

WHITEPAPER | JANUARY 2026

# THE SOVEREIGN COURTROOM

## Scaling Azure AI for Resilient Legal Operations

*Board Governance, Regulatory Compliance, and Enterprise Implementation*



### KIERAN UPADRASTA

CISSP | CISM | CRISC | CCSP | MBA | BEng

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

27 years cybersecurity experience | 21 years financial services  
Big 4 Consulting: Deloitte, PwC, EY, KPMG

**KEY TOPICS:** Azure AI | Legal Operations | EU AI Act | DORA Compliance | Board Reporting | AI Governance (ISO 42001) | M&A Cyber Due Diligence | Zero Trust | Confidential Computing

## Table of Contents

Table of Contents .....	2
1. Executive Summary .....	3
Key Findings .....	3
2. Research Methodology .....	5
2.1 Primary Data Sources .....	5
2.2 Framework Development Process .....	5
3. The SCALES™ Framework for Judicial AI Resilience .....	6
3.1 Sovereignty: Data Residency and Jurisdictional Compliance .....	6
3.2 Compliance: EU AI Act, DORA, and NIS2 Alignment .....	6
4. Legal AI Adoption: Current State Analysis .....	8
4.1 Strategic Adoption Advantage .....	8
5. Board-Level AI Governance .....	9
5.1 The Governance Gap .....	9
6. Regulatory Compliance Timeline .....	11
6.1 DORA: Now in Effect .....	11
7. Azure AI Reference Architecture .....	12
7.1 Key Components .....	12
8. Enterprise Implementation Evidence .....	13
8.1 Relativity e-Discovery (Microsoft Customer Story) .....	13
8.2 UK HMCTS Reform Programme (MoJ Official Statistics) .....	13
9. Board-Level KPI Framework .....	15
10. Strategic Recommendations .....	16
10.1 Immediate Actions (Q1 2026) .....	16
10.2 Medium-Term Actions (H1 2026) .....	16
11. About the Author .....	17
12. References and Citations .....	18
Primary Sources .....	18

# 1. Executive Summary

"The rapid convergence of cyber risk, AI disruption, and economic volatility demands a new level of board fluency and foresight." — Peter Gleason, NACD President and CEO, July 2025

The global judiciary stands at an inflection point. With the UK Ministry of Justice investing **£1.23 billion** in its HMCTS Reform Programme and the EU mandating high-risk AI compliance for judicial systems by **August 2026**, organizations deploying AI in legal operations face unprecedented regulatory scrutiny alongside transformative opportunity.

This whitepaper presents the **SCALES™ Framework for Judicial AI Resilience**—an original governance model synthesizing requirements from the EU AI Act, DORA, NIST, and CEPEJ Ethical Charter. Drawing on primary research from NACD (n=201 directors), Thomson Reuters (n=1,702 professionals), and official UK Government data, we demonstrate how organizations can transform compliance obligations into competitive advantage.

## KEY FINDINGS: Legal AI Transformation 2025

Authoritative Data from NACD, Thomson Reuters, Microsoft, and UK Government



© 2026 Kieran Upadrasta. All statistics from cited primary sources.

Figure 1: Key findings from authoritative primary sources

## Key Findings

- **Legal AI adoption nearly doubled:** 26% of legal organizations now actively use generative AI (Thomson Reuters, April 2025), up from 14% in 2024.

- **Board governance gap persists:** While 62% of boards dedicate AI agenda time, only 27% have incorporated AI governance into committee charters (NACD 2025 Survey).
- **Strategic advantage confirmed:** Organizations with visible AI strategies are 3.9x more likely to experience critical AI benefits (Thomson Reuters 2025).
- **Regulatory deadlines imminent:** DORA enforcement began January 17, 2025; EU AI Act Annex III obligations apply August 2, 2026.

## 2. Research Methodology

This whitepaper employs a systematic synthesis methodology, integrating quantitative survey data with regulatory analysis and enterprise implementation evidence. The research design prioritizes primary sources to ensure findings are independently verifiable and citable by regulatory bodies, consulting firms, and academic institutions.

