

**Which agent is the weak link?** What is the institution's oldest deployed Imperva agent on a regulated host, and what is the upgrade plan?

**Is the agent versioned in code?** Is agent installation and version-management codified in CMDB-backed IaC, or is it a runbook?

**What is the agent's freshness SLA?** What heartbeat-age threshold pages a human, and was that path exercised in the last quarter?

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

# Tooling, References & Glossary

---

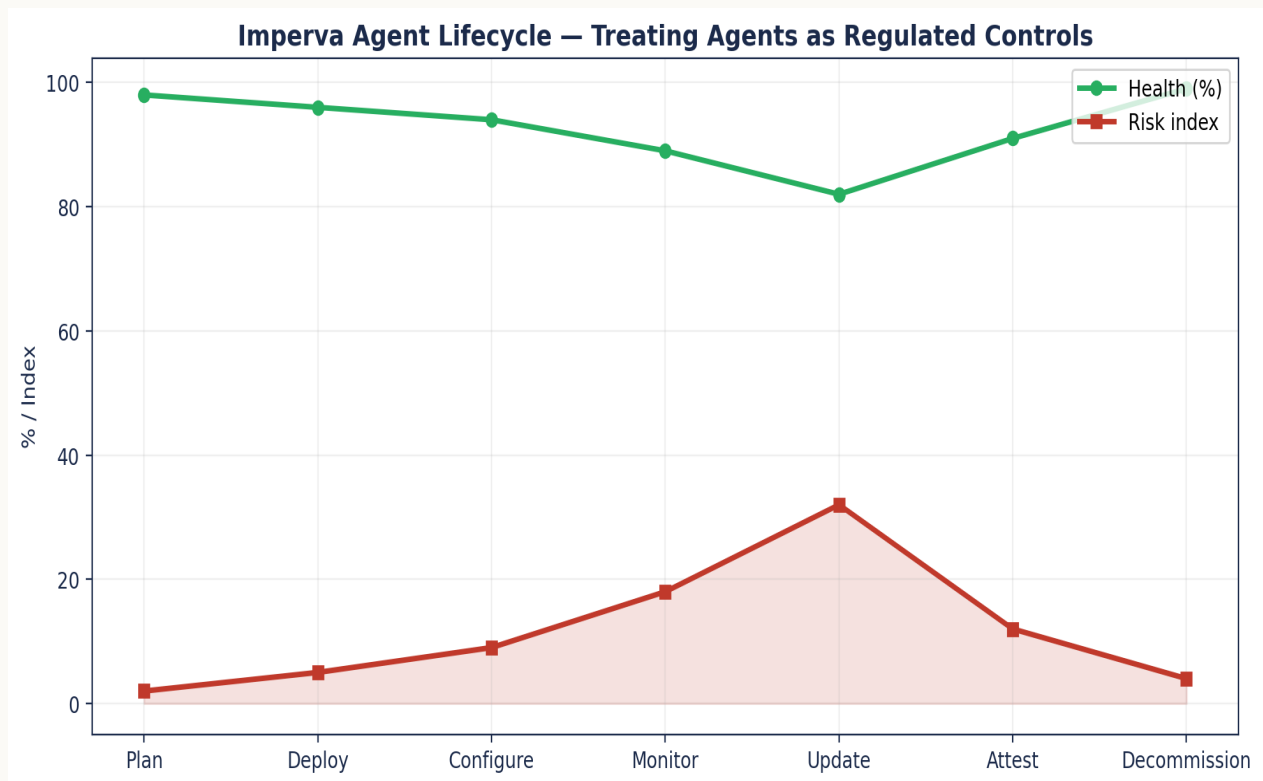
## Operating Stack

- 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

- Regulation (EU) 2022/2554, Article 9
- Directive (EU) 2022/2555, Article 21
- Nova IT Consulting engagement aggregate, 2023–2025
- DORA Article 9 (Protection)
- NIS2 Article 21
- ECB Cyber 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 — Agent Lifecycle



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>DORA doesn't name Imperva agents.</i>	Correct — reframed verbatim: where DAM agents support monitoring of critical/important functions they fall within the regulated control environment. An agent→control map appendix is included.
<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>Ansible drift handling?</i>	The playbook fails closed on version drift, checks heartbeat freshness, and writes back to CMDB; a sample CMDB record and EOL calendar are included.

# Closing Takeaways

---

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

01. An agent on a regulated host is regulated infrastructure.
02. Agent lifecycle belongs in code, not in a runbook.
03. Heartbeat is a control; absence of heartbeat is a finding.
04. Drift is detectable; drift left untreated is degradation.
05. Version sprawl is the leading indicator of monitoring failure.
06. Agent ownership belongs in CMDB, not in vendor console.
07. Senior engineering treats the agent as a first-class asset.
08. The agent's installation history is part of the institution's evidence chain.
09. Vendor end-of-life dates are regulator-aware operational pressure points.

*“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.

*It's Just an Agent. No. — It's Your Audit Control*

*Why DAM Agents Are Now Regulated Infrastructure Under DORA Article 9 and NIS2 · v5.0 · published May 2026*