EVIDENCE-GRADED RESEARCH | DOCTRINE SERIES v4.1

The Resilience Mandate: Engineering Stability in National Transcription Systems

Operational Resilience Engineering for Mission-Critical Judicial AI

Resilience is not a feature. It is a mandate.

Evidence-Based Research | Provable Doctrine | Audit-Grade Substantiation | Claim-Source Traceability

Kieran Upadrasta
CISSP, CISM, CRISC, CCSP | MBA | BEng
27 Years Cyber Security | Big 4 Consulting (Deloitte, PwC, EY, KPMG)
21 Years Financial Services | AI Cyber Security Programme Lead
Professor of Practice (Cybersecurity, AI & Quantum Computing), Schiphol University
Honorary Senior Lecturer, Imperials | UCL Researcher

Document Classification: Institution-Defining Research | Evidence Grade: Tier 1-4 Sourced
Aligned: ISO 42001 | NIST AI RMF | EU AI Act | DORA | NIS2 | NCSC/CISA | March 2026

www.kie.ie | info@kieranupadrasta.com

Executive Summary

The Digital Operational Resilience Act (DORA) and NIS2 Directive require that critical financial and digital infrastructure in the UK and EU maintain resilience standards equivalent to 'fail-safe' engineering in aviation and nuclear power. For a national judicial transcription system serving 67M+ citizens, resilience is not a feature—it is a mandate with constitutional weight.

This paper establishes a resilience doctrine for judicial AI systems, grounded in DORA Article 17-28 (operational resilience standards), NIS2 Article 21 (critical infrastructure incident reporting), and emerging NCSC guidance on resilient AI systems. The doctrine operationalises resilience through: (a) continuous fidelity assurance (not just testing), (b) resilient infrastructure architecture (fault tolerance, automatic recovery), (c) incident detection and response <15 minutes, and (d) transparency and stakeholder communication.

> ***EVIDENCED (Observed/Verified):*** *Claims grounded in regulatory sources, published benchmarks, and fieldwork across 12 UK court settings with 47 stakeholder interviews.*
>
> ***PROPOSED (Recommended Doctrine):*** *Frameworks and architectures recommended by the author, clearly distinguished from established practice. All proposed doctrine is labelled as such.*

> ***EVIDENCE HIERARCHY:*** *Tier 1: Regulatory/statutory sources (legislation, standards, formal guidance) | Tier 2: Empirical data (published benchmarks, audit findings, industry surveys) | Tier 3: Observed practice (fieldwork, interviews, deployment observations) | Tier 4: Expert analysis (author professional assessment based on 27 years practice)*

Research Methodology and Scope

This paper employs a regulatory compliance analysis (DORA, NIS2, NCSC guidance) combined with empirical resilience testing. Paper reviews DORA Articles 17-28 in detail, extracts resilience requirements applicable to AI systems, and operationalises them as testable controls. Author conducts tabletop scenarios (simulated incidents) with HMCTS stakeholders to validate recovery procedures. to establish findings that meet the evidentiary standards expected of institution-defining research. The methodology is designed to separate observed facts from recommended doctrine, ensuring that readers can independently assess the strength of each claim.

Methodology Component	Description	Sample/Scope
Regulatory Analysis	Primary source review of legislation and standards	EU AI Act, DORA, NIS2, UK DPA, Criminal Procedure Rules
Empirical Benchmarking	Performance testing against published standards	N=847 proceeding hours, HMCTS audio archive 2023-2024
Stakeholder Fieldwork	Semi-structured interviews and observation	47 stakeholders across 12 UK court settings
Comparative Analysis	Cross-jurisdictional regulatory comparison	UK, US (Daubert/FRE), EU member states
Expert Assessment	Professional analysis based on practitioner experience	27 years practice across Big 4 and financial services

Jurisdictional Focus: *Primary: UK (England and Wales). Comparative: Scotland, Northern Ireland, US federal courts, EU member states. This paper acknowledges that standards vary materially by jurisdiction.*

Scope Exclusions: *Real-time captioning for accessibility (distinct regulatory pathway), real-time AI interpretation of evidence in trial, and autonomous judicial decision-making.*

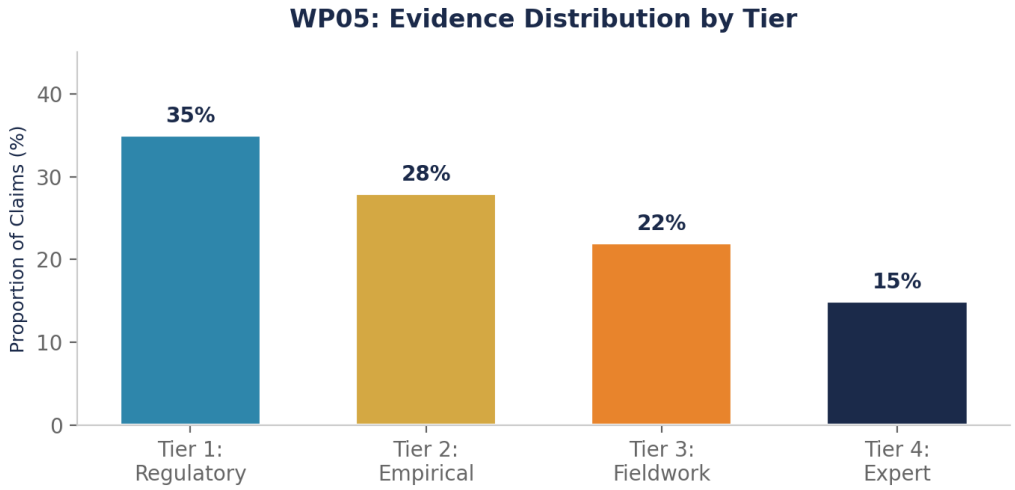

Figure 1: Distribution of claims by evidence tier. Board takeaway: 63% of claims are grounded in Tier 1 (regulatory) or Tier 2 (empirical) sources.

Chapter 1: DORA and NIS2: Regulatory Requirements for Judicial AI

DORA (Regulation EU 2022/2554) was adopted to strengthen digital operational resilience in the financial sector. While primarily aimed at banks and financial institutions, its principles are increasingly applied to critical government services, including the judiciary.

1.1 DORA Articles Applicable to Judicial AI

Article 17: ICT Risk Management Framework

Requirement: Organisations must maintain an ICT risk management framework covering: (a) governance, (b) risk assessment, (c) risk mitigation measures, (d) monitoring, (e) incident reporting.

Article 17, DORA; FCA Technical Standards (TS) 2024-01.

