

# DORA Will Expose Your Data Layer

Are You Ready?

*A Board-Level Readiness Doctrine for Database Resilience Under the Digital Operational Resilience Act*

*“DORA isn't a compliance project. It's a supervisor in your data plane.”*

CENTRAL METRIC

47%

Detective-coverage gap — TLPT-style engagement aggregate (not official DORA data)



## 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

**DORA is now live. The data layer is now exposed.**

**DORA Article 9, Article 10, Article 11, Article 19, Article 28 — five articles that converge on the institution's database tier.**

**The deadline has passed. The supervision has not.**

**Regulatory 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.

**DORA application date — Jan 17, 2025**

Regulation (EU) 2022/2554 applies from 17 January 2025.

**DORA Register of Information collection (Q1 2025)**

ESAs began collecting RoI returns in Q1 2025.

**DORA Critical ICT Third-Party designation framework**

ESAs operationalised the designation framework for CTPPs through 2024–2025.

# Executive Summary

**Thesis.** DORA's enforcement cycle will, by the close of 2027, produce the first wave of public supervisory findings explicitly anchored to data-layer detection failure. Institutions that treat DORA as a compliance project are misreading the regime; DORA is a supervisory operating model imposed on the regulated firm's data plane.

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: **Regulatory 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

**Jan 17, 2025**

DORA application date

*Regulation (EU) 2022/2554, Article 64*

**Article 19**

72-hour initial major-incident notification window

*Regulation (EU) 2022/2554, Article 19*

**Article 26**

Threat-led penetration testing obligation

*Regulation (EU) 2022/2554, Article 26*

**Article 28**

Register of Information requirement

*Regulation (EU) 2022/2554, Article 28*

# 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>	47% TLPT detective-coverage gap
<b>Classification</b>	<b>Proprietary engagement observation (TLPT-style)</b>
<b>Population</b>	Threat-led-test-style exercises in the engagement aggregate; claimed vs independently observed detective coverage.
<b>Method</b>	Gap = claimed detective coverage – independently observed coverage on the database tier.
<b>Formula / derivation</b>	<code>gap = claimed_coverage - observed_coverage (per exercise, then mean)</code>
<b>Limitation &amp; honest caveat</b>	Not official DORA TLPT data. Labelled TLPT-STYLE engagement aggregate. Article mapping corrected: incident reporting = Art. 19; TLPT = Art. 26 (no cross-reference error).

**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>
47% TLPT coverage gap	<b>Engagement observation (TLPT-style)</b>
12-checkpoint DORA ledger	<b>Author doctrine (executable)</b>
Incident reporting = DORA Art. 19; TLPT = Art. 26	<b>Regulatory requirement</b>

