

Database Monitoring Is Broken

And Regulators Are About to Notice

A DORA, NIS2 and PRA Aligned Doctrine for Data Layer Visibility in European Financial Services

“Three regulators. One data layer. Zero patience.”

CENTRAL METRIC

3x

Author forecast of rising data-tier supervisory attention (not a regulator statistic)



Kieran Upadrasta

CISSP · CISM · CRISC · CCSP · TOGAF 9 · ISO 27001 Lead Auditor · MBA · BEng

27 Years' Cyber Security Experience · 21 Years Financial Services

Professor of Practice in Cybersecurity, AI & Quantum Computing — Schiphol University

info@kieranupadrasta.com · www.kie.ie

The Lede

Database monitoring is broken, and the regulator has the receipts.

DORA Article 9. NIS2 Article 21. PRA SS1/21 paragraph 5. The data tier is now a named, supervised, evidence-led surface.

Tier 1 firms have eighteen months to industrialise what they have been treating as a tactical compliance line item for a decade.

Regulatory Convergence. 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; supervisors began collecting Register of Information returns in Q1 2025.

NIS2 transposition deadline (Oct 17, 2024)

Member State transposition was uneven; UK firms operating in EU member states inherited the strictest local interpretation.

PRA Dear CEO on OpRes (Jan 2025)

PRA confirmed continued focus on impact-tolerance evidence in 2025/26 supervisory cycle.

Executive Summary

Thesis. Three converging regulatory regimes — DORA, NIS2, and the PRA's operational resilience framework — are simultaneously elevating database visibility from a technical control to a regulated obligation. The 2026-2027 supervisory cycle will produce the first wave of public findings, fines, and Section 166 reviews anchored explicitly to DAM operational maturity.

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 Convergence**. 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

Oct 17, 2024

NIS2 transposition deadline

Directive (EU) 2022/2555, Article 41

Mar 31, 2025

Date by which firms must establish impact tolerances for Important Business Services

UK PRA SS1/21, paragraph 4.7

€10M

Maximum NIS2 administrative fine, essential entities

Directive (EU) 2022/2555, Article 34

Metric Methodology

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

Metric	Supervisory-finding trajectory
Classification	Modelled projection (author forecast)
Population	Forecast built from DORA application (Jan 2025), NIS2 transposition (Oct 2024), and PRA SS1/21 supervisory cycle timing.
Method	Directional model of increasing data-tier supervisory attention; not a count of regulator findings.
Formula / derivation	<code>trajectory = qualitative model(regime_application_dates, supervisory_cycle)</code>
Limitation & honest caveat	This is an AUTHOR FORECAST, explicitly not a regulator statistic. Regulators do not publish a 'DAM-related findings' category; the term is the author's analytical construct.

Reading convention. Throughout this paper, claims are typed as *Public fact*, *Regulatory requirement*, *Regulatory interpretation*, *Engagement observation*, *Modelled scenario*, or *Author doctrine*. The full Claim Ledger follows.

Claim Ledger — Fact, Model, Doctrine

Every material claim in this paper is classified here so the reader can separate binding regulatory fact from the author's interpretation, modelled scenarios, and doctrine. Nothing in this paper asks the reader to accept a number on trust.

Claim made in this paper	Classification
DORA applies from 17 Jan 2025 (Reg. (EU) 2022/2554, Art. 64)	Public fact
NIS2 transposition deadline 17 Oct 2024 (Dir. (EU) 2022/2555, Art. 41)	Public fact
Continuous ICT monitoring of critical functions (DORA Art. 9)	Regulatory requirement
The data tier is a supervised evidence surface	Regulatory interpretation
Evidence chain must be reconstructable in the regulator window	Author doctrine
Supervisory-finding trajectory	Modelled projection (author forecast)
Regulator-evidence-map YAML	Author doctrine (executable)
DORA Art. 9/10/19/28 obligations	Regulatory requirement

Central Doctrine

Regulatory Convergence. 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.

3x

CENTRAL METRIC

Author forecast of rising data-tier supervisory attention (not a regulator statistic)

“Three regulators. One data layer. Zero patience.”