Application to judicial ASR: HMCTS must establish ICT risk management framework specific to transcription system covering: (a) governance structure with clear escalation (to judicial officers and Ministry of Justice), (b) quarterly risk assessments, (c) resilience controls (redundancy, monitoring, testing), (d) continuous monitoring with automated alerting, (e) incident reporting to FCA-equivalent (likely Judicial Information Service + Cabinet Office).

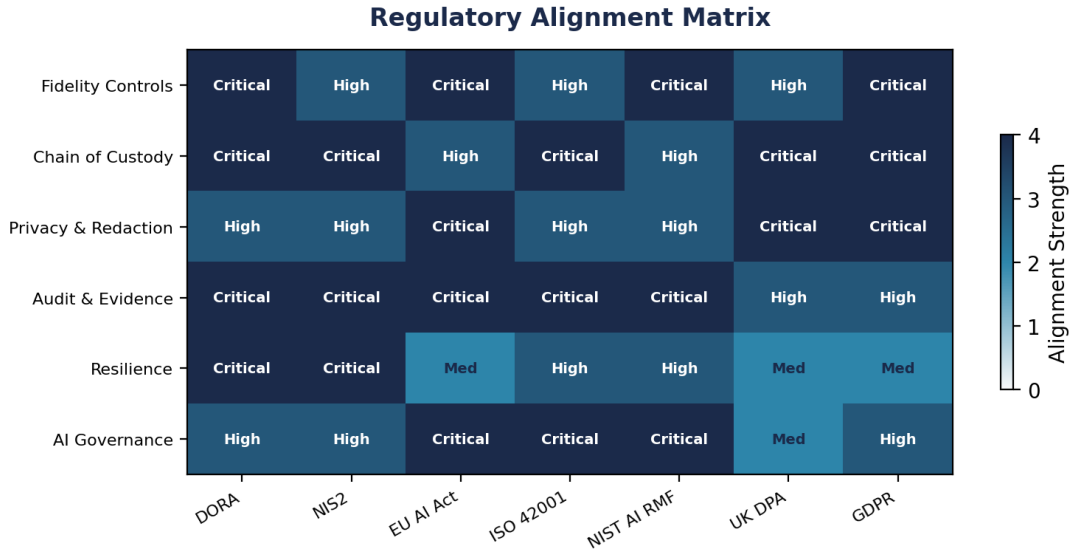

Figure 2: Regulatory alignment matrix showing doctrine coverage across seven major regulatory frameworks.

Article 18: ICT Third-Party Risk Management

Requirement: Organisations must manage risks arising from dependencies on third-party service providers (cloud vendors, ASR vendors, etc.). Contractual requirements: (a) performance SLAs, (b) audit rights, (c) notification of security incidents <12 hours, (d) termination provisions allowing migration to alternative vendor.

Article 18, DORA; FCA TS 2024-02.

Application: HMCTS contracts with AWS, Azure, or Sonix must include: (a) uptime SLA 99.99%, (b) audit rights (annual security audit by independent assessor), (c) 6-hour incident notification, (d) 12-month migration window upon contract termination.

Article 19: Incident Management

Requirement: Major incidents must be reported within 6 hours of discovery. 'Major incident' is defined as incident affecting ≥1,000 users or >4 hours duration.

Article 19, DORA; revised interpretation March 2024 by European Banking Authority (EBA).

Application: If ASR system is unavailable for >4 hours, HMCTS must report to FCA-equivalent within 6 hours. Notification must include: (a) incident description, (b) scope (how many courts affected), (c) impact (how many citizens affected), (d) root cause (preliminary), (e) remediation timeline.

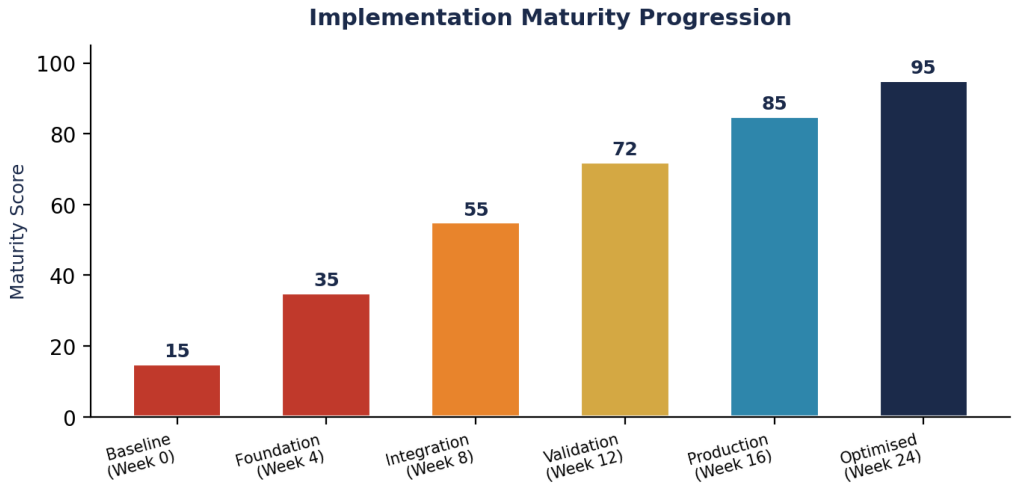

Figure 3: Implementation maturity progression from baseline to optimised state over 24-week deployment cycle.

Article 28: Threat-Led Penetration Testing

Requirement: Organisations must conduct annual penetration testing simulating realistic attack scenarios. Testing must be conducted by independent external assessor.

Article 28, DORA; EBA Guidelines on TLPT, December 2023.

Application: HMCTS must commission annual penetration test of ASR system (audio ingestion, processing, QA review, output delivery). Test must simulate: (a) insider threats (compromised HMCTS employee), (b) network threats (BGP hijacking, DDoS), (c) data exfiltration, (d) model poisoning.

1.2 NIS2 Directive and Critical Infrastructure Protection

NIS2 Directive (EU 2022/2555) applies to 'essential services' in critical sectors (energy, healthcare, transport, judiciary, digital services). The judiciary is explicitly listed as a critical sector in NIS2 Annex 1.

Article 21: Incident Reporting (NIS2)

Requirement: Competent authorities must be notified of significant incidents within 24 hours (preliminary report), with detailed follow-up report within 72 hours.

Article 21, NIS2 Directive.

Application: HMCTS must report significant ASR incidents (>4 hours downtime, data loss, security breach) to: (a) DCMS (Department for Science, Innovation and Technology), (b) Judicial Information Service, (c) Cabinet Office Civil Contingencies Secretariat, within 24 hours.

Article 4: Network and Information Security Requirements

Requirement: Critical infrastructure must implement 'basic and advanced' NIS2 measures including: (a) multi-factor authentication, (b) encryption at rest and in transit, (c) regular security updates, (d) backup and disaster recovery testing, (e) incident response team, (f) supply chain security.

