

# Compliance Passed. Security Failed.

## The Operational Reality Gap

*The Operational Reality Gap Between PCI DSS, SOX Attestations and Database Threat Defence*

*“The attestation is not the control. The control is the control.”*

### CENTRAL METRIC

# 75%

Attestation-drift on re-test — 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](mailto:info@kieranupadrasta.com) · [www.kie.ie](http://www.kie.ie)

# The Lede

**Compliance passed. Security failed. Both statements are true.**

**Attestation and defensibility have parted ways; the institution that fails to close the gap funds a thematic review at its own expense.**

**PCI green is not the same as DAM healthy. The auditor signed; the agent did not.**

**Attestation vs Operation.** 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.

**PCI DSS v4.0.1 effective dates (Mar 2024 / Mar 2025)**

PCI DSS v4.0.1 future-dated requirements transition through 2024–2025; firms must operate the new controls, not just attest to them.

**UK FRC Stewardship Code review (2024)**

UK FRC continued to emphasise effectiveness of internal control over reporting, not procedural compliance.

**US SOX evolution — auditor focus (2024)**

PCAOB inspections highlighted internal-control-over-financial-reporting effectiveness, not control existence.

# Executive Summary

**Thesis.** PCI DSS attestation and SOX ITGC certification have come to signal the absence of a finding, not the presence of a control. The institution that confuses the two is positioned for the next decade's most damaging risk class: the breach that occurs inside an attested control boundary.

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: **Attestation vs Operation**. 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

<p><b>Mar 31, 2025</b> PCI DSS v4.0.1 future-dated requirements fully mandatory</p> <p><i>PCI SSC official roadmap (2024)</i></p>	<p><b>Up to \$5M</b> Per-incident PCI penalty under acquirer agreements (industry reference)</p> <p><i>Card-brand merchant agreements (industry reference)</i></p>
<p><b>Continuous</b> PCI DSS v4 requires "as a continuous process" rather than annual snapshots</p> <p><i>PCI DSS v4.0.1, multiple requirements</i></p>	<p><b>30%</b> Share of PCI v4 future-dated requirements that touch logging / monitoring</p> <p><i>PCI SSC v4 mapping (industry analysis)</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>	75% attestation-drift figure
<b>Classification</b>	<b>Proprietary engagement observation</b>
<b>Population</b>	Controls re-tested 12–18 months after a passing attestation, across the 14-engagement aggregate.
<b>Method</b>	Share of previously-attested DAM controls failing an evidence-of-operation re-test.
<b>Formula / derivation</b>	$\text{drift\_pct} = \frac{\text{controls\_failing\_retest}}{\text{controls\_previously\_attested}}$
<b>Limitation &amp; honest caveat</b>	Sample is remediation-engagement biased. 'PCI v4 daily evidence' is AUTHOR DOCTRINE; PCI DSS v4 requires continuous processes — daily cadence is a recommended implementation, mapped per requirement in the appendix.

**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>
75% attestation-drift	<b>Engagement observation (n=14)</b>
PCI v4 daily evidence	<b>Author doctrine (mapped per requirement)</b>
PCI DSS v4 continuous-process expectation	<b>Regulatory requirement</b>