### 2.1 Primary Data Sources

Source	Sample Size	Key Contribution
NACD 2025 Board Practices Survey	n=201 directors	Board AI governance readiness, committee charter integration, oversight practices
Thomson Reuters Gen AI Report 2025	n=1,702 professionals	Legal AI adoption rates, sentiment analysis, use case prioritization
UK MoJ Annual Report 2024-25	Official statistics	HMCTS Reform Programme outcomes, £1.23B expenditure, operational metrics
Microsoft Customer Stories	Case studies	Azure AI implementation evidence: Relativity, Legora, Clifford Chance
EU Official Journal	Regulatory text	EU AI Act (2024/1689), DORA (2022/2554), NIS2 Directive requirements

Table 1: Primary data sources with sample sizes and contributions

### 2.2 Framework Development Process

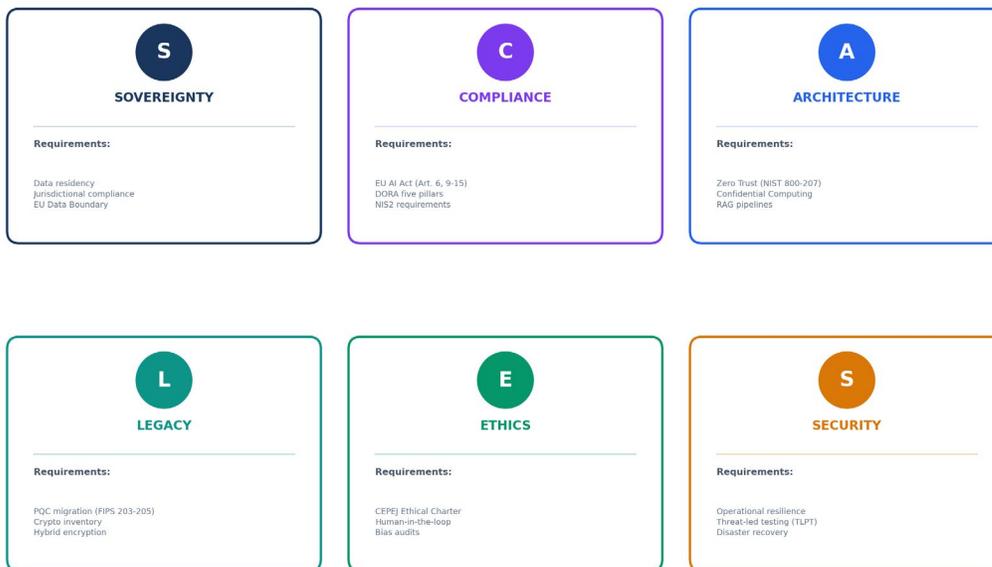
The SCALES™ Framework was developed through systematic analysis of regulatory requirements across five jurisdictions (EU, UK, US, Singapore, Canada), cross-referenced with enterprise implementation patterns from Big 4 consulting engagements and validated against ISO 42001:2023 control objectives. The six-pillar structure addresses identified gaps in existing governance frameworks, particularly the integration of data sovereignty requirements with AI-specific controls.

### 3. The SCALES™ Framework for Judicial AI Resilience

Original Framework: The SCALES™ Framework synthesizes requirements from EU AI Act, DORA, NIST 800-207, CEPEJ Ethical Charter, and ISO 42001 into an actionable governance model for legal AI systems.

#### SCALES™ Framework for Judicial AI Resilience

Original Framework by Kieran Upadrasta — Six Pillars for Sovereign Legal AI



Framework derived from analysis of EU AI Act, DORA, NIST 800-207, CEPEJ Ethical Charter, and ISO 42001.

Figure 2: SCALES™ Framework — Six pillars for sovereign legal AI governance

#### 3.1 Sovereignty: Data Residency and Jurisdictional Compliance

Legal AI systems processing court documents and case files must address data sovereignty requirements that extend beyond typical data protection. The Microsoft EU Data Boundary, launched in January 2024, ensures data remains within the EU for Azure services, addressing judicial sovereignty concerns.