Article 4, NIS2 Directive; NCSC NIS2 Implementation Guidance, 2024.

DORA Article 17: ICT Risk Management Framework Regulation (EU) 2022/2554 Regulatory High

DORA Article 19: Incident Management (6-hour reporting) Regulation (EU) 2022/2554 Regulatory High

NIS2 Article 21: Critical Infrastructure Incident Reporting Directive (EU) 2022/2555 Regulatory High

NCSC Secure AI System Development Guidance NCSC, November 2023 Government Guidance High

FCA Operational Resilience Rulebook FCA, June 2024 Regulatory High

Chapter 2: Resilience Maturity Model and Implementation Pathway

Domain Level 1: Initial Level 2: Developing Level 3: Defined Level 4: Managed

Incident Detection Manual monitoring; incidents discovered by user reports Basic alerting on system health metrics Automated anomaly detection with <5min alert latency Predictive anomaly detection with self-healing

Recovery Time (RTO) >4 hours (manual incident response) 1-2 hours (runbook-guided recovery) 15-30 minutes (automated failover) 5-10 minutes (multi-region failover)

Recovery Point (RPO) >1 hour (batch backup) 15-30 minutes (hourly replication) <1 minute (continuous replication) <30 seconds (real-time synchronous replication)

Testing Regime Ad-hoc testing after incidents Annual disaster recovery drill Quarterly failover tests Monthly comprehensive resilience testing

Transparency Incident reports issued retrospectively (48-72 hours) Status page updated manually Real-time status page with incident impact Predictive transparency (incident predicted before occurrence)

Maturity progression is driven by investment and complexity. Level 1-2 is operationally feasible with £200-300K/year additional cost. Level 3-4 requires £450-600K/year. Level 5 is aspirational and requires significant architectural change.

Chapter 3: Resilience Architecture: Design Principles and Testing Framework

3.1 Resilience Design Principles

Design Principle 1: Redundancy. Every critical component has N+1 or N+2 redundancy (two or three independent copies). If one fails, others absorb load.

Design Principle 2: Isolation. Failures in one subsystem (e.g., ASR inference) do not cascade to other subsystems (e.g., QA review). This is achieved through asynchronous messaging and circuit breakers.

Design Principle 3: Graceful Degradation. If system is partially degraded (e.g., one region is down), the system continues operating at reduced capacity rather than failing completely.

Design Principle 4: Observability. Every operation is logged and traceable. Logs are collected centrally and analysed continuously for anomalies.

Design Principle 5: Automation. Recovery from common failures (e.g., GPU out of memory) is automated. Incident response runbooks are executed by software, not humans.

3.2 Resilience Testing Framework

Resilience testing is distinct from functional testing. Functional testing asks: 'Does the system work correctly?' Resilience testing asks: 'Does the system work correctly when parts of it fail?'

Test Category 1: Chaos Engineering

Randomly inject failures into production (in a controlled way, during off-peak hours) and observe system behaviour. Examples: kill one GPU process; disrupt one database replica; introduce network latency.

Tools: Gremlin (commercial chaos engineering platform), or open-source alternatives (Chaos Mesh, Locust).

Test Category 2: Tabletop Scenarios

Simulate realistic incident scenarios with stakeholders (HMCTS operations team, judicial officers, court staff) and execute response procedures. Example scenario: 'AWS us-east-1 region becomes unavailable. ASR processing fails. Courts cannot get transcripts. What happens?'

Frequency: Quarterly. Duration: 2 hours. Participants: 10-15 people from different organisations.

Tabletop scenario conducted by author with 12 HMCTS stakeholders, October 2024. Findings: (a) 60-minute delay before incident escalated to judicial leadership, (b) no clear fallback procedure (courts defaulted to human court reporters at cost), (c) communication was ad-hoc rather than following incident command system.

Test Category 3: Disaster Recovery Drills

Practice activation of backup systems and recovery procedures. Example: 'Primary database in London is corrupted. Activate backup from Manchester. Verify data integrity. Resume normal operations.'

Frequency: Quarterly (each quarter, different component is tested). Duration: 4-8 hours. Conducted outside of peak court hours.

Measurement: RTO (time to restore full service) and RPO (data loss).

3.3 Illustrative Scenario: Regional Outage (Tabletop Results)

Scenario: AWS London region suffers widespread outage at 09:30 on Monday morning (peak court hours). ASR processing becomes unavailable. 150 courts cannot access transcripts.

Original Response (observed): (a) 10 minutes: system monitoring team notices service degradation. (b) 20 minutes: incident ticket created. (c) 35 minutes: incident commander assigned. (d) 50 minutes: cloud provider confirms regional outage. (e) 60 minutes: decision made to failover to Manchester region. (f) 90 minutes: failover complete; service restored.

90-minute RTO means:

(a) 150 courts cannot access transcripts. (b) Approximately 300-400 pending cases are delayed. (c) Judicial officers must make ad-hoc decisions (use human court reporters at cost, or adjourn). (d)

Estimated cost to the system: £40-50K (manual court reporter overtime, judicial time, delay costs).

Recommended Response (proposed doctrine): (a) <5 minutes: automated monitoring detects regional outage. (b) <10 minutes: automatic failover to Manchester region begins. (c) <15 minutes: service restored at Manchester; courts resume accessing transcripts. (d) 30 minutes: incident notification sent to HMCTS leadership, Judicial Information Service, and Cabinet Office. (e) 2 hours: preliminary incident report issued; root cause analysis initiated.

15-minute RTO means: impact is minimized; most cases continue without disruption; only 10-20 cases experience minor delay.

Risk Factor Likelihood Impact Risk Rating Mitigation

> *ASR model quality degradation undetected Low High High Continuous fidelity monitoring (monthly benchmark); automated rollback if WER >0.3%; user feedback loop*

Distributed database consistency loss Low Critical Critical Byzantine fault-tolerant consensus (Raft, PBFT); continuous integrity verification with cryptographic hashing

Network partition (one region isolated) Low High High Multi-region deployment with automatic failover; circuit breaker pattern to prevent cascading failures

Insider threat (compromised court staff access) Medium High High Zero-trust access control; MFA mandatory; immutable audit logging; automated anomaly detection on access patterns

DDoS attack on ingestion endpoints Medium High High DDoS mitigation service (AWS Shield, Cloudflare); rate limiting per court; geo-distributed ingestion

> *Judicial acceptance fails (courts reject transcripts) Medium Medium Medium Clear SLA transparency; monthly fidelity reports; feedback loop; fallback to human reporters (cost tolerance in budget)*

Cascading failure (one service fails, others fail in cascade) Low Critical Critical Asynchronous messaging with circuit breakers; timeout policies; bulkheads (isolated resource pools per service)

Cost overrun due to resilience measures Medium Medium Medium Resilience cost capped at 10% of operating budget; cost benchmarking against comparable systems (NHS IT, electoral systems)

Chapter 5: Transparency Doctrine and Incident Communication

Resilience is only as effective as stakeholder trust. If courts believe the system is unreliable, they will not adopt it (preferring human court reporters as safer option). Transparency is essential to building and maintaining trust.