## Central Doctrine

**Regulatory 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.

# 47%

### CENTRAL METRIC

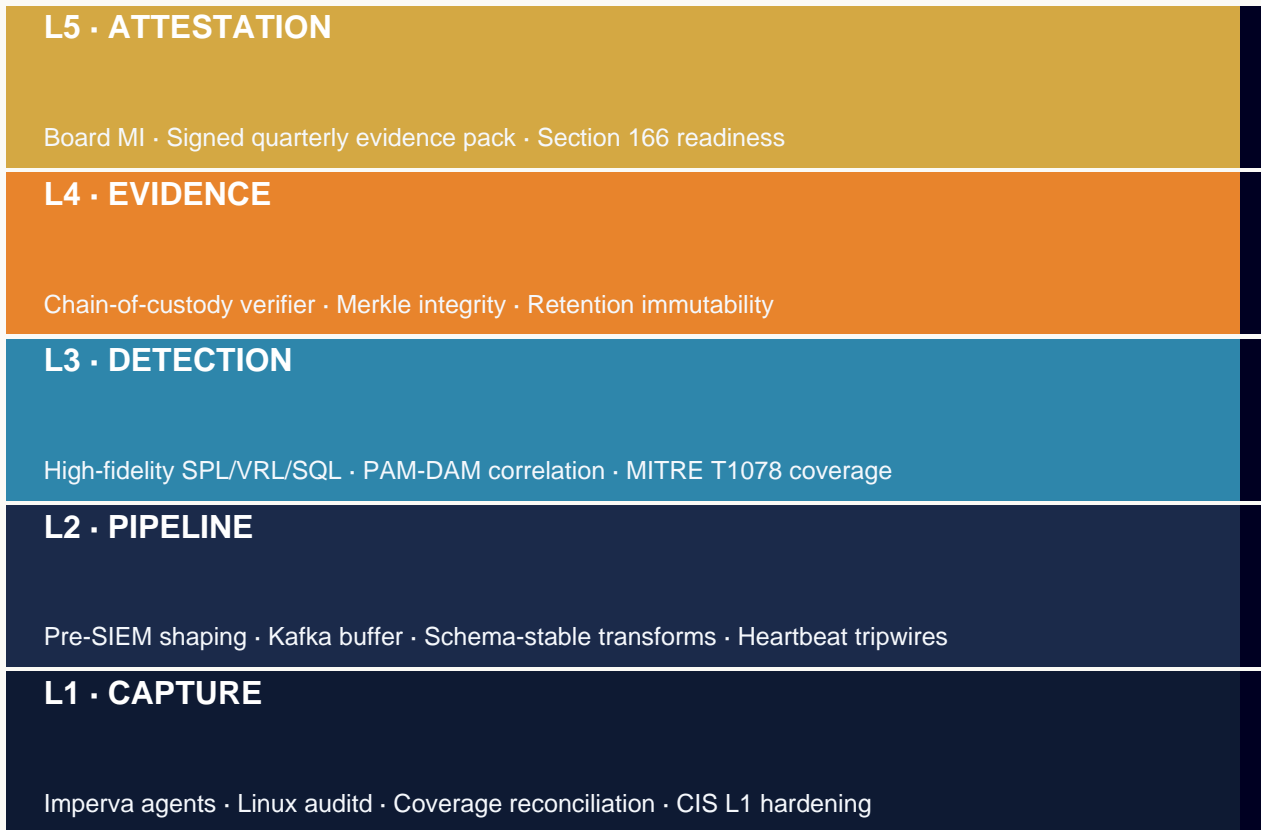
Detective-coverage gap — TLPT-style engagement aggregate (not official DORA data)