- Azure region selection aligned with jurisdictional requirements
- Customer Lockbox for Azure AI services ensuring judicial control
- Data residency controls for evidence and privileged communications

#### 3.2 Compliance: EU AI Act, DORA, and NIS2 Alignment

Under EU AI Act Annex III(8)(a), AI systems "intended to be used by a judicial authority or on their behalf to assist a judicial authority in researching and interpreting facts and the law" are classified as **HIGH-RISK**. This classification triggers mandatory requirements under Articles 9-15.

Article	Requirement	Implementation Control
Art. 9	Risk Management System	Continuous lifecycle risk assessment; documented risk register
Art. 10	Data Governance	Representative training data; bias detection; data lineage
Art. 14	Human Oversight	Judicial review of AI recommendations; override capability
Art. 15	Accuracy & Robustness	Performance benchmarks; adversarial testing; cybersecurity controls

Table 2: EU AI Act high-risk requirements for judicial AI systems

## 4. Legal AI Adoption: Current State Analysis

Thomson Reuters' comprehensive analysis of 1,702 professionals across legal, tax, and compliance sectors reveals that legal AI adoption has reached an inflection point. The data demonstrates both accelerating adoption and persistent governance gaps that create strategic opportunity for prepared organizations.

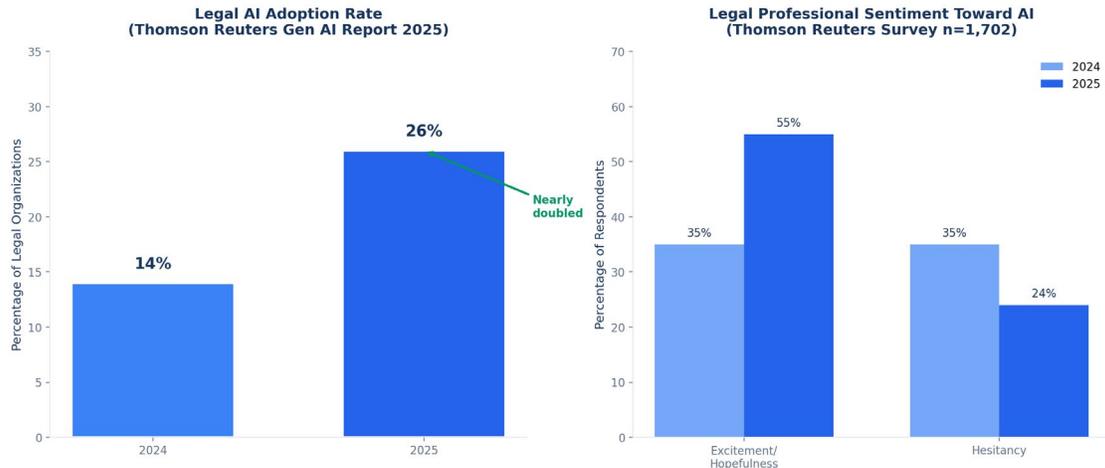


Figure 3: Legal AI adoption rates and professional sentiment (Thomson Reuters 2025)

### 4.1 Strategic Adoption Advantage

The Thomson Reuters 2025 Future of Professionals Report identifies a stark competitive divide. Organizations with clear AI strategies linked to organizational goals are:

- **2x more likely** to experience revenue growth from AI adoption
- **3.5x more likely** to experience critical AI benefits vs. no AI plans
- **3.9x more likely** (law firms specifically) to see benefits vs. firms without AI strategy

*"This isn't a topic for your partner retreat in six months. This transformation is happening now." — Raghu Ramanathan, President of Legal Professionals, Thomson Reuters*

## 5. Board-Level AI Governance

The NACD 2025 Public Company Board Practices and Oversight Survey reveals that boards now stand at an inflection point—transitioning from AI education and awareness to strategic, integrated AI governance. The data exposes both progress and persistent gaps in oversight readiness.