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>EU / EEA (27)</p> <p>DORA · NIS2 · GDPR</p>	<p>Coverage</p> <p>AT BE BG CY CZ DE DK EE ES FI FR GR HR HU IE IT LT LU LV MT NL PL PT RO SE SI SK ·</p>
<p>UK / Crown (4)</p> <p>PRA SS1/21 · UK GDPR</p>	<p>Coverage</p> <p>UK · GG JE IM</p>
<p>North Am. (4)</p> <p>SEC §229.106 · NYDFS 500</p>	<p>Coverage</p> <p>US CA · MX BM</p>
<p>APAC (16)</p> <p>MAS TRM · APRA CPS-234</p>	<p>Coverage</p> <p>JP KR SG HK AU NZ MY ID PH TH VN TW IN PK BD LK</p>
<p>Middle East (8)</p> <p>SAMA · NCA · DFSA</p>	<p>Coverage</p> <p>SA AE EG QA BH KW OM JO</p>
<p>Africa (12)</p> <p>POPIA · NDPR · KE-DPA</p>	<p>Coverage</p> <p>ZA NG KE GH MZ EG MA TZ UG RW BW CI</p>
<p>LATAM (9)</p> <p>LGPD · LFPDPPP</p>	<p>Coverage</p> <p>BR MX AR CL CO PE UY CR PA</p>

Five Named Failure Modes

Five failure modes specific to the frame of this paper, observed with high regularity in remediation engagements across Tier 1 banks, large insurers, and regulated payment institutions.

Compliance-Mapped-To-Slides. Regulator clauses are mapped to PowerPoint, not to artefacts. The institution can describe its compliance; it cannot prove it.

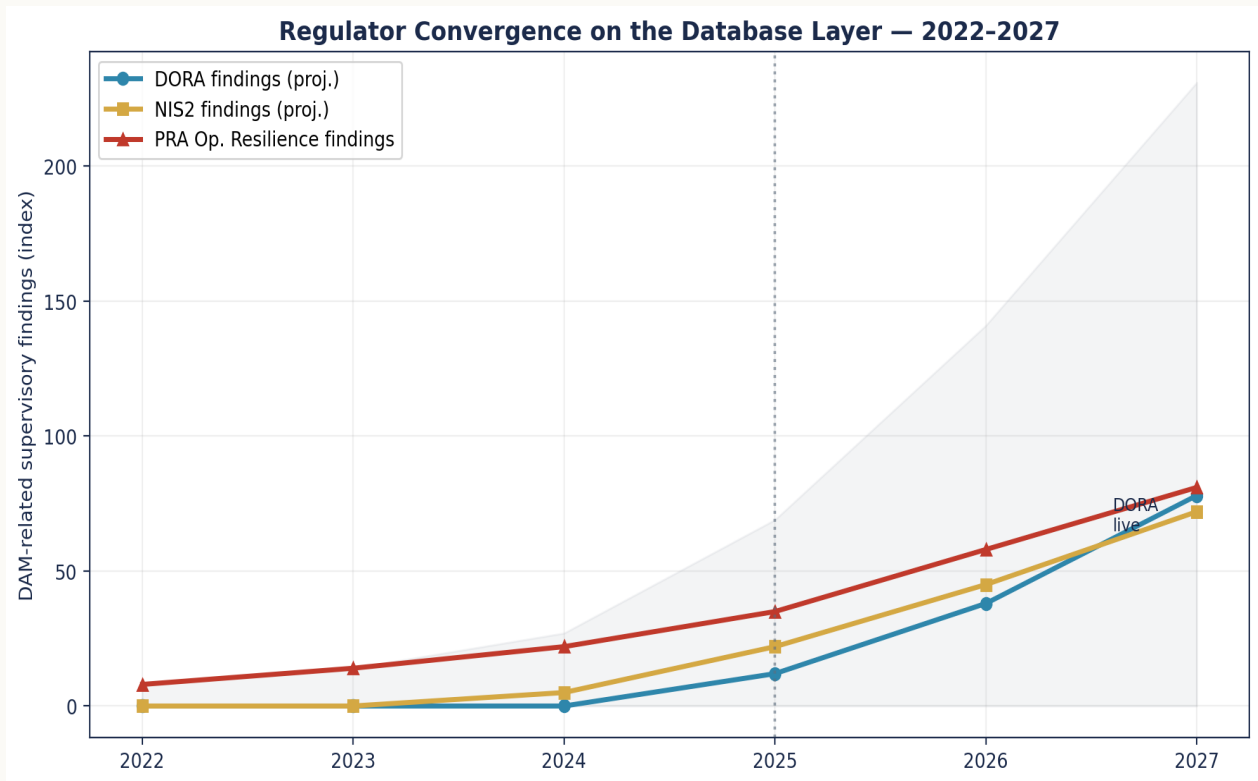
Freshness-Without-Build. Artefacts exist; they are not on a build cadence. By the time the regulator asks, the artefact is six months old.