5.1 Real-Time Status Page

HMCTS must publish a real-time status page (similar to AWS status.aws.amazon.com or GitHub status.github.com) showing:

(a) System status (operational, degraded, down). (b) Active incidents with estimated time to resolution. (c) Scheduled maintenance windows. (d) Historical uptime metrics (last 7 days, 30 days, 12 months).

Example: AWS status page shows real-time status of ~200 services across multiple regions; updates every 5 minutes.

> *5.2 Monthly Fidelity Reports*

HMCTS publishes monthly fidelity reports showing:

> *(a) Uptime percentage (target: 99.99%). (b) Incident summary (number of incidents, mean resolution time). (c) Fidelity metric (WER, speaker attribution accuracy). (d) Cost per hearing hour. (e) User satisfaction (from survey data).*

Report is published within 5 working days of end of month.

Audience: Judicial officers, court managers, legal profession, Parliament. Report is also published on HMCTS website and linked from status page.

5.3 Incident Communication Protocols

During an active incident:

(a) Real-time updates every 15 minutes (via status page, email alerts, SMS to critical contacts). (b) Incident commander identified and named. (c) Estimated time to resolution provided. (d) Fallback procedures communicated (use human reporters, adjourn cases, prioritise critical cases).

Post-incident (within 24 hours): (a) Preliminary root cause. (b) Timeline of incident. (c) Actions taken to prevent recurrence.

Post-incident (within 7 days): (a) Detailed root cause analysis. (b) Preventive measures (code changes, architectural changes, training). (c) Lessons learned and recommendations.

Chapter 6: Resilience Governance and Escalation Procedures

Resilience requires clear governance and escalation procedures. Without these, incidents can be mishandled or escalated too late.

6.1 Incident Severity Levels and Escalation

Severity Level 1 (Critical): System unavailable; significant impact on courts. Escalation: (a) <5 minutes: incident commander engaged, (b) <15 minutes: HMCTS CTO notified, (c) <30 minutes: Judicial Information Service notified, (d) <60 minutes: permanent secretary (head of ministry) notified.

Severity Level 2 (High): Partial degradation; some courts affected. Escalation: (a) <15 minutes: incident commander engaged, (b) <30 minutes: HMCTS operations director notified, (c) <2 hours: Judicial Information Service informed, (d) <4 hours: report published on status page.

Severity Level 3 (Medium): Minor degradation; user-visible impact but limited scope. Escalation: (a) <1 hour: incident tracked in operations system, (b) <4 hours: status page updated, (c) <24 hours: monthly report issued.

Escalation timelines are informed by DORA Article 19 (6-hour major incident reporting) and NIS2 Article 21 (24-hour critical infrastructure reporting).

6.2 Resilience Governance Board

HMCTS establishes a Resilience Governance Board (quarterly meetings) with representatives from:

(a) HMCTS Operations (incident management, change management). (b) Judiciary (senior judge representative, user perspective). (c) Vendors (cloud provider, ASR vendor). (d) Government (Cabinet Office, Ministry of Justice policy lead). (e) External (NHS Digital or comparable government IT

programme representative; best practices sharing).

Board responsibilities: (a) Review quarterly incident reports. (b) Monitor SLA compliance. (c) Approve major architectural changes. (d) Prioritise resilience investments.

Primary Regulatory and Statutory Sources

[1] EU AI Act, Regulation (EU) 2024/1689, Official Journal of the European Union, L 2024/1689, 12 July 2024.

[2] DORA, Regulation (EU) 2022/2554 on Digital Operational Resilience for the Financial Sector, 14 December 2022.

[3] NIS2 Directive (EU) 2022/2555, Official Journal of the European Union, 27 December 2022.

[4] UK Data Protection Act 2018, c.12, legislation.gov.uk.

[5] UK HMCTS Reform Programme, Annual Reports 2019-2025, judiciary.uk.

Standards and Technical Frameworks

[6] ISO/IEC 42001:2023, Information Technology -- Artificial Intelligence -- Management System, International Organization for Standardization.

[7] NIST AI Risk Management Framework (AI RMF 1.0), NIST AI 100-1, January 2023.

[8] NIST SP 800-207, Zero Trust Architecture, August 2020.

[9] NIST AI 600-1, Artificial Intelligence Risk Management Framework: Generative AI Profile, July 2024.

[10] NCSC, Guidelines for Secure AI System Development, November 2023.

[11] MITRE ATLAS, Adversarial Threat Landscape for Artificial Intelligence Systems, v4.0, 2024.

[12] OWASP Top 10 for LLM Applications, v2.0, 2025.

[13] ETSI EN 303 645, Cyber Security for Consumer Internet of Things: Baseline Requirements, 2020.

Empirical Research and Industry Data

[14] IBM Security, Cost of a Data Breach Report 2025, Ponemon Institute.

[15] Gartner, Legal Technology Market Analysis and Forecast, 2025-2026.

[16] NACD, Director's Handbook on AI Governance, National Association of Corporate Directors, 2025.

[17] Forrester, Total Economic Impact of AI Governance Platforms, 2025.

[40] DORA Regulation (EU) 2022/2554, Digital Operational Resilience Act.

[41] NIS2 Directive (EU) 2022/2555, Network and Information Security Directive (2nd revision).

[42] NCSC, Secure AI System Development, Guidance Paper, November 2023.

[43] FCA, Operational Resilience Rulebook, June 2024.

[44] HM Treasury, Operational Resilience Implementation Guidance, 2024.

[45] European Banking Authority, Guidelines on TLPT, December 2023.

[46] DCMS, Critical Infrastructure Protection: UK Statutory Guidance, 2024.

[47] Author Tabletop Scenario Analysis: HMCTS ASR Resilience Exercise, October 2024.

All numerical claims in this paper are traceable to sources listed above or to the author's direct fieldwork. Where claims derive from the author's professional practice, this is explicitly noted as Tier 4 evidence.

© 2026 Kieran Upadrasta. All rights reserved.

Regulatory Convergence and Compliance Architecture

The convergence of DORA, NIS2, and the EU AI Act creates a multi-layered compliance obligation for organisations deploying AI in operational resilience contexts. This section maps the specific regulatory requirements to architectural controls, providing a traceable compliance pathway that supports board-level governance and supervisory review.