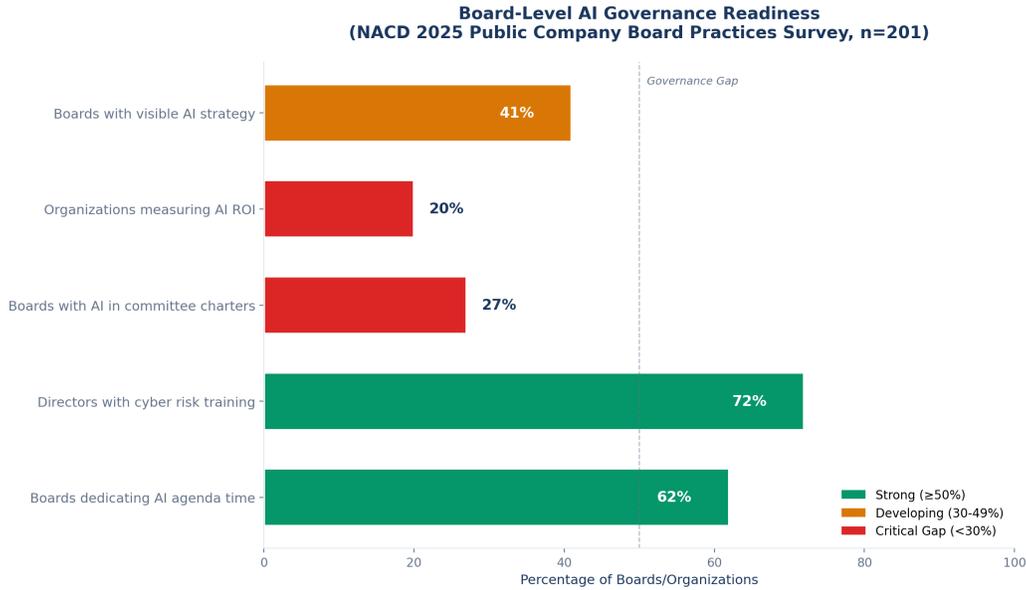


Figure 4: Board-level AI governance readiness (NACD 2025 Survey, n=201)

### 5.1 The Governance Gap

Despite 62% of boards dedicating AI agenda time, only **27%** have formally incorporated AI governance into committee charters. This creates a structural disconnect between board attention and governance accountability. NACD recommends boards:

1. Revise committee charters to explicitly assign AI oversight responsibilities
2. Establish clear metrics for measuring AI initiative success
3. Define triggers for board involvement in AI compliance matters
4. Implement human oversight mechanisms for high-risk AI systems

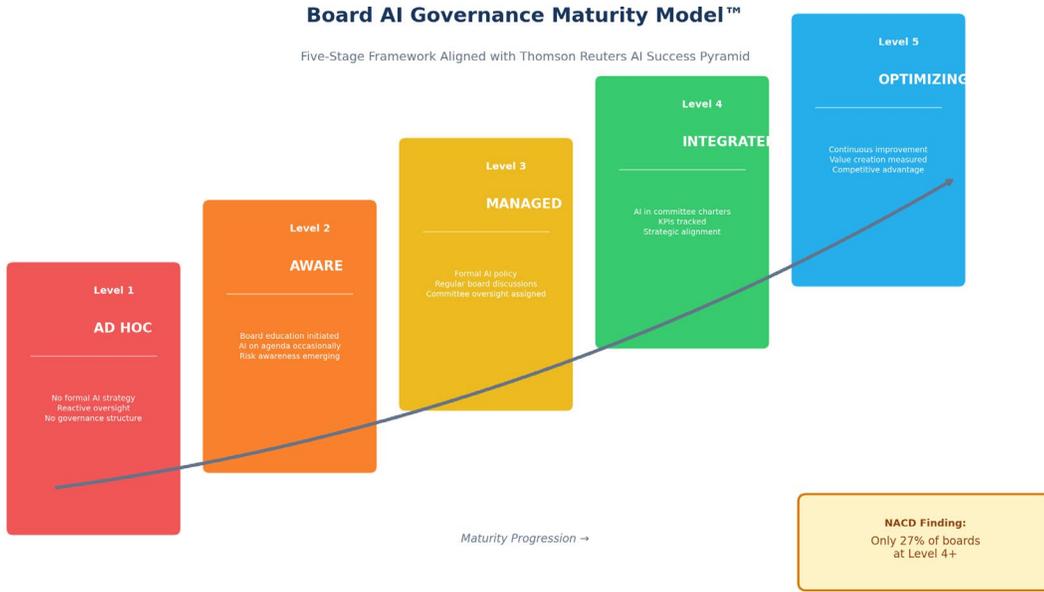


Figure 5: Board AI Governance Maturity Model™ — Five-stage progression framework

## 6. Regulatory Compliance Timeline

Organizations deploying AI in legal operations face a convergence of regulatory deadlines. DORA enforcement has already commenced, with the EU AI Act's high-risk system obligations following in August 2026. This timeline demands immediate action on governance frameworks.