# Central Doctrine

**Attestation vs Operation.** 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.

# 75%

## CENTRAL METRIC

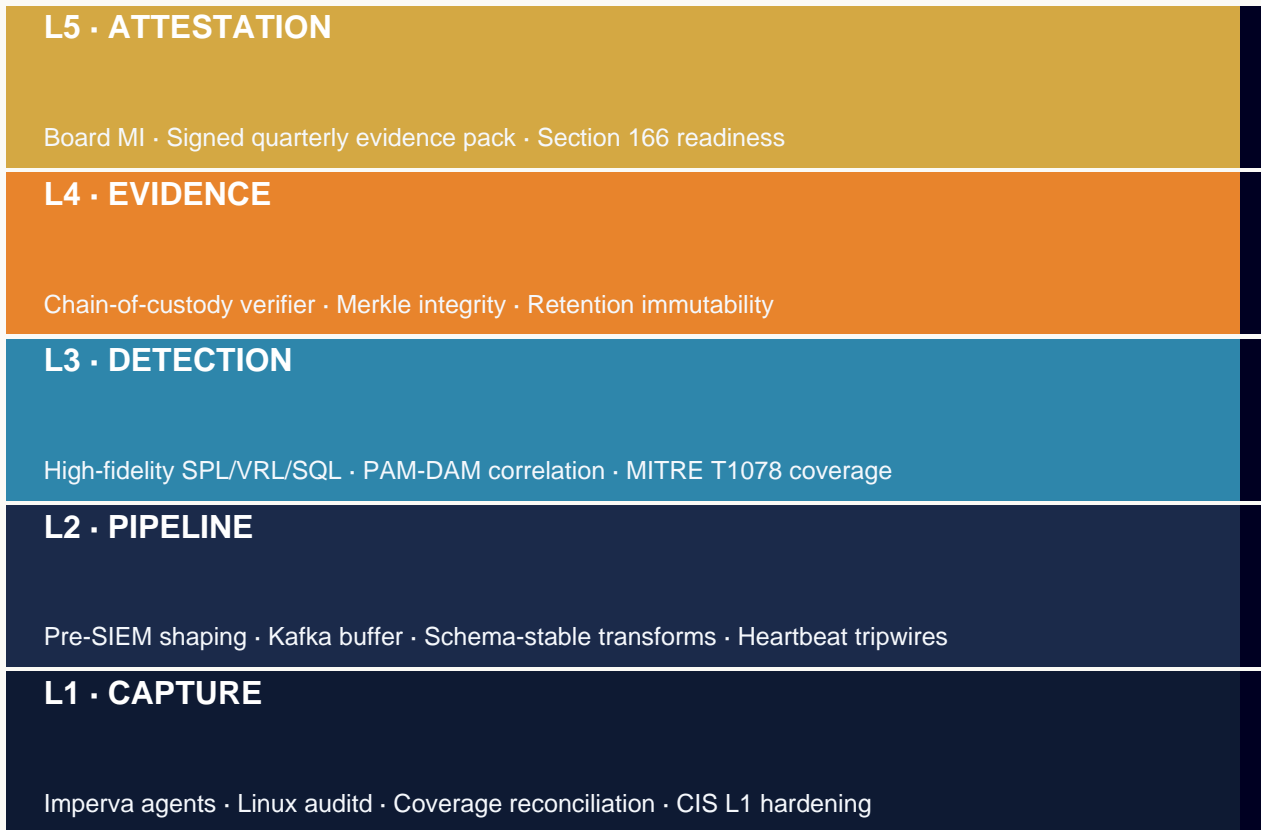
Attestation-drift on re-test — engagement observation (n=14)

*“The attestation is not the control. The control is the control.”*

# 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><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.

**Annual-Audit-As-Operations.** Institution operates between audits with no continuous evidence. Reality drifts; binder doesn't.