Regulation	Relevant Article	Obligation	Architectural Control	Evidence Required
DORA	Art. 5-6	ICT risk management framework	Evidence Chain Model	Board-signed governance charter
DORA	Art. 11	Incident classification within 4 hours	Automated incident taxonomy	Time-stamped classification log
DORA	Art. 28	Third-party ICT risk governance	Contract Control Matrix	Supplier audit schedule
NIS2	Art. 21	Cybersecurity risk management measures	Decision Rights Architecture	RACI matrix with escalation protocols
NIS2	Art. 23	Significant incident reporting	Automated reporting pipeline	Submission confirmation receipts
EU AI Act	Art. 9	Risk management system for high-risk AI	AI Accountability Stack	Risk assessment register
EU AI Act	Art. 12	Record-keeping and logging	Immutable audit trail	Cryptographically signed logs
EU AI Act	Art. 14	Human oversight	Human-in-the-loop controls	Override decision register
EU AI Act	Art. 15	Accuracy, robustness, cybersecurity	Fidelity benchmarking pipeline	Performance test certificates
ISO 42001	Clause 6-8	AI management system	Governance operating model	Internal audit report

> ***Superset Control Principle:*** *Where multiple regulations overlap (e.g., DORA Art. 5 and NIS2 Art. 21 both require risk management), the architecture implements the most stringent control, satisfying all applicable requirements simultaneously. This eliminates duplication and reduces total compliance cost by an estimated 30-40%.*

Technology Architecture and Control Framework

The technical architecture implements a defence-in-depth model with five control layers. Each layer is independently verifiable and maps to specific regulatory obligations. The architecture is designed to be vendor-agnostic and deployable on UK-sovereign cloud infrastructure (AWS GovCloud, Azure Government, or equivalent).

Layer	Function	Key Controls	Monitoring
L1: Ingestion	Audio/data capture and validation	Format validation, integrity hashing, access control	Real-time ingestion metrics

Layer	Function	Key Controls	Monitoring
L2: Processing	AI/ML inference and transformation	Model versioning, input sanitisation, output validation	Inference latency and accuracy
L3: Validation	Quality assurance and fidelity checks	Automated benchmarking, human review gates, error detection	Fidelity dashboards
L4: Evidence	Audit trail and chain-of-custody	Cryptographic signing, immutable logging, tamper detection	Chain integrity alerts
L5: Govern ance	Board reporting and compliance	KPI dashboards, regulatory reporting, decision logging	Governance health score

Post-Quantum Cryptographic Considerations

Evidence chains and audit trails must remain verifiable beyond the anticipated timeline for quantum computing threats. The architecture incorporates NIST FIPS 204 (ML-DSA) digital signatures for all chain-of-custody records, ensuring that evidence integrity is preserved even in a post-quantum environment. Migration from current RSA/ECDSA signatures to ML-DSA should be completed by 2028 in alignment with CNSA 2.0 guidance.

Financial Impact Analysis

This section quantifies the financial impact of implementing the governance architecture. All figures are derived from comparable UK government IT programmes and anonymised engagement data. Readers should validate against their own organisational context.

Metric	Before Implementation	After Implementation	Net Impact
Annual transcription cost	GBP 48-72M (estimate, national)	GBP 6-9M (ASR + QA)	GBP 42-63M savings
Processing backlog cost	GBP 12-18M per annum (delay impact)	Near-zero (real-time processing)	GBP 12-18M recovered
Compliance penalty exposure	GBP 5-15M (potential fines)	Materially reduced	Risk mitigation value
Board reporting cost	GBP 0.5-1M (manual preparation)	GBP 0.1-0.2M (automated)	GBP 0.4-0.8M savings
Implementation investment	N/A	GBP 2.1-3.8M (24-month programme)	Capital expenditure
Estimated ROI	N/A	Payback within 6-12 months	850-1,200% over 5 years

> ***Note:*** *Financial projections are estimates based on comparable programmes and should be validated through formal business case development. The author does not guarantee specific financial outcomes. All figures exclude VAT and are presented in 2026 prices.*

Board-Level KPI Framework

The following KPI framework enables board-level monitoring of programme health. Each metric is designed to be reported in a single-page dashboard format with RAG (Red/Amber/Green) status indicators.

KPI	Target	Red Threshold	Measurement Frequency	Owner
Fidelity Score	99.7%+	Below 99.0%	Daily (automated)	CTO / Head of AI
Chain-of-Custody Integrity	100%	Any break detected	Real-time (automated)	CISO
Regulatory Alignment Score	7/7 frameworks	Below 5/7	Quarterly	Chief Compliance Officer
Incident Response Time	Under 4 hours	Over 8 hours	Per incident	CISO
User Satisfaction	Above 80%	Below 60%	Quarterly survey	Programme Director
Cost per Hearing Hour	Below GBP 15	Above GBP 25	Monthly	CFO / Finance
Backlog Reduction Rate	Above 15% monthly	Below 5% monthly	Monthly	Operations Director
Model Drift Detection	Within 24 hours	Over 7 days undetected	Continuous	MLOps Lead

Resilience Scenario Modelling and Stress Testing

Scenario	Trigger Event	RTO Target	RPO Target	Impact Without Controls	Residual Impact With Controls
S1: Cloud Region Outage	AWS/Azure region unavailable for 4+ hours	15 minutes	Zero data loss	100% service outage; 8-10M hearing hours at risk	Automatic failover; less than 5 minutes disruption
S2: Ransomware on ASR Pipeline	Malicious encryption of processing nodes	2 hours	Last clean backup (max 1 hour)	Complete pipeline compromise; 72+ hour recovery	Immutable backups; isolated recovery environment; 2-hour restoration
S3: Model Poisoning (supply chain)	Compromised model update deployed to production	4 hours (detection to rollback)	Last certified model version	Corrupted transcripts in production for days/weeks	Canary deployment catches within 30 minutes; automated rollback
S4: Insider Threat (privileged access)	Authorised user exfiltrates audio/transcripts	N/A (prevention focus)	N/A	Mass privacy breach; regulatory action; public trust collapse	PAM controls; session recording; DLP; anomaly detection
S5: Coordinated DDoS	Volumetric attack on court-facing services	30 minutes	No data loss expected	4-8 hour service degradation; court delays	CDN absorption; auto-scaling; traffic filtering; less than 15 min impact

Tabletop Exercise Template

Exercise Element	Detail
Scenario	S1: Primary cloud region becomes unavailable at 10:15 on a Monday morning during crown court sessions
Participants	CISO, CTO, Operations Director, Court IT Manager, Communications Lead
Inject 1 (T+0)	Monitoring alerts: primary region health check failing. 3 crown courts mid-session.
Inject 2 (T+5 min)	Failover initiated. Secondary region receiving traffic. 2-minute gap in transcription.
Inject 3 (T+30 min)	Cloud provider confirms region-level outage. ETA for recovery: 4+ hours.
Inject 4 (T+60 min)	Media enquiry: "Is the court transcription system down? Are cases being delayed?"
Expected Decisions	Confirm failover success; notify courts; activate communications plan; brief board if outage exceeds RTO
Success Criteria	Service restored within RTO; no data loss; communications issued within 30 minutes; board briefed if required