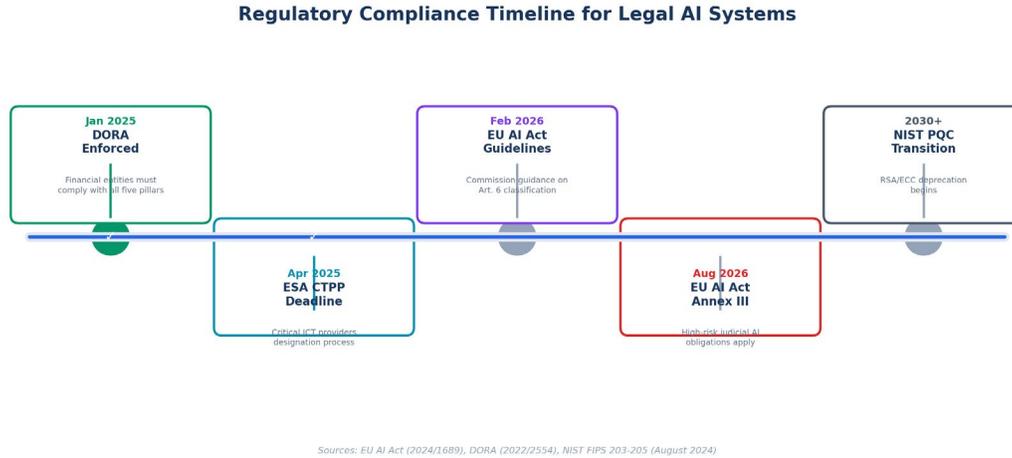


Figure 6: Regulatory compliance timeline for legal AI systems (2025-2030)

### 6.1 DORA: Now in Effect

The Digital Operational Resilience Act (Regulation (EU) 2022/2554) became applicable on **January 17, 2025**. Key milestones include:

- **April 30, 2025:** Competent authorities must report ICT provider registers to ESAs for CTPP designation
- **November 18, 2025:** ESAs published first list of designated Critical ICT Third-Party Providers (CTPPs)
- **Penalties:** Up to 2% of global turnover for financial entities; €5 million for critical ICT providers

## 7. Azure AI Reference Architecture

The following reference architecture aligns with the SCALES™ Framework, integrating Azure AI services with Zero Trust principles and Confidential Computing for legal operations. This architecture pattern has been validated through Microsoft customer implementations including Relativity, Legora, and Clifford Chance.