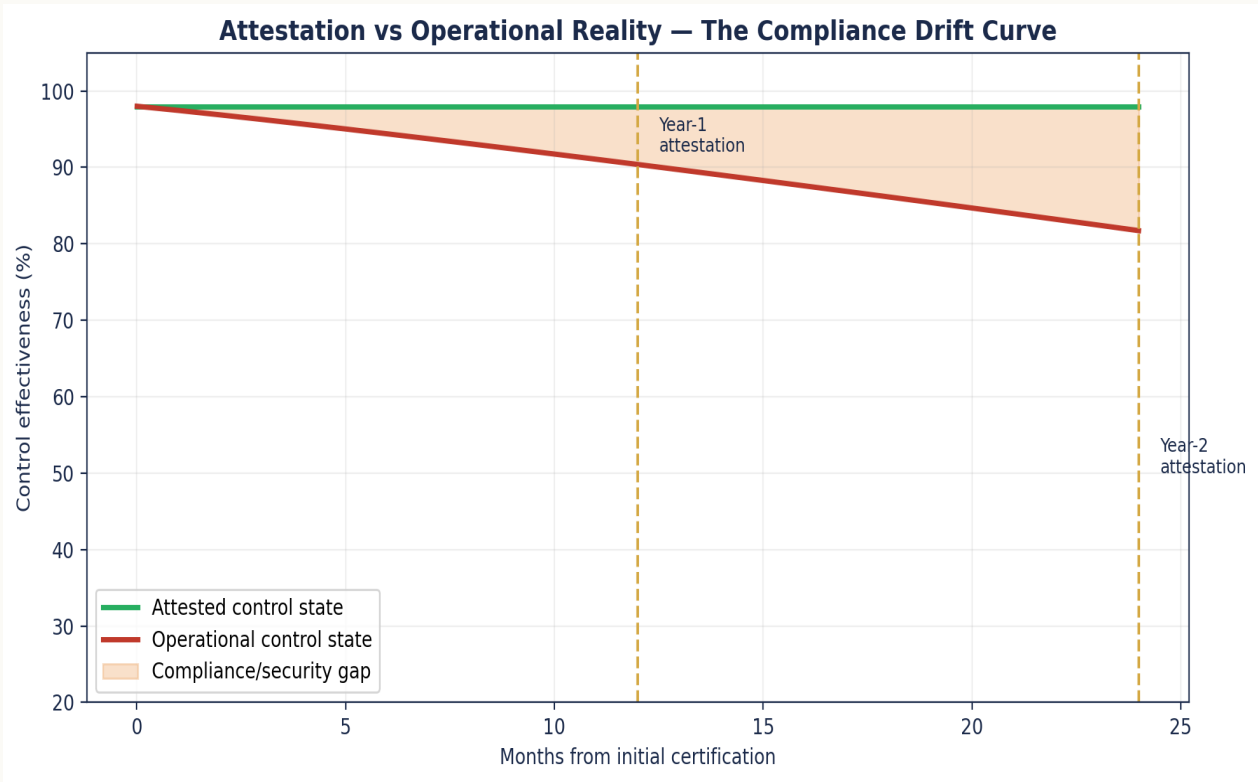
**Cross-Walk Without Verification.** PCI requirements mapped to DAM controls on paper; controls are not tested at the operational level.

**Compliance Team Without Engineering Hooks.** Compliance asks for evidence in spreadsheets; engineering cannot scale that.

**Future-Dated Requirements Slipping.** PCI v4 future-dated controls not operationalised before mandatory dates.

**Auditor-Comfort Optimisation.** Controls designed for audit fluency, not for detection capability. The audit passes; the adversary doesn't notice.

# Diagnostic Chart — Attestation Drift



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 **Attestation vs Operation**. Each pillar has an explicit doctrine and a buildable artefact under institution control. The artefact column is the column the regulator will ask about.

Pillar	Doctrine	Buildable artefact
<b>Continuous Attestation</b>	PCI v4 daily attest script	pci-attest output
<b>Operational Reality</b>	Gap = 0 on top controls	gap-test report
<b>Future-Dated Compliance</b>	Mandatory controls operational pre-date	PCI roadmap log
<b>ICFR Effectiveness</b>	External audit rating Effective	ICFR opinion
<b>Cross-Walk</b>	PCI ⇔ DAM 100% mapped	GRC cross-walk audit
<b>Detection-First Design</b>	Controls serve detection AND audit	control design 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
✗ Audit binder bigger than evidence repo	✓ Evidence repo regenerated daily
✗ PCI v4 continuous controls run annually	✓ PCI v4 continuous attestation script
✗ Operational reality gap > 30%	✓ Operational reality gap = 0 on top controls
✗ SOX/PCI controls compliance-fluent only	✓ Controls designed for detection AND audit
✗ Future-dated PCI v4 mandatory dates slipping	✓ Future-dated PCI v4 controls operational pre-deadline