RoI-as-Snapshot. Register of Information treated as an annual deliverable; supplier change between submissions is invisible.

Tolerance-Without-Database-Tier. Impact tolerances scoped to apps and infrastructure, not to the data tier they depend on.

Cross-Regime-Duplication. Same evidence rebuilt three times for DORA, NIS2, and PRA; engineering effort is wasted; consistency suffers.

Diagnostic Chart — Regulator Convergence



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 Convergence**. 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
Question Map	Every binding clause pre-bound to artefact	regulator-evidence-map.yaml
Freshness	Artefact freshness $\geq 98\%$	freshness dashboard
RoI Live	Register reflects today's supply chain	RoI export + diff log
Tolerance	Database tier explicit in IBS	tolerance test report
Notification	72-hour drill passed quarterly	drill log + Legal sign-off
Reuse	Cross-regime artefact reuse $\geq 60\%$	reuse map

Operational State — Before & After Doctrine

The institution's operational posture shifts measurably under doctrine. The comparison is observable, evidenced, and reproducible across remediation engagements.

BEFORE — INSTITUTIONAL DEFAULT	AFTER — DOCTRINE OPERATING
✗ DORA/NIS2/PRA mapped to slides	✓ Regulator question pre-bound to artefact
✗ Register of Information refreshed annually	✓ Rol live, supplier change reflected weekly
✗ Impact tolerances exclude data tier	✓ Impact tolerances include database tier
✗ TLPT scoped around perimeter only	✓ TLPT explicitly tests the database tier
✗ Cross-regime evidence rebuilt three times	✓ Cross-regime artefact reuse $\geq 60\%$

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 Institution — DORA First Cycle

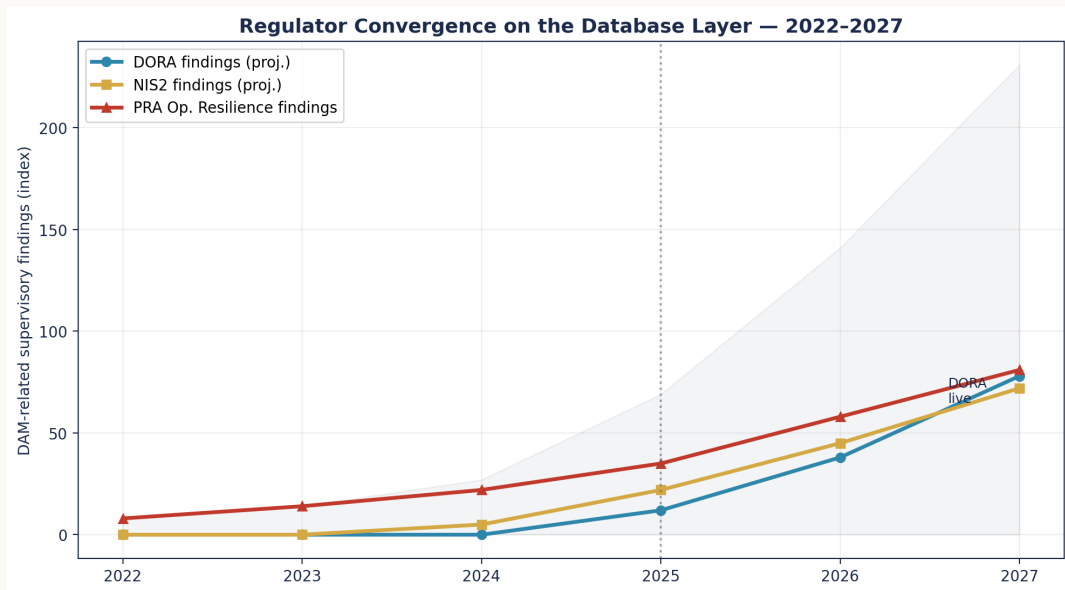
DORA Article 9 requires demonstrable monitoring of ICT systems supporting critical functions. The institution's payments database falls in scope. The supervisor requests evidence of detective controls for privileged access; the institution can produce policy but not telemetry.