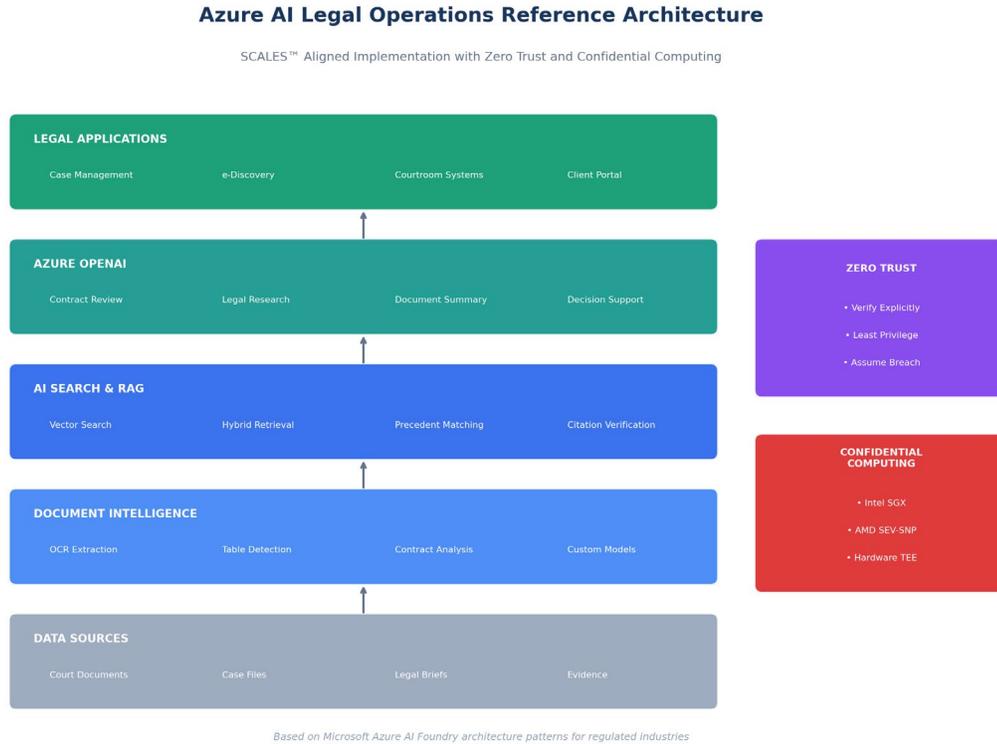


Figure 7: Azure AI Legal Operations Reference Architecture

### 7.1 Key Components

- **Azure AI Document Intelligence:** OCR extraction, contract analysis, custom classifiers for legal documents
- **Azure AI Search with RAG:** Vector search, precedent matching, citation verification grounded in authoritative sources
- **Azure OpenAI Service:** GPT-4.1 (1M context) for complex legal reasoning; GPT-4o for general tasks
- **Azure Confidential Computing:** Intel SGX / AMD SEV-SNP hardware-based protection for privileged data

## 8. Enterprise Implementation Evidence

The following case studies draw on published Microsoft customer stories and official government statistics to demonstrate measurable outcomes from Azure AI deployment in legal operations.