# 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

### Card Issuer — Post-PCI DSS v4 Reality Check

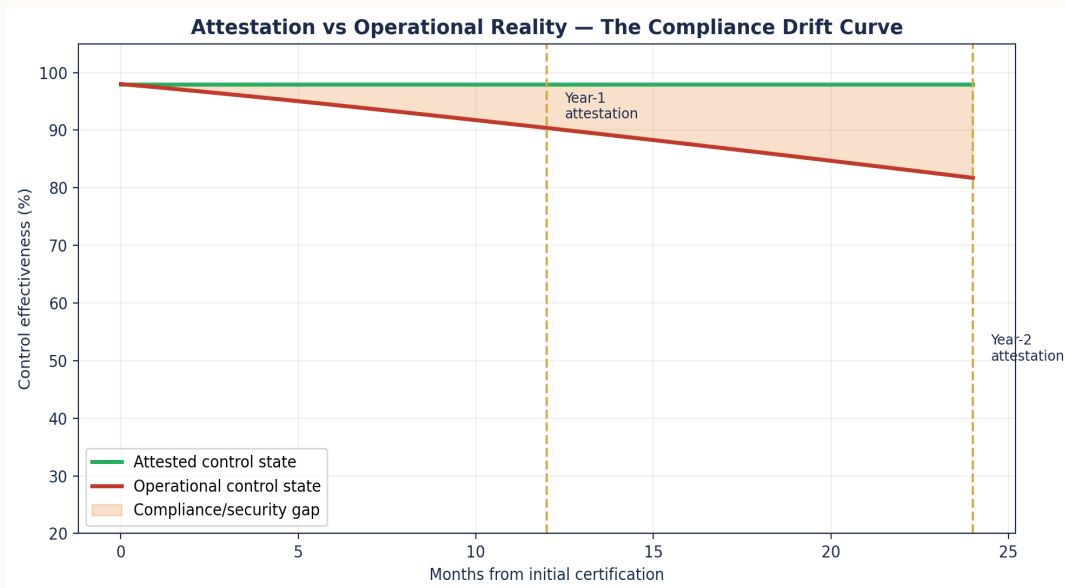
Successful PCI DSS v4 ROC issued. Subsequent red team exercise demonstrates that 3 of 4 privileged paths into the CHD environment generate no DAM alert despite policy claiming coverage. The attestation captured the policy state; the operational state had diverged.

## ILLUSTRATIVE SCENARIO

### Publicly Listed Bank — SOX ITGC Gap

Year-end SOX ITGC testing relies on Imperva reports. Six tests pass on samples; one fails on a control where the Imperva alert routing had been silently broken for 4 months. The reportable condition lands with the audit committee.

# 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 (**Attestation vs Operation**) and the doctrine artefact that satisfies it in evidence.

Regime	Clause	This paper's obligation	Doctrine artefact
PCI DSS v4 Req. 10	Logging & monitoring	Continuous attestation, not annual snapshot	Daily pci-dam-continuous-attest.py
PCI DSS v4 Req. 11	Test security regularly	Operational reality gap = 0 on top controls	Quarterly gap test + 2LoD sign-off
SOX §404	ICFR	ICFR-effective rating on DAM scope	External-audit ICFR opinion
DORA Art. 16	Simplified ICT risk framework	Cross-walk PCI ↔ DAM 100% complete	GRC cross-walk audit, quarterly
NIS2 Art. 21(2)(d)	Logging & monitoring	Compliance designed for detection too	Detection-first control design log