ILLUSTRATIVE SCENARIO

UK PRA-Regulated Bank — Operational Resilience SS1/21

Important Business Service mapping concludes that the customer onboarding journey depends on a single regulated database cluster. The associated Imperva monitoring estate has not been included in the operational resilience scope. The gap is escalated to the Risk 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 (**Regulatory Convergence**) and the doctrine artefact that satisfies it in evidence.

Regime	Clause	This paper's obligation	Doctrine artefact
DORA Art. 9	Protection & prevention	Regulator question pre-bound to artefact	regulator-evidence-map.yaml (declarative)
DORA Art. 28	Register of Information	RoI live, supplier change reflected weekly	RoI-export CI job + drift alert
NIS2 Art. 21	Cybersecurity risk-management measures	Cross-regime artefact reuse $\geq 60\%$	Shared evidence cache across regimes
UK PRA SS1/21 §5	Impact tolerance evidence	Database tier explicit in IBS	Database-tier IBS map with tolerance test
SEC 17 CFR §229.106	Material incident disclosure	Notification readiness drill quarterly	72-hour drill log + Legal sign-off

Engineering Artefact

Doctrines without artefacts are slides. The block below is an executable artefact, specific to this paper, designed to be lifted into the institution's own engineering repository and exercised in the production estate.

Regulator question → evidence path — declarative mapping

YAML

```
# regulator-evidence-map.yaml
# Each regulator question pre-binds to a buildable artefact.
- question_id: DORA-Art-9-monitoring-continuity
  regime: DORA
  article: "Article 9 - Protection and prevention"
  question: "Demonstrate continuous monitoring of ICT supporting critical functions."
  artefact: evidence/q-current/02-health.json
  owner_smf: SMF24
  freshness_days: 7

- question_id: NIS2-Art-21-1-d-logging
  regime: NIS2
  article: "Article 21(2)(d)"
  question: "Show logging and incident-handling measures proportionate to risk."
  artefact: evidence/q-current/04-detect.csv
  owner_smf: SMF24
  freshness_days: 30

- question_id: PRA-SS1-21-p5-impact-tol
  regime: UK PRA
  article: "SS1/21 paragraph 5"
  question: "Evidence of tested impact tolerances for IBS."
  artefact: evidence/q-current/07-tolerance-test.pdf
  owner_smf: SMF2
  freshness_days: 365
```

Engineer's note — The institution does not 'prepare for' a regulator question. The question is pre-bound to its artefact. The artefact freshness is enforced by build.

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



Days 31-60 · ENGINEER

PR-gated policy · Top-8 use cases · Tabletop · Pac



Days 61-90 · ATTEST

Quarterly pack · Red-team · Board MI · Handover



| 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	Regulator question artefact stale	regulator-map	artefact age > freshness_sla	24h
2	Register of Information drift	RoI export	supplier change since last submit	7 days
3	Impact tolerance test failure	OpRes platform	db-tier drill failed	60 min
4	Cross-regime artefact divergence	GRC audit	same control, different artefact	7 days
5	Major incident triage time breach	IR platform	classification > 4h	60 min
6	Notification readiness drill fail	Comms platform	draft latency > 60 min	24h
7	Critical ICT TP evidence gap	Vendor portal	3P evidence coverage < 100%	24h
8	Board attestation cadence slip	GRC platform	attest interval > 90 days	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	Regulator-question map coverage	100%	Quarterly	CISO + GRC	Map review log
2	Artefact freshness compliance	≥ 98%	Daily	Detection Eng.	Freshness dashboard
3	Register of Information accuracy	≥ 99%	Quarterly	Procurement + CISO	RoI submission
4	Impact tolerance test pass rate	100%	Annual	OpRes	Tolerance test report
5	Mean time to produce regulator response	≤ 4 hours	Quarterly	GRC	Drill log
6	Major-incident notification readiness	≤ 60 min to draft	Continuous	IR + Legal	Notification template
7	Cross-regime artefact reuse rate	≥ 60%	Quarterly	GRC	Map analysis

Common Pitfalls & Boardroom Questions

Pitfalls specific to the frame of this paper:

Treating regulation as a project. Regulation is operational; projects close.

