

