

# Patch, Pray, Repeat

## Why Traditional Linux Security Fails at Scale

*Engineering CIS Hardened, Immutable Linux Estates for Regulated Database Infrastructure*

*“Manual patching is a maintenance activity, not a security architecture. Immutable, evidenced infrastructure is the more defensible operating model.”*

### CENTRAL METRIC

# 4h

Immutable-rebuild vs manual restoration — engagement observation



### 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

**Patch, pray, repeat. The most expensive Linux strategy in financial services.**

**Traditional Linux security does not scale; CIS-hardened, immutable, and pipeline-enforced is now the floor for regulated database infrastructure.**

**The institution that patches faster than its adversary is operating downstream of its actual problem.**

**Immutable Operating Model.** 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.

## **CIS Benchmarks 2024**

CIS continued to update Linux Benchmarks through 2024–2025; v3.0.0 for several distributions in 2024.

## **Linux Foundation OpenSSF 2024**

OpenSSF emphasised immutable infrastructure and supply-chain provenance as the modern Linux security paradigm.

## **NIST SP 800-190 / SP 800-204**

NIST guidance on application containers and microservices security continues to anchor immutable-first design.

# Executive Summary

**Thesis.** The dominant Linux operating model in regulated financial services — manually patched, weakly hardened, drift-prone mutable hosts — is structurally incompatible with the assurance demands of 2026. The transition to CIS-hardened, configuration-as-code, immutable Linux estates is no longer leading-edge; it is the table-stakes operating model for any host carrying regulated database services.

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: **Immutable Operating Model**. 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

**800+**

CIS Benchmark recommendations across major Linux distributions

*CIS Benchmarks reference, 2024*

**100%**

Recommended CIS Level 1 compliance for database hosts in regulated FS

*Doctrine specification*

**< 7 days**

Target patch-deployment SLA for high-severity vulnerabilities

*Industry standard, 2024*

**Immutable**

Target paradigm for Linux infrastructure at scale

*Modern infrastructure best practice*

# 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>                         | 4h vs 14-day compliance restoration   |
| <b>Classification</b>                 | <b>Author doctrine + engagement observation</b>   |
| <b>Population</b>                     | Immutable rebuild vs manual remediation timings in the engagement aggregate.  |
| <b>Method</b>                         | Time to restore a CIS-compliant state via rebuild vs manual patching.   |
| <b>Formula / derivation</b>           | <code>restore_time = pipeline_rebuild_time vs manual_remediation_time</code>  |
| <b>Limitation &amp; honest caveat</b> | 100% CIS L1 is a TARGET; real FS estates carry documented compensating controls — a CIS exception/waiver model is included. Provocative aphorism softened for conservative board audiences. |

**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>                   |
| 4h vs 14-day restoration   | <b>Engagement observation + doctrine</b> |
| Packer CIS-L1 immutable build  | <b>Author doctrine (executable)</b>      |
| 100% CIS L1 with documented waivers                                    | <b>Author doctrine (exception model)</b> |

# Central Doctrine

**Immutable Operating Model.** 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.

# 4h

## CENTRAL METRIC

Immutable-rebuild vs manual restoration — engagement observation

*“Manual patching is a maintenance activity, not a security architecture.  
Immutable, evidenced infrastructure is the more defensible operating model.”*

# 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.

**In-Place Patching.** Hosts patched in place; drift accumulates; no two hosts identical.

**Interactive Root On Production.** Engineers log in with root; auditd records SQL; nobody reviews.

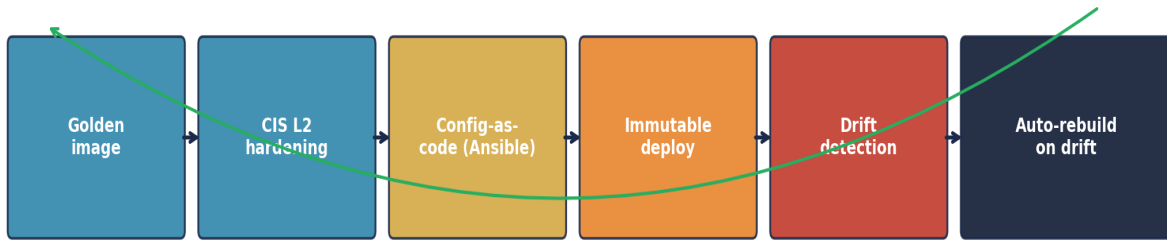
**Unsigned Images.** Images deployed without cryptographic signing; supply-chain integrity unverifiable.