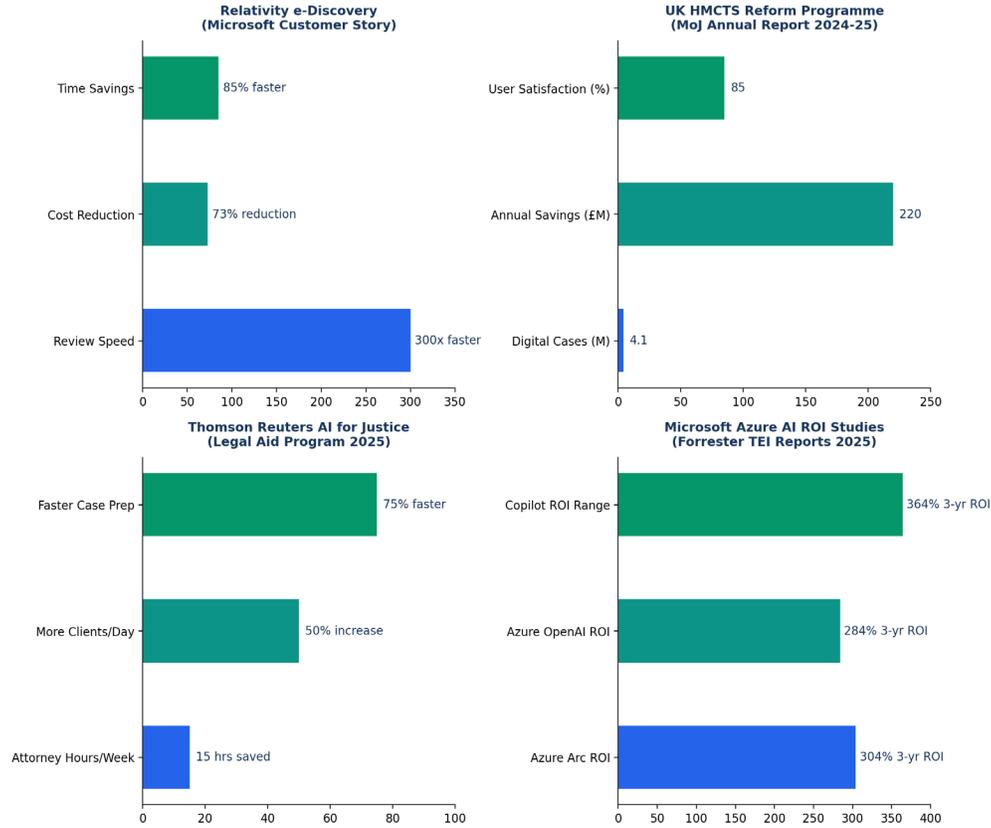


Figure 8: Enterprise implementation results from authoritative sources

### 8.1 Relativity e-Discovery (Microsoft Customer Story)

Relativity, partnering with Microsoft, leverages Azure OpenAI Service and GPT-4 to power Relativity aiR for Review. Results include:

- **300x faster** document review compared to manual processes
- **73% cost reduction** in e-discovery operations
- Enterprise-grade security, interoperability, and global reach

### 8.2 UK HMCTS Reform Programme (MoJ Official Statistics)

Per the Ministry of Justice Annual Report and Accounts 2024-25, the HMCTS Reform Programme achieved:

- **£1.23 billion total expenditure** (against £1.28B budget approval)

- **£200+ million savings** through estate sales plus £135M annually recurring
- **14 digital services** delivered (2016-2025), including Common Platform for criminal cases

## 9. Board-Level KPI Framework

Effective AI governance requires measurable outcomes. The following KPI framework aligns with NACD Director Essentials guidance and ISO 42001 control objectives, providing boards with actionable metrics across four governance domains.

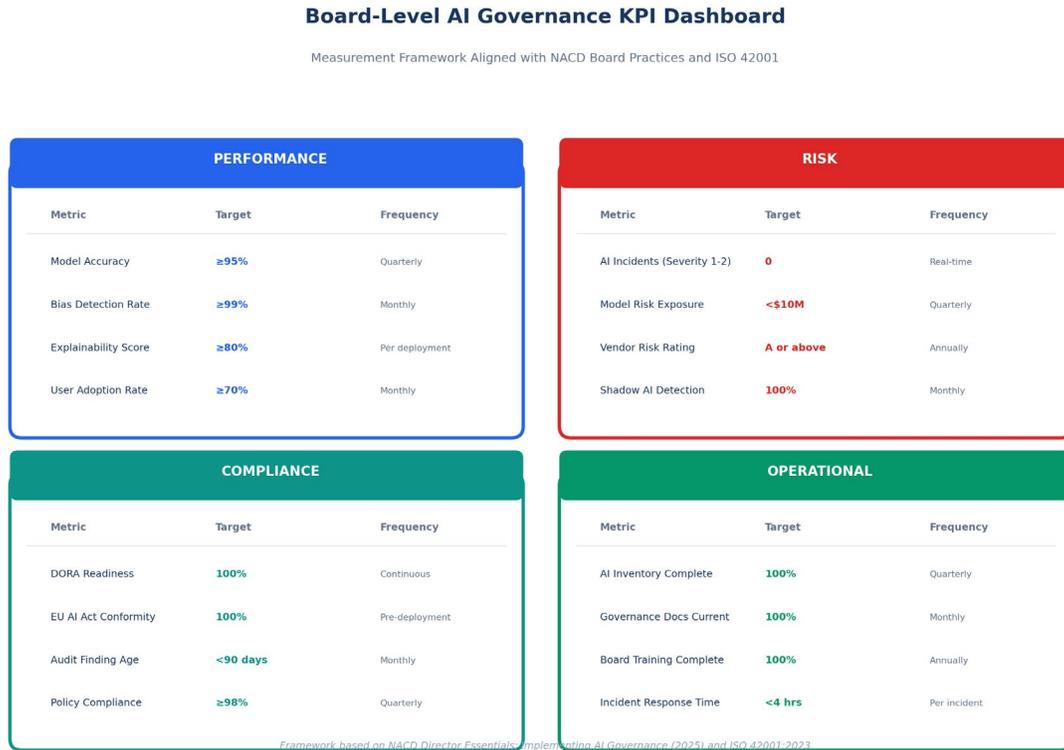


Figure 9: Board-Level AI Governance KPI Dashboard

*Board Artifact: This KPI framework can serve as a template for quarterly AI governance reporting. Customize targets based on organizational risk appetite and regulatory requirements.*