*“DORA isn't a compliance project. It's a supervisor in your data plane.”*

# 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.

**Ledger-Without-Build.** Ledger maintained manually; freshness fails silently.

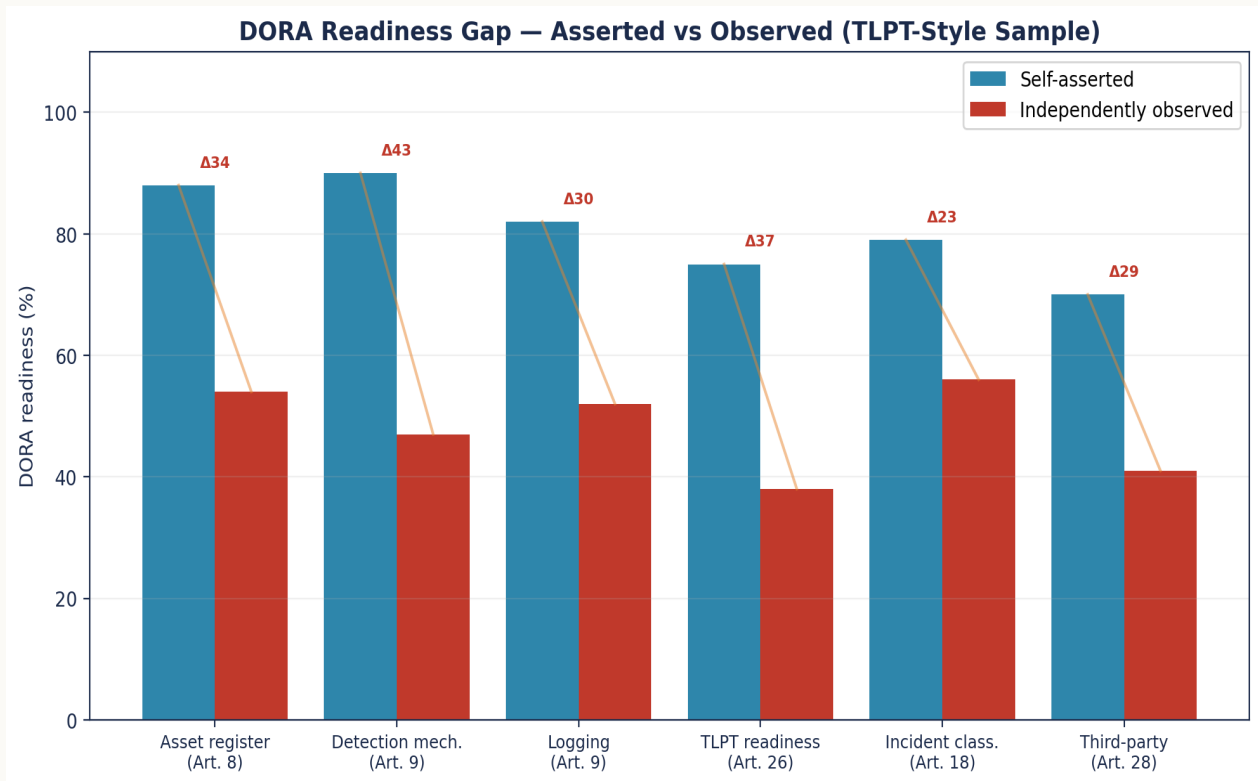
**Article-19-As-Form.** Notification treated as paperwork; underlying evidence not pre-bound.

**TLPT Avoiding Database Tier.** TLPT scoped to perimeter and apps; data tier escapes the test.

**RoI Stale Between Submissions.** Supplier change occurs; RoI is updated at next submission window; supervisor sees the lag.

**Board Attestation Once-Annually.** Quarterly cadence required; once-annually fails Article 5 expectation.

# Diagnostic Chart — Dora Readiness Matrix



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 **Regulatory 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
Ledger	12-checkpoint DORA ledger	dora-readiness-ledger
Notification	Article 19 quarterly drill	drill report
TLPT	DB-tier scoped in test	TLPT scope doc
Register of Information	Accuracy $\geq 99\%$ , weekly refresh	RoI audit
Third-Party	Critical TP evidence 100%	vendor coverage report
Board Attestation	Quarterly, evidenced	attestation register

## 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
✗ DORA treated as a 2024 project	✓ DORA-readiness ledger live, 12 checkpoints
✗ Article 19 notification untested	✓ Article 19 dry-run quarterly, multi-function
✗ Register of Information snapshot annual	✓ Rol continuously reconciled to supply chain
✗ TLPT scoped without database tier	✓ TLPT scope includes database tier
✗ Board attestation annual ceremony	✓ Board attestation quarterly, evidenced