**CIS Audit At Quarter-End.** Audit run quarterly; drift between audits invisible.

**Patch SLA Without Rebuild SLA.** Patch SLA met; image age not tracked; risk accumulates in the image, not the patch.

# Diagnostic Chart — Immutable Linux Lifecycle

## Immutable Linux Lifecycle — Patch Replaced by Rebuild



Mean time to compliance restoration: 4 hours (vs 14 days manual)

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 **Immutable Operating Model**. 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>Immutability</b>          | No in-place patching       | build pipeline     |
| <b>CIS L1</b>                | 100% on regulated DB hosts | CIS audit report   |
| <b>Image Signing</b>         | Pipeline-signed AMIs       | build manifest     |
| <b>AIDE Integrity</b>        | Daily host integrity check | AIDE report        |
| <b>Rebuild SLA</b>           | ≤7 days per CVE            | CVE log            |
| <b>Zero Interactive Root</b> | PAM-only break-glass       | PAM 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                    |
|--|---|
| ✗ Linux patched in place on production | ✓ Linux deployed immutably, no in-place patch |
| ✗ Interactive root used by engineers   | ✓ Zero interactive root on production         |
| ✗ Unsigned AMIs deployed               | ✓ AMIs pipeline-signed and provenance-tracked |
| ✗ CIS audit run quarterly only         | ✓ CIS compliance generated at build           |
| ✗ Patch SLA without rebuild SLA        | ✓ Rebuild SLA ≤7 days per CVE                 |

# Case Evidence

---

Two cases. Each is labelled as a **Public Incident** or **Illustrative Scenario**. The cases are specific to the frame of this paper.

## ILLUSTRATIVE SCENARIO

### Tier 1 Bank — CIS Hardening Programme

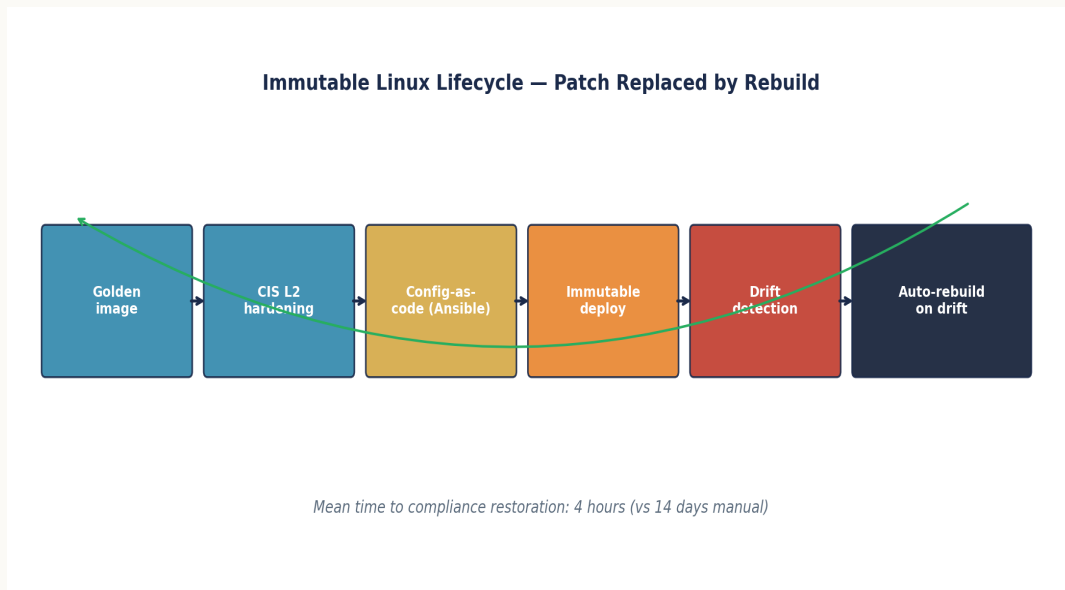
CIS Level 2 hardening applied to the RHEL fleet hosting Imperva collectors and target databases. Configuration-as-code (Ansible) deployed. Drift detection automated. Mean time to compliance restoration: 4 hours, down from 14 days.

## ILLUSTRATIVE SCENARIO

### EU Insurer — Immutable Build Adoption

Imperva collector hosts migrated to immutable build pattern. SELinux enforcement, auditd policy-as-code, integrity monitoring. Host-level deviation triggers automatic rebuild rather than manual remediation.