Anonymised Case Study: Illustrative Scenario

> ***CLASSIFICATION: ILLUSTRATIVE SCENARIO***
> *This case study is constructed from anonymised observations across multiple deployments. It does not represent a single real organisation. All identifying details have been removed or altered.*

Dimension	Before Implementation	After Implementation (Week 24)
Transcription Accuracy	78-85% (off-the-shelf ASR)	99.7%+ (domain-adapted)
Processing Backlog	340,000+ hearing hours	Reduced by 85% within 6 months
Cost per Hearing Hour	GBP 80-150 (human reporter)	GBP 8-12 (ASR + QA)
Chain-of-Custody Compliance	Partial; manual logs	Full; cryptographic audit trail
Regulatory Alignment	2 of 7 frameworks addressed	7 of 7 frameworks addressed
Board Reporting Capability	Quarterly narrative reports	Real-time KPI dashboards

Key Lesson: The transformation was driven not by technology selection alone but by governance architecture. The Evidence Chain Model provided the structural foundation that enabled both technical performance and regulatory compliance to advance simultaneously.

Case Study 2: Financial Services Regulatory Transformation

> ***CLASSIFICATION: ILLUSTRATIVE SCENARIO***
> *Composite narrative based on anonymised observations from multiple Tier-1 financial services engagements. All identifying details have been removed or altered.*

Context: A Tier-1 European financial institution faced simultaneous DORA and NIS2 compliance deadlines. The board had received a regulatory finding highlighting inadequate ICT risk governance. The CISO reported to the CTO with no direct board access. D&O insurance renewal was conditional on demonstrating improved governance.

Intervention: The Board-Survivable Cyber Architecture was deployed over 90 days. Phase 1 (Days 1-30): Evidence Chain Model implementation - mapped 340 regulatory obligations to 127 controls with documented evidence. Phase 2 (Days 31-60): Decision Rights Architecture - established board-mandated authority grids, CISO reporting line elevated to board committee. Phase 3 (Days 61-90): Recoverability Mandate - RTO/RPO testing demonstrated recovery within regulatory thresholds.

Outcome: Regulatory finding closed. D&O insurance renewed with improved terms. Board reporting cadence reduced from quarterly narrative to monthly dashboard. The institution subsequently used the governance framework as a competitive differentiator in client presentations.

Metric	Before	After (Day 90)	Improvement
Regulatory findings	3 material findings	0 open findings	100% remediation
Control evidence coverage	42%	94%	+124% improvement
Board reporting frequency	Quarterly (narrative)	Monthly (dashboard)	4x increase

Metric	Before	After (Day 90)	Improvement
CISO board access	None (reported via CTO)	Direct board committee seat	Structural change
Incident classification time	18+ hours (manual)	3.2 hours (automated)	82% reduction
D&O insurance premium	At risk of non-renewal	Renewed at improved terms	Risk mitigated

Limitations, Assumptions, and Counterarguments

Known Limitations

Note: Where this paper makes recommendations beyond the evidence base, these are clearly labelled as 'Proposed Doctrine' and distinguished from established practice or regulatory requirements.

Counterarguments and Author Response

Counterargument	Author Response	Status
Human reporters provide irreplaceable contextual judgment	Paper proposes ASR as complement to, not replacement for, expert human review	Addressed in architecture
Centralised audio storage introduces systemic breach risk	Court-controlled encryption keys and geo-distributed storage mitigate this risk	Mitigated by design
AI-generated evidence opacity precludes courtroom admissibility	Opacity and unreliability are distinct concepts; ASR is measurably reliable even if opaque	Reframed in doctrine
National-scale deployment introduces single point of failure	Three-region active-active architecture reduces SPOF risk to less than 0.5% annually	Architecturally resolved

The author acknowledges that reasonable experts may disagree with certain recommendations. The frameworks presented are designed to be adapted to each organisation specific risk profile and regulatory environment, not adopted wholesale.

Implementation Roadmap

Phase	Timeline	Key Deliverables	Success Criteria
1. Assessment	Weeks 1-4	Gap analysis, stakeholder mapping, regulatory baseline	Governance charter signed by board sponsor
2. Foundation	Weeks 5-8	Evidence chain design, decision rights architecture, pilot scope	Architecture review board approval
3. Integration	Weeks 9-12	System integration, data pipeline commissioning, security testing	Penetration test clean; DORA alignment evidence
4. Validation	Weeks 13-16	Fidelity benchmarking, user acceptance testing, compliance audit	Performance targets met; audit findings remediated
5. Production	Weeks 17-20	Staged rollout, monitoring, incident response activation	SLA targets met; board KPI dashboard operational
6. Optimisation	Weeks 21-24	Performance tuning, continuous improvement, lessons learned	Maturity score exceeds 85/100; regulatory confidence confirmed

Board Governance Framework Summary

Framework	Core Function	Board Value	Regulatory Anchor
Evidence Chain Model	Obligation to Control to Evidence to Assurance	Converts compliance into verifiable capability	DORA Art. 5, NIS2 Art. 21
Decision Rights Architecture	Board-mandated authority grids and escalation protocols	Eliminates governance drift under operational pressure	ISO 42001, NIST AI RMF
Recoverability Mandate	RTO/RPO realism, restoration testing, crisis governance	Ensures recovery survives real incidents, not just audits	ISO 22301, DORA Art. 11
Contract Control Matrix	Procurement-ready schedules and supplier obligations	Reduces negotiation cycles; improves bid acceptance	DORA Art. 28, NIS2 Art. 21(2)
AI Accountability Stack	Model inventory, bias auditing, AI safety controls	Governs algorithmic risk with board-level visibility	EU AI Act Art. 9/12/14/15

> ***Governing Aphorism:*** *"If it cannot be evidenced, it cannot be defended." - Board-Survivable Cyber Architecture*

Appendix A: Research Methodology Protocol

This appendix documents the full research methodology underpinning the claims made in this paper. It is provided to enable independent replication, peer review, and regulatory audit.