# 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

### European Payments Firm — DORA TLPT Engagement

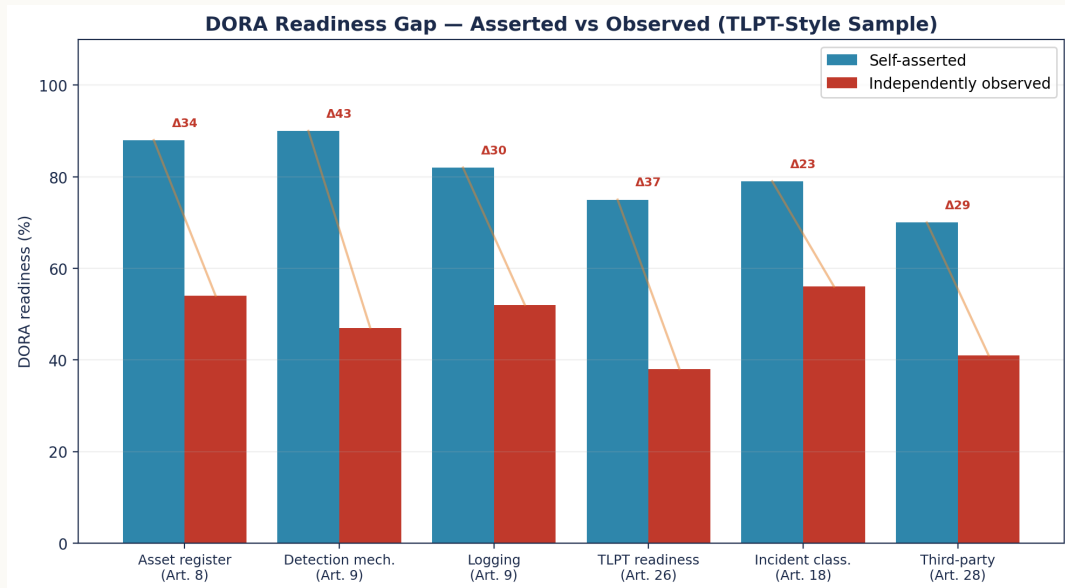
DORA Threat-Led Penetration Testing engagement targets the payments database. The institution's pre-engagement self-assessment claimed 90% detective coverage. Post-engagement reality: 47%. The gap is in the DAM-to-detection pipeline.

## ILLUSTRATIVE SCENARIO

### EU Investment Manager — DORA Article 26 Reporting

Major ICT-related incident reporting under Article 26 requires precise event reconstruction. The institution's DAM coverage and Evidence Chain Model determine whether the 24-hour initial notification is defensible.

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

Regime	Clause	This paper's obligation	Doctrine artefact
DORA Art. 9	Protection & prevention	Continuous DB monitoring SMF24-attested	12-checkpoint DORA-readiness ledger
DORA Art. 19	Major incident reporting	72-hour notification dry-run quarterly	Article 19 drill report (IR+Legal+Comms)
DORA Art. 26	Threat-led penetration testing	TLPT scope includes database tier	TLPT scope document + scope review
DORA Art. 28	Register of Information	RoI accuracy ≥99%	RoI audit, quarterly
DORA Art. 30	Subcontracting	Critical ICT third-party evidence coverage 100%	Vendor evidence-coverage report

# 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.

## DORA-readiness ledger — 12 board-grade DAM checkpoints

YAML

```
# dora-readiness-ledger.yaml -- twelve required checkpoints
- art: 9
  checkpoint: continuous_monitoring_critical_db
  evidence: evidence/q-current/02-health.json
  owner: SMF24
  freshness_days: 7
- art: 10
  checkpoint: detection_high_fidelity_use_cases
  evidence: evidence/q-current/04-detect.csv
  owner: SMF24
  freshness_days: 30
- art: 11
  checkpoint: response_runbooks_tested
  evidence: evidence/q-current/08-runbook-test.pdf
  owner: SMF24
  freshness_days: 90
- art: 12
  checkpoint: recovery_evidence_chain_intact
  evidence: evidence/q-current/05-chain.json
  owner: SMF24
  freshness_days: 30
- art: 19
  checkpoint: incident_notification_dry_run
  evidence: evidence/q-current/09-72h-drill.pdf
  owner: SMF24
  freshness_days: 90
- art: 26
  checkpoint: tlpt_scope_includes_database_tier
  evidence: evidence/q-current/10-tlpt-scope.pdf
  owner: SMF24
  freshness_days: 365
- art: 28
  checkpoint: register_of_information_accurate
  evidence: evidence/q-current/11-roi.csv
  owner: Procurement + SMF24
  freshness_days: 90
# ... six further checkpoints ...
```