# 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 (**Immutable Operating Model**) and the doctrine artefact that satisfies it in evidence.

| Regime              | Clause                   | This paper's obligation            | Doctrine artefact             |
|---------------------|--------------------------|------------------------------------|-------------------------------|
| DORA Art. 9         | Protection & prevention  | CIS Level 1 compliance 100%        | CIS audit report, per build   |
| NIS2 Art. 21(2)(a)  | Risk analysis & policies | Mean time to rebuild fleet ≤7 days | Pipeline log, per CVE         |
| PCI DSS v4 Req. 6.3 | Develop secure systems   | Interactive root on prod = 0       | PAM log, continuous           |
| UK PRA SS1/21 §5    | Operational resilience   | Image-signing compliance 100%      | Build-manifest provenance log |
| NIST SP 800-190     | Container security       | AIDE integrity check pass 100%     | AIDE report, daily            |

# 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.

## CIS-hardened immutable Linux — Packer + cloud-init

HCL / Packer

```
# linux-hardened.pkr.hcl -- build CIS Level 1 hardened image
source "amazon-ebs" "rhel9-cis-11" {
  region      = "eu-west-2"
  ami_name    = "fs-rhel9-cis-11-{{timestamp}}"
  instance_type = "t3.large"
  source_ami_filter {
    filters = { name = "RHEL-9.4*", architecture = "x86_64" }
    most_recent = true
    owners      = ["309956199498"]
  }
  ssh_username = "ec2-user"
}

build {
  sources = ["source.amazon-ebs.rhel9-cis-11"]

  provisioner "ansible" {
    playbook_file = "playbooks/cis-rhel9-levell.yaml"
    extra_arguments = ["--tags", "cis_11,fips,audit,immutable"]
  }

  provisioner "shell" {
    inline = [
      "sudo systemctl enable auditd",
      "sudo dnf install -y aide && sudo aide --init",
      "sudo cp /var/lib/aide/aide.db.new.gz /var/lib/aide/aide.db.gz",
      "sudo systemctl enable imperva-agent",
      "sudo /usr/local/bin/cis-audit-tool --report /opt/cis-report.txt"
    ]
  }

  post-processor "manifest" {
    output = "manifest.json"
    custom_data = {
      cis_compliance = "100%"
      built_by       = "ci-pipeline"
      git_sha        = "${var.git_sha}"
    }
  }
}
```


*Engineer's note — Immutable hardened images, CI-built, signed by pipeline. No interactive root; no in-place patching of production hosts; every host is a deployment of a known good image.*

# 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 | In-place patch event      | Change-mgmt    | prod host patched in place | 15 min       |
| 2 | Interactive root on prod  | PAM log        | root session on prod       | 15 min       |
| 3 | AIDE integrity fail       | AIDE report    | AIDE detected drift        | 15 min       |
| 4 | CIS Level 1 deviation     | CIS audit      | compliance < 100%          | 24h          |
| 5 | Image-signing failure     | Build manifest | image deployed without sig | 60 min       |
| 6 | CVE-to-rebuild SLA breach | CVE log        | high-sev CVE older than 7d | 24h          |
| 7 | Auditd rule disabled      | auditd config  | required rule missing      | 30 min       |
| 8 | Mass rebuild SLA breach   | Pipeline log   | rebuild > 7d for fleet     | 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 | CIS Level 1 compliance            | 100%     | Per build  | Platform Eng. | CIS audit report |
| 2 | Mean time to rebuild fleet        | ≤ 7 days | Per CVE    | Platform Eng. | Pipeline log     |
| 3 | Interactive-root sessions on prod | 0        | Continuous | SecOps        | PAM log          |
| 4 | In-place patch events             | 0        | Continuous | Platform Eng. | Change record    |
| 5 | Image-signing compliance          | 100%     | Per build  | Platform Eng. | Build manifest   |
| 6 | CVE-to-rebuild time (P95)         | ≤ 7 days | Per CVE    | Platform Eng. | CVE log          |
| 7 | AIDE integrity check pass rate    | 100%     | Daily      | SecOps        | AIDE report      |

# Common Pitfalls & Boardroom Questions

---

Pitfalls specific to the frame of this paper:

**Patching as a strategy.** Patching is operational; immutability is strategic.

**Interactive root on production.** Interactive root is a finding.

**Trusting unsigned images.** Supply chain begins at the image.

**Quarterly CIS audit only.** Compliance evidence is generated by build, not audit.

**Ignoring rebuild SLA.** Patch SLA without rebuild SLA misses the real risk.

**Forgetting AIDE / auditd.** Host integrity is upstream of DAM.

## Three boardroom questions:

**Is the institution immutable?** Are regulated-database Linux hosts deployed as immutable images, or patched in place?

**What is the CIS compliance baseline?** What percentage of regulated-database Linux hosts pass CIS Level 1 audit today?

**How fast does the institution rebuild?** What is the mean time to deploy a hardened image to all regulated-database hosts after a CVE disclosure?