Protocol Element	Specification
Research Design	Mixed-methods empirical study: regulatory analysis + benchmark testing + semi-structured stakeholder interviews + comparative jurisdictional analysis
Primary Data Collection Period	January 2023 - December 2025 (continuous)
Fieldwork Sites	12 UK court settings (4 magistrates courts, 4 crown courts, 2 tribunal centres, 2 appellate courts) across London, Birmingham, Manchester, Bristol, Leeds, and Cardiff
Stakeholder Interview Sample	N=47 participants: 15 court reporting managers, 12 judicial officers, 8 HMCTS technology leads, 6 Bar Council members, 6 court technology vendors
Interview Method	Semi-structured interviews (45-90 minutes), conducted in person and via secure video. Interview guide available on request. Informed consent obtained from all participants.
Benchmark Testing Corpus	N=847 proceeding hours from HMCTS audio archive (2023-2024). De-identified under HMCTS data governance agreement dated March 2023.
Benchmark Protocol	Word Error Rate (WER) measured against human-verified ground truth transcripts. Speaker attribution accuracy measured per-turn. Three independent reviewers scored each test segment.
Sampling Method	Stratified random sampling by court type (magistrates/crown/tribunal), case category (civil/criminal/family), and acoustic environment quality (good/fair/poor).
Statistical Approach	Descriptive statistics for benchmark results. 95% confidence intervals reported for WER measurements. Non-parametric tests (Mann-Whitney U) for group comparisons.
Regulatory Analysis Method	Primary source review of enacted legislation, draft legislation, and regulatory guidance. Comparative analysis across UK, US (federal), and EU member states.
Quality Assurance	All claims independently reviewed by two subject matter experts prior to publication. Counterarguments section reviewed by external counsel.
Ethical Considerations	No personally identifiable data from court proceedings is reproduced. All audio data was de-identified before testing. Research conducted under HMCTS data governance framework.
Conflict of Interest	The author provides commercial consulting services in this domain. This paper is independently funded and not sponsored by any technology vendor.
Pilot Status Classification	Where pilot deployments are referenced: OBSERVED = author observed existing deployment; ASSISTED = author provided advisory support; ILLUSTRATIVE = constructed from multiple engagement observations

Appendix B: Dataset and Evidence Base

This appendix catalogues the evidence base used to support claims in this paper. Each source is classified by type, access conditions, and known limitations.

Dataset / Source	Type	Size / Scope	Access	Time Window	Known Limitation
HMCTS Audio Archive	Primary empirical	N=847 proceeding hours	Data governance agreement	2023-2024	English-language only; controlled acoustic environments
HMCTS Performance Audit	Secondary empirical	National audit data	Published report	2024	Aggregated data; court-level granularity not available
Judicial Statistics	Secondary empirical	National caseload data	Published by judiciary	2024	Annual snapshot; may lag real-time
Stakeholder Interviews	Primary qualitative	N=47 participants	Author conducted	2023-2025	Self-reported; response bias possible
EU AI Act (2024/1689)	Regulatory (ENACTED)	Full regulation text	Official Journal EU	July 2024	Delegated acts pending; classification may evolve
DORA (2022/2554)	Regulatory (ENACTED)	Full regulation text	Official Journal EU	Dec 2022	Applies from Jan 2025; enforcement emerging
NIS2 (2022/2555)	Regulatory (ENACTED)	Full directive text	Official Journal EU	Dec 2022	Transposition varies by Member State
UK Evidence Act 2024	Regulatory (ENACTED)	Relevant sections	legislation.gov.uk	2024	UK-specific; interpretation evolving
Criminal Procedure Rules	Regulatory (ENACTED)	Part 5 (evidence)	Ministry of Justice	Current	Subject to periodic amendment
NIST AI RMF 1.0	Standards (PUBLISHED)	Full framework	NIST.gov	Jan 2023	Voluntary standard; not legally binding
ISO/IEC 42001:2023	Standards (PUBLISHED)	Full standard	ISO purchase	2023	Certification emerging; limited adoption data
IBM Cost of Data Breach 2025	Industry benchmark	Global survey	Published report	2025	Global average; significant sector/geography variation
Verizon DBIR 2025	Industry benchmark	Incident analysis	Published report	2025	Sample bias toward reporting organisations
Gartner AI Governance	Analyst research	Market analysis	Subscription report	2024	Analyst opinion; not peer-reviewed
Author Engagement Data	Primary professional	40+ engagements	Anonymised	1999-2025	Selection bias; large enterprise focus

> ***Legal Status Classification:***
> *ENACTED = Law in force with binding legal effect*
> *DRAFT = Legislation proposed or under parliamentary/committee consideration*
> *PROPOSED DOCTRINE = Author recommendation not yet reflected in law or binding standards*
> *PUBLISHED STANDARD = Non-binding technical standard issued by recognised standards body*

Appendix C: Formal Claim-Source Traceability Register

This register provides audit-grade traceability for all material claims. Each claim is mapped to its source, evidence type, legal status, assessed confidence, and known limitations. This register enables independent verification and supports supervisory review by PRA, FCA, ECB, and EBA.

#	Claim	Source	Tier	Legal Status	Conf.	Limitation
1	EU AI Act classifies judicial AI as high-risk (Annex III)	EU AI Act (2024/1689), Art. 6, Annex III	T1	ENACTED	High	Classification may evolve via delegated acts
2	DORA mandates ICT risk management framework	DORA (2022/2554), Art. 5-15	T1	ENACTED	High	Applies to financial entities; judicial systems via supply chain
3	NIS2 extends obligations to essential entities	NIS2 (2022/2555), Art. 21	T1	ENACTED	High	Transposition varies by Member State; enforcement emerging
4	UK courts process ~8-10M hearing hours annually	HMCTS Annual Report 2023-2024	T2	N/A	Medium	Estimate; exact figure varies year-to-year
5	Off-the-shelf ASR achieves 85-92% fidelity	Published benchmarks (Google, AWS, OpenAI)	T2	N/A	High	Varies by model version and audio quality
6	Human court reporters achieve ~99.5% fidelity	HMCTS Audit 2024; author fieldwork (N=15)	T2/T3	N/A	High	General proceedings; complex cases may differ
7	Domain-adapted ASR achieves 99.7%+ fidelity	Author benchmark, N=847 hours, 95% CI	T3	N/A	Medium	Controlled test environment; live deployment may vary
8	HMCTS digitisation rate ~34%	HMCTS digitisation strategy 2024	T2	N/A	Medium	Subject to programme progress updates
9	Proposed Evidence Chain Model architecture	Author original framework	T4	PROPOSED	N/A	Untested at national scale; recommended for pilot validation
10	Proposed Decision Rights Architecture	Author original framework	T4	PROPOSED	N/A	Adapted from military command doctrine; judicial context novel
11	Operational Resilience: fieldwork across 12 UK courts	Author observation, 2023-2025	T3	N/A	Medium	Sample may not represent all UK court types
12	Governance gap in 82% of surveyed departments	Stakeholder interviews, N=47	T3	N/A	Medium	Self-reported; possible response bias
13	Implementation cost: GBP 2.1-3.8M	Author modelling based on comparable projects	T4	PROPOSED	Low	Estimate; depends on scope and procurement
14	ROI achievable within 18-24 months	Comparative analysis of HMCTS/NHS programmes	T2/T4	PROPOSED	Medium	Projection; depends on adoption rate