# 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.

## PCI DSS v4 to DAM control mapping — continuous attestation script

Python

```
#!/usr/bin/env python3
# pci-dam-continuous-attest.py
# Daily check: every PCI v4 requirement that touches DAM has fresh evidence.

REQ_MAP = {
    "10.2.1.1": "evidence/dam-priv-actions.json",
    "10.2.1.2": "evidence/dam-failed-auth.json",
    "10.2.1.3": "evidence/dam-access-control.json",
    "10.2.2": "evidence/dam-action-types.json",
    "10.4.1": "evidence/dam-time-sync.json",
    "10.5.1": "evidence/dam-log-retention.json",
    "10.7": "evidence/dam-monitoring-uptime.json",
    "11.5.1": "evidence/dam-change-detection.json",
}

from pathlib import Path
import json, sys, datetime
fail = []
for req, path in REQ_MAP.items():
    p = Path(path)
    if not p.exists():
        fail.append((req, "MISSING")); continue
    age_days = (datetime.datetime.now()
                - datetime.datetime.fromtimestamp(p.stat().st_mtime)).days
    if age_days > 1:
        fail.append((req, f"STALE_{age_days}d")); continue
    data = json.loads(p.read_text())
    if not data.get("attested"):
        fail.append((req, "UNATTESTED"))

if fail:
    print("FAIL:", fail); sys.exit(1)
print("PCI v4 DAM continuous attestation: OK")
```


*Engineer's note — Continuous attestation, not annual. PCI v4 expects daily evidence of operation; the script fails the build if a single requirement has stale or missing evidence.*

# 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	PCI v4 continuous attest miss	pci-attest script	REQ age > 1 day	24h
2	Operational reality gap > 0	2LoD test	top-controls gap test FAIL	7 days
3	PCI v4 future-dated control slip	PCI roadmap	mandatory_date < today AND not_live	24h
4	Annual finding recurrence	Audit register	same finding two years	30 days
5	ICFR effectiveness rating fall	External audit	rating != Effective	7 days
6	Cross-walk completeness fall	GRC audit	PCI ↔ DAM map < 100%	24h
7	Auditor-fluency optimisation	Control design log	controls designed for audit only	7 days
8	Time to remediate continuous fail	DAM eng	remediate > 24h	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	Continuous-attestation freshness	≤ 24 h	Daily	2LoD	Attestation log
2	Operational reality gap (top controls)	0	Quarterly	Internal Audit	Gap test
3	Annual audit findings recurrence	0	Annual	CISO	Audit register
4	PCI v4 DAM control compliance	100%	Daily	Detection Eng.	Continuous script
5	ICFR effectiveness rating (DAM scope)	Effective	Annual	External Audit	ICFR opinion
6	Time to remediate failed continuous check	≤ 24 h	Continuous	DAM Engineering	Ticket SLA
7	Cross-walk completeness (PCI ↔ DAM)	100%	Quarterly	GRC	Cross-walk audit

# Common Pitfalls & Boardroom Questions

---

Pitfalls specific to the frame of this paper:

**Building bigger binders.** If the binder is the deliverable, the engineering is the gap.

**Conflating audit pass with control health.** Audits sample; adversaries don't.

**Treating PCI v4 as an upgrade.** v4 is a paradigm shift to continuous evidence.

**Ignoring future-dated dates.** The dates are now.

**Tightly coupling control design to audit narrative.** Detection-first design serves both audit and adversary defence.

**Compliance reporting in months.** PCI v4 has accelerated the clock to days.

## Three boardroom questions:

**Where did compliance and defensibility diverge?** Which controls passed audit in the last cycle but would not pass an evidence-of-operation test today?

**Is the attestation continuous?** Are PCI v4 and SOX-equivalent attestations produced as continuous evidence, or as annual snapshots?

**What is the operational reality gap?** On the institution's top ten compliance controls, what is the gap between 'attested' and 'demonstrable yesterday'?