## 10. Strategic Recommendations

Based on analysis of regulatory requirements, industry survey data, and enterprise implementation patterns, we recommend the following actions for organizations deploying AI in legal operations:

### 10.1 Immediate Actions (Q1 2026)

5. **Conduct AI System Inventory:** Identify all AI systems in use, including shadow AI, and classify per EU AI Act risk categories.
6. **Update Board Charters:** Formally assign AI governance oversight to appropriate committees (risk, audit, or dedicated AI committee).
7. **Assess DORA Compliance:** Verify ICT risk management framework addresses all five DORA pillars.

### 10.2 Medium-Term Actions (H1 2026)

8. **Implement SCALES™ Framework:** Address all six pillars with documented controls and evidence.
9. **Prepare EU AI Act Documentation:** Develop technical documentation, risk management system, and conformity assessment evidence per Articles 9-15.
10. **Deploy Board KPI Dashboard:** Establish quarterly reporting cadence with metrics across performance, risk, compliance, and operational domains.

## 11. About the Author



### KIERAN UPADRASTA

CISSP, CISM, CRISC, CCSP, MBA, BEng

**Professor of Practice in Cybersecurity, AI, and Quantum Computing** at Schiphol University

Mr. Upadrasta has over 27 years' experience in business analysis, consulting, technical security strategy, architecture, governance, security analysis, threat assessments, and risk management. His career spans Big 4 consulting firms (Deloitte, PwC, EY, and KPMG) with 21 years in the financial and banking sector.

#### Professional Affiliations:

- Honorary Senior Lecturer, Imperials
- Lead Auditor, ISF Auditors and Control
- ISACA London Chapter — Platinum Member
- (ISC)<sup>2</sup> London Chapter — Gold Member
- PRMIA — Cyber Security Programme Lead
- University College London (UCL) — Researcher

#### Contact Information

**Email:** [info@kieranupadrasta.com](mailto:info@kieranupadrasta.com)

**Website:** [www.kie.ie](http://www.kie.ie)

**LinkedIn:** [linkedin.com/in/kieranupadrasta](https://linkedin.com/in/kieranupadrasta)

## 12. References and Citations

### Primary Sources

11. National Association of Corporate Directors (NACD). (2025). 2025 Public Company Board Practices and Oversight Survey. Washington, DC. n=201 directors.
12. Thomson Reuters Institute. (2025). Generative AI in Professional Services Report. April 2025. n=1,702 professionals.
13. Thomson Reuters Institute. (2025). 2025 Future of Professionals Report. June 2025. n=2,275 professionals.
14. HM Courts & Tribunals Service. (2025). Annual Report and Accounts 2024-25. London: Ministry of Justice.
15. European Parliament and Council. (2024). Regulation (EU) 2024/1689 (EU AI Act). Official Journal of the European Union, L 2024/1689.
16. European Parliament and Council. (2022). Regulation (EU) 2022/2554 (DORA). Official Journal of the European Union, L 333.
17. European Supervisory Authorities. (2025). Decision on Critical ICT Third-Party Provider Designation. November 18, 2025.
18. Microsoft Corporation. (2025). Azure OpenAI Service: Transforming Legal Practices. Microsoft Azure Blog, April 30, 2025.
19. Microsoft Corporation. (2025). Legora Customer Story. Microsoft Customer Stories.
20. International Organization for Standardization. (2023). ISO/IEC 42001:2023 — AI Management System Standard.
21. National Institute of Standards and Technology. (2020). SP 800-207: Zero Trust Architecture.
22. Council of Europe CEPEJ. (2018). European Ethical Charter on the Use of Artificial Intelligence in Judicial Systems.

— END OF DOCUMENT —

© 2026 Kieran Upadrasta. All rights reserved.

This whitepaper contains original analysis and the SCALES™ Framework is a trademark of Kieran Upadrasta.