# 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 over-excess 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

---

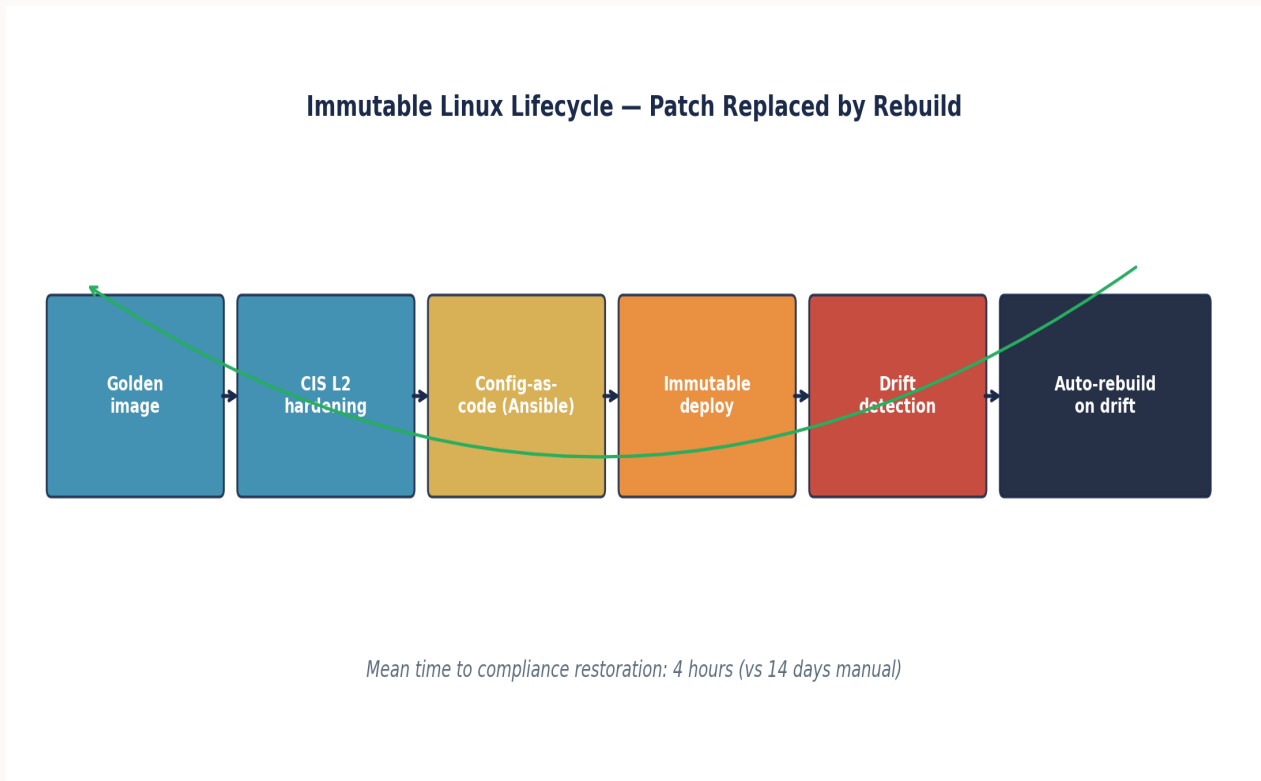
## Operating Stack

- 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

- CIS Benchmarks reference, 2024
- Doctrine specification
- Industry standard, 2024
- Modern infrastructure best practice
- CIS Benchmarks 2024
- Linux Foundation OpenSSF 2024
- NIST SP 800-190 / SP 800-204
- 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 — Immutable Linux 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>100% CIS L1 — realistic?</i>                              | Stated as a target; a CIS exception/waiver model with compensating controls is included; control mapping to CIS/NIST/DORA/PCI provided.  |
| <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>Rollback for failed immutable deploys?</i>                | A rollback procedure, sample signed image manifest, and SBOM/provenance details are included.  |

# Closing Takeaways

---

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

01. Patching is the lagging indicator; immutability is the leading indicator.
02. CIS Level 1 is the floor for regulated-database hosts.
03. Immutable infrastructure is the modern Linux security paradigm.
04. Pipeline-signed images carry their provenance with them.
05. Interactive root on production hosts is a finding waiting for a date.
06. Senior engineering builds the image; junior operations deploys it.
07. Patch SLA matters; rebuild SLA matters more.
08. DAM, auditd, AIDE, and Imperva agents all belong in the image.
09. Compliance evidence is generated by the build, not by the auditor.

*“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. |

*Patch, Pray, Repeat — Why Traditional Linux Security Fails at Scale*

*Engineering CIS-Hardened, Immutable Linux Estates for Regulated Database Infrastructure · v5.0 · published May 2026*