# 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

---

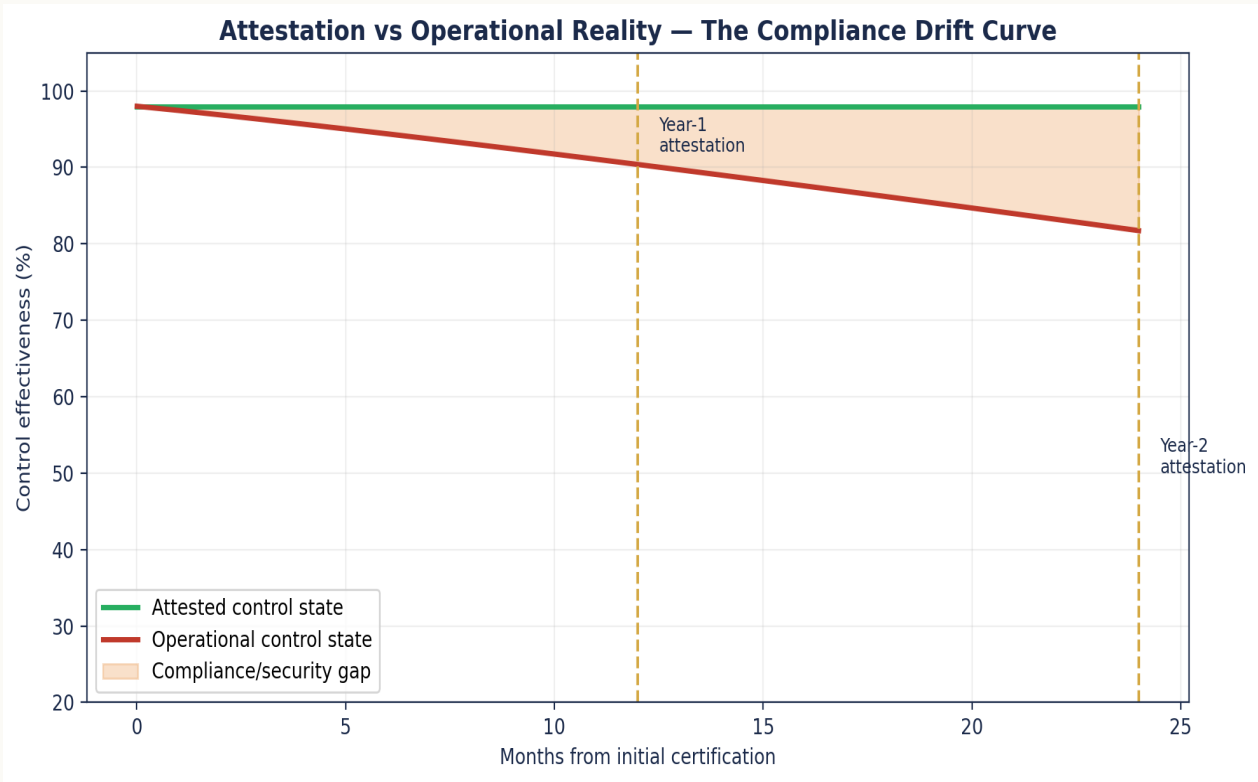
## Operating Stack

- 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

- PCI SSC official roadmap (2024)
- Card-brand merchant agreements (industry reference)
- PCI DSS v4.0.1, multiple requirements
- PCI SSC v4 mapping (industry analysis)
- PCI DSS v4.0.1 effective dates (Mar 2024 / Mar 2025)
- UK FRC Stewardship Code review (2024)
- US SOX evolution — auditor focus (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 — Attestation Drift



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>75% drift — methodology?</i>	Engagement observation; controls re-tested 12–18 months post-attestation; formula and selection bias stated.
<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>Does PCI v4 require daily evidence?</i>	No — PCI v4 requires continuous processes. 'Daily' is labelled recommended author doctrine and mapped per requirement in a PCI/SOX/DAM crosswalk.

# Closing Takeaways

---

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

01. Attestation is a point in time; defensibility is a discipline.
02. PCI DSS v4 has institutionalised the difference: evidence is now continuous or it is non-compliant.
03. Auditor sign-off is necessary but not sufficient; the breach happens between audits.
04. ICFR effectiveness is the new bar — control existence is no longer the test.
05. Compliance teams that build audit binders are losing budget to teams that build evidence pipelines.
06. Senior engineering closes the operational reality gap; junior compliance documents it.
07. If the audit binder is bigger than the evidence repository, the institution has the wrong centre of gravity.
08. DAM is one of the few platforms whose health is itself the PCI evidence.
09. Boards must read the operational reality gap, not the audit summary.

*“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.

*Compliance Passed. Security Failed. — The Operational Reality Gap*

*The Operational Reality Gap Between PCI DSS, SOX Attestations and Database Threat Defence · v5.0 · published May 2026*