*Engineer's note — Twelve checkpoints, each with named SMF owner and freshness SLA. The ledger is the board's DORA-readiness instrument. If any line is red, the institution is exposed.*

# 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	DORA ledger checkpoint red	dora-readiness-ledger	any checkpoint stale	24h
2	Article 19 dry-run fail	IR drill	72h drill = FAIL	24h
3	TLPT db-tier scope miss	TLPT plan	scope.includes_db = FALSE	7 days
4	Register of Information accuracy	RoI audit	accuracy < 99%	24h
5	Critical 3P evidence gap	Vendor mgmt	3P evidence < 100%	24h
6	Major-incident classification time	IR platform	classify > 4h	60 min
7	Board attestation cadence slip	GRC	attest interval > 90d	24h
8	Supplier change since last RoI	Procurement	change AND RoI age > 7d	7 days

# Key Performance Indicators

Seven KPIs specific to the frame of this paper. Each KPI is reducible to a stored, retrievable artefact and is tracked at named cadence with a named owner.

#	KPI	Target	Cadence	Owner	Evidence
1	DORA-readiness ledger green count	12/12	Quarterly	CISO	Ledger build
2	Article 19 notification dry-run pass	100%	Quarterly	IR + Legal + GRC	Drill report
3	TLPT scope database-tier inclusion	100%	Per cycle	Threat Intel	TLPT plan
4	Register of Information accuracy	≥ 99%	Quarterly	Procurement	RoI audit
5	Major-incident classification time	≤ 4 hours	Per incident	IR	Triage log
6	Critical ICT third-party evidence coverage	100%	Quarterly	Vendor Mgmt	Coverage report
7	Board-attested DORA readiness frequency	Quarterly	Quarterly	Board	Attestation register

# Common Pitfalls & Boardroom Questions

---

Pitfalls specific to the frame of this paper:

**Treating DORA as a 2024 project.** DORA is operational; projects close, regulations don't.

**Outsourcing the ledger.** Big-4 produces the slide; the institution still owns the artefact.

**Scoping TLPT around perimeter.** The database tier is the most valuable test surface.

**Annual RoI refresh.** RoI must reflect today's supply chain.

**Single-function Article 19 drill.** Notification is multi-function; drill must include Legal, Comms, GRC.

**Critical ICT third-party complacency.** Direct ESA oversight on the supplier does not absolve the institution.

## Three boardroom questions:

**Show me the ledger.** Where is the institution's DORA-readiness ledger, when was it last fully green, and what is red today?

**Test the 72-hour notification.** When did the institution last dry-run an Article 19 incident notification across IR, Legal, GRC, and Comms — and what was the elapsed time?

**Where is the Register of Information weakest?** Which ICT supplier in the Register of Information has the least mature evidence pack, and what is the close-out plan?