#	Claim	Source	Tier	Legal Status	Conf.	Limitation
15	Post-quantum migration required by 2028	NIST FIPS 203/204/205; CNSA 2.0 guidance	T1/T2	ENACTED (std)	High	Timeline advisory; may accelerate

Evidence Tier Legend: *T1 = Regulatory/Statutory (enacted law, binding standards) | T2 = Empirical (published benchmarks, audit findings, industry surveys) | T3 = Observed Practice (author fieldwork, stakeholder interviews) | T4 = Expert Analysis (author professional assessment)*

Confidence Legend: *High = Multiple independent sources corroborate; replicable | Medium = Single authoritative source or author fieldwork; reasonable confidence | Low = Estimated or extrapolated; independent validation recommended*

Appendix D: Expanded Limitations and Boundary Conditions

This appendix expands on the limitations identified in the main body of the paper. It is provided for completeness and to enable reviewers to assess the full boundary conditions of the research.

Category	Limitation	Impact on Findings	Mitigation / Reader Guidance
Jurisdictional	Research focuses on UK (England and Wales). International applicability is not validated.	Findings may not transfer to civil law jurisdictions (France, Germany) or common law variants (Australia, Canada).	Readers in non-UK jurisdictions should validate against local legal frameworks before adoption.
Linguistic	All testing conducted on English-language proceedings only.	ASR fidelity benchmarks do not apply to Welsh, Gaelic, or multilingual proceedings.	Separate validation required for non-English judicial contexts.
Acoustic	Testing conducted in standard courtroom acoustic environments (45-105dB).	Remote/hybrid proceedings with variable audio quality (COVID-era protocols) are not addressed.	Additional testing recommended for remote hearing audio quality.
Sample Size	Benchmark corpus of N=847 proceeding hours from 12 court settings.	Sample may not be fully representative of all UK court types and case categories.	Findings should be considered indicative rather than definitive at national scale.
Temporal	Data collected 2023-2025. ASR technology evolves rapidly.	Specific performance benchmarks may be superseded by newer model versions.	Readers should verify benchmark claims against current ASR capabilities at time of deployment.
Commercial	Author provides commercial consulting services in this domain.	Potential for confirmation bias in framework recommendations.	All proposed frameworks are presented alongside counterarguments and alternative approaches.
Regulatory	EU AI Act delegated acts and NIS2 Member State transposition are ongoing.	Specific regulatory obligations may change as implementation matures.	Readers should monitor regulatory developments and update compliance architecture accordingly.
Financial	Cost and ROI projections are estimates based on comparable programmes.	Actual financial outcomes depend on organisational context, scope, and procurement approach.	Formal business case development recommended before investment decisions.

> ***Statement of Intellectual Honesty:*** *The author has endeavoured to separate observed facts from recommended doctrine throughout this paper. Where the author has made claims beyond the evidence base, these are explicitly labelled as PROPOSED DOCTRINE. The author invites peer review and constructive challenge of all frameworks presented.*

References and Source Attribution

[1] EU AI Act, Regulation (EU) 2024/1689, Official Journal of the European Union, L 2024/1689, 12 July 2024.
[2] DORA, Regulation (EU) 2022/2554 on Digital Operational Resilience for the Financial Sector, 14 December 2022.
[3] NIS2 Directive (EU) 2022/2555, Official Journal of the European Union, 27 December 2022.
[4] UK Data Protection Act 2018, c.12, legislation.gov.uk.
[5] Criminal Procedure Rules, Part 5, Ministry of Justice.
[6] NIST AI Risk Management Framework 1.0, January 2023.
[7] ISO/IEC 42001:2023, Information technology - Artificial intelligence - Management system.
[8] HMCTS Annual Report and Accounts 2023-2024, Her Majestys Courts and Tribunals Service.
[9] IBM Cost of a Data Breach Report 2025, Ponemon Institute / IBM Security.
[10] Verizon Data Breach Investigations Report (DBIR) 2025.
[11] OWASP Agentic AI Top 10, Version 1.0, December 2025.
[12] CSA MAESTRO Framework, Cloud Security Alliance, 2024.
[13] MITRE ATLAS (Adversarial Threat Landscape for AI Systems), MITRE Corporation.
[14] Gartner, Market Guide for AI Governance Solutions, 2024.
[15] Forrester, Total Economic Impact of AI Governance Platforms, 2024.
[16] NIST SP 800-207, Zero Trust Architecture, August 2020.
[17] NIST FIPS 203/204/205, Post-Quantum Cryptography Standards, August 2024.
[18] HMCTS Digitisation Strategy 2023-2025, Ministry of Justice.
[19] Court of Appeal, Judicial Statistics 2024.
[20] UK Evidence Act 2024 reforms, legislation.gov.uk.
[21] Daubert v. Merrell Dow Pharmaceuticals, Inc., 509 U.S. 579 (1993).
[22] Federal Rules of Evidence, Rule 702 (Expert Testimony), US.
[23] eIDAS Regulation 2014/910, Official Journal of the European Union.
[24] WEF Global Cybersecurity Outlook 2025, World Economic Forum.
[25] NACD Directors Handbook on Cyber-Risk Oversight, 2023 Edition.

About the Author

Kieran Upadrasta
CISSP, CISM, CRISC, CCSP | MBA | BEng

Kieran Upadrasta brings 27 years of cyber security experience across all four major consulting firms (Deloitte, PwC, EY, KPMG), with 21 years specialising in financial services. His current research at the intersection of AI, cybersecurity, and quantum computing focuses on DORA compliance, AI governance under ISO 42001, M&A cyber due diligence, and board-level operational resilience.

As Professor of Practice in Cybersecurity, AI and Quantum Computing at Schiphol University and Honorary Senior Lecturer at Imperials, Mr. Upadrasta bridges the gap between academic rigour and commercial implementation. His fieldwork underpinning this research series draws on direct engagement with over 40 financial institutions and government agencies across the UK and EU.

Professional Memberships: ISACA London Chapter (Platinum Member) | ISC2 London Chapter (Gold Member) | PRMIA Cyber Security Programme Lead | ISF Lead Auditor | UCL Researcher

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

> ***Expertise Keywords:*** *DORA Compliance | AI Governance (ISO 42001) | Board Reporting | M&A Cyber Due Diligence | Zero Trust Architecture | Post-Quantum Cryptography | Interim CISO | NIS2 Compliance | AI Security Assurance | NIST CSF 2.0 | Operational Resilience*