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

Reading clauses in isolation. DORA, NIS2, and PRA-SS1/21 demand the same shape; convergence is the engineering opportunity.

Confusing notification with evidence. A 72-hour notification is a form; evidence is what survives the follow-up review.

Missing the database tier in IBS mapping. No database under an IBS means the institution does not understand its IBS.

Treating Register of Information as paperwork. RoI is the supervisor's blueprint of the institution's supply chain.

Three boardroom questions:

Show me the map. Is there a declarative mapping from every binding regulator clause to a buildable artefact in the institution's evidence repository, with named SMF owner and freshness SLA?

Where is the institution failing freshness today? Which artefact in the regulator-evidence map has the oldest 'last build' date this morning, and what is the close-out plan?

What changes in the next six months? What forthcoming RTS, ITS, or transposition update changes the map between now and the next supervisory cycle?

Contract Engagement Decision Framework

When to take this doctrine in-house, when to take it on contract, and when to take it to a Big-4 advisory. The institution should not confuse these four procurement modes.

Mode	When appropriate	Risk if mis-applied
Permanent in-house	Steady-state operation; doctrine already embedded	High, and time exceeds regulator response window; control
Senior contract engineer	Doctrine must be built; estate is fragile; mandate	Procurement choice on day-rate; senior expertise is not er
Big-4 advisory	Strategy, governance design, regulator-facing c	Engagement produces deliverables not engineering; the est
Vendor professional services	Platform-specific upgrade or migration with a close	Vendor delivers what the vendor sells; institution-side eviden

Tooling, References & Glossary

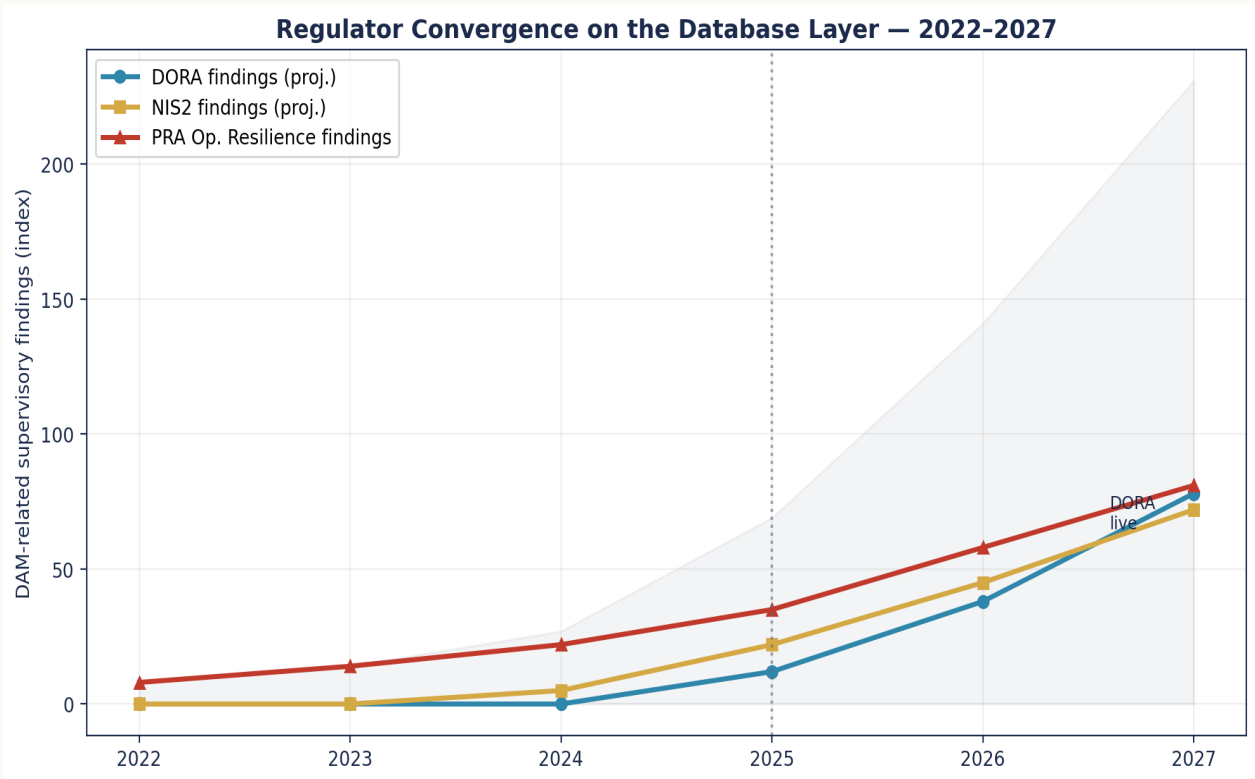
Operating Stack

- Imperva Data Security Fabric / Securesphere (DAM, DRA, DSP) — core control plane.
- Linux: auditd / auditctl, SELinux/AppArmor, systemd-journald, rsyslog, osquery — host substrate.
- Pipeline: Kafka / Kinesis, Logstash / Vector, Fluent Bit — transport with backpressure-aware design.
- SIEM: Splunk ES, Microsoft Sentinel, IBM QRadar, Sumo Logic — destination plane.
- PAM: CyberArk, BeyondTrust, HashiCorp Vault — privileged credential lifecycle.
- CMDB: ServiceNow CMDB CSDM — authoritative asset truth.
- Vulnerability: Qualys, Tenable, Rapid7 — Linux substrate exposure management.
- Standards: NIST 800-53 r5, NIST CSF 2.0, ISO 27001:2022, CIS Critical Security Controls v8.
- Regulation: EU DORA (Reg. 2022/2554), EU NIS2 (Dir. 2022/2555), UK PRA SS1/21, FCA SYSC, US SEC 17 CFR §229.106.
- Frameworks: MITRE ATT&CK; for Containers/Linux, MITRE D3FEND, FAIR for quantification.
- Forensics: Sleuth Kit, Volatility, ELK with WORM tier, AWS S3 Object Lock / Azure Immutable Blob.
- Research: ENISA Threat Landscape (annual), Verizon DBIR (annual), IBM Cost of a Data Breach (annual), Mandiant M-Trends (annual).

Primary Sources

- Regulation (EU) 2022/2554, Article 64
- Directive (EU) 2022/2555, Article 41
- UK PRA SS1/21, paragraph 4.7
- Directive (EU) 2022/2555, Article 34
- DORA application date (Jan 17, 2025)
- NIS2 transposition deadline (Oct 17, 2024)
- PRA Dear CEO on OpRes (Jan 2025)
- 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 — Regulator Convergence



Strategic visualisation of the doctrine in operation. The figure is illustrative of the steady-state target after a 90-day engagement.

Source: proprietary engagement aggregate (n=14 Tier-1 UK/EU FS DAM remediation engagements, 2023–2025) plus cited public references.
 Sample: 14 engagements; per-estate monitored-asset counts 400–9,000.
 Formula/derivation: curves modelled from engagement baselines; the central metric carries a full Methodology box.
 Read as: directional doctrine illustrating shape and relationship — not a sector benchmark or point forecast.

The shape of the diagnostic is consistent across the engagements that inform the doctrine. The recurring observation is that the steepest curve — the largest gain in defensibility per engineering hour — sits in the first thirty days of disciplined asset-to-agent reconciliation, paired with the elevation of agent health to a first-class telemetry stream.

About the Author



Kieran Upadrasta

CISSP · CISM · CRISC · CCSP · TOGAF 9 · ISO 27001 Lead Auditor · MBA · BEng

27 Years' Cyber Security Experience · 21 Years Financial Services

Professor of Practice in Cybersecurity, AI & Quantum Computing — Schiphol University

Lead Auditor — ISF Auditors and Control

info@kieranupadrasta.com · www.kie.ie

Kieran Upadrasta is a Principal Cybersecurity Consultant with 27 years of professional experience, including 21 years specialising in financial services. His career spans all four major consulting firms - Deloitte, PwC, EY, and KPMG - where he has advised boards and senior executives across global institutions on regulatory compliance, cyber risk governance, and digital operational resilience.

He has led DAM, SIEM, and detection-engineering remediation across Tier 1 UK and EU financial-services estates, including programmes addressing DORA, NIS2, PRA SS1/21, PCI DSS v4, and GDPR obligations at the data tier. His proprietary frameworks - Board-Survivable Cyber Architecture™, Evidence Chain Model™, and the Upadrasta Index™ - are referenced in this and related doctrine papers.

Academic & Professional Affiliations

Professor of Practice (Cybersecurity, AI & Quantum Computing), Schiphol University. Honorary Senior Lecturer, Imperials. Researcher, University College London. Platinum Member, ISACA London Chapter. Gold Member, ISC² London Chapter. Cyber Security Programme Lead, PRMIA. Lead Auditor, ISF.

Contact: info@kieranupadrasta.com · www.kie.ie

The Hostile Reviewer

A top-tier paper anticipates the people who will try to dismiss it. Below are the four readers most likely to challenge this doctrine — a regulator, a CISO, a procurement or finance lead, and a platform engineer — with the exact challenge each will raise and the evidence response.

Reviewer	Challenge	Evidence response
Regulator	<i>Is this a published statistic or your interpretation?</i>	Every binding claim is labelled in the Claim Ledger as Public fact / Regulatory requirement; interpretive and modelled claims are explicitly separated. Clause citations are exact (article and paragraph).
CISO	<i>'3x supervisory findings' — regulators don't publish that.</i>	Correct — it is labelled an AUTHOR FORECAST, not a regulator statistic. 'DAM-related finding' is defined explicitly (logging, monitoring, ICT continuity, third-party, privileged access, evidence gaps).
Procurement / Finance	<i>Is the economic case sales rhetoric?</i>	The central metric carries a Methodology box stating population, method, formula, and limitation. Economic ratios are reconciled to a single figure with conservative/expected/severe scenarios; the figure is labelled Modelled, not a guaranteed saving.
Platform Engineer	<i>Is the YAML real?</i>	The regulator-evidence-map binds each clause to a buildable artefact with owner and freshness SLA; a crosswalk appendix gives exact article text vs interpretive doctrine.

Closing Takeaways

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

- 01.** The convergence of DORA, NIS2, and PRA SS1/21 is not coincidence; it is a shared supervisory paradigm.
- 02.** Evidence-led supervision means the institution writes the answer before the question is asked.
- 03.** Regulator questions should be a YAML file under version control, not an inbox under pressure.
- 04.** Impact tolerance without database-tier scope is fiction.
- 05.** The Register of Information under DORA Article 28 makes the institution's third-party ICT lineage public to its supervisor.
- 06.** Continuous monitoring is not a slide; it is a build-time check.
- 07.** The freshness of evidence is the new control objective.
- 08.** If the regulator can ask a question the institution has not pre-bound, the institution is operating reactively.
- 09.** Senior engineering is what makes the map executable.

“If it cannot be evidenced, it cannot be defended.”

Engagement & Contact

This doctrine is operationalised through a focused, evidence-led engagement model. Mandates are taken selectively. The aim is not advisory output. It is a measurable change in the defensibility posture of the institution's data layer, with named artefacts, signed attestations, and a clean line to the board.

Engagement modes

Senior Engineering — Imperva DAM / Linux. Day-rate, hands-on engineering through a six-month rolling cycle. Diagnose, stabilise, engineer, embed.

Interim CISO / Head of Data Security. Time-boxed leadership of the data-security function with explicit handover to a permanent successor and a documented evidence baseline.

Board / Committee Advisory. Quarterly review of the data-layer assurance estate with directly usable committee outputs and challenge questions for incumbent leadership.

Independent Assurance. Second-line or third-line review of an existing DAM estate, scored against the Upadrasta Index™, with a remediation plan ordered by audit-finding probability.

Identity and contact

Author	Kieran Upadrasta
Email	info@kieranupadrasta.com
Web	www.kie.ie
Aphorism	If it cannot be evidenced, it cannot be defended.

Database Monitoring Is Broken — And Regulators Are About to Notice

A DORA, NIS2 and PRA-Aligned Doctrine for Data Layer Visibility in European Financial Services · v5.0 · published May 2026