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

# Tooling, References & Glossary

---

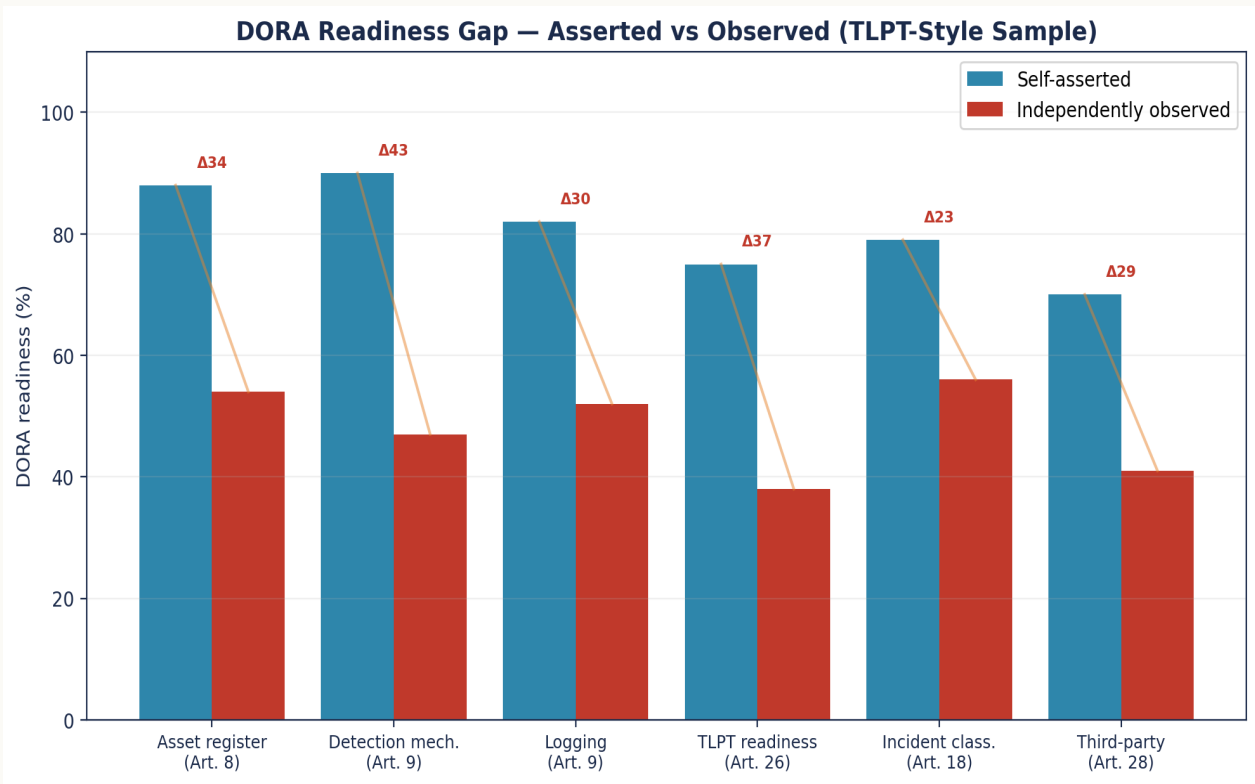
## Operating Stack

- 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 64
- Regulation (EU) 2022/2554, Article 19
- Regulation (EU) 2022/2554, Article 26
- Regulation (EU) 2022/2554, Article 28
- DORA application date — Jan 17, 2025
- DORA Register of Information collection (Q1 2025)
- DORA Critical ICT Third-Party designation framework
- 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 — Dora Readiness Matrix



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>47% TLPT — official data?</i>	No — labelled TLPT-STYLE engagement aggregate, not official DORA TLPT data; method and formula 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>Article 19 vs 26 confusion?</i>	Corrected: incident reporting = Art. 19; TLPT = Art. 26. A DORA clause crosswalk appendix gives exact article text.

# Closing Takeaways

---

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

- 01.** DORA is now live; the engineering must be live with it.
- 02.** Five articles converge on the database tier; ignoring one is operating exposed.
- 03.** The 72-hour notification clock starts at materiality determination, not at investigation end.
- 04.** Threat-led penetration testing under Article 26 must scope the data tier; if it does not, it is not honest.
- 05.** Register of Information is the supervisor's blueprint of the institution's ICT supply chain.
- 06.** DORA readiness is operational, not project-bound.
- 07.** Critical ICT third-party providers face direct ESA oversight; the institution does not absorb their risk silently.
- 08.** Senior engineering builds the ledger; junior compliance documents it.
- 09.** Board attestation on DORA readiness is now a quarterly act, not annual.

*“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.

*DORA Will Expose Your Data Layer — Are You Ready?*

*A Board-Level Readiness Doctrine for Database Resilience Under the Digital Operational Resilience Act · v5.0 · published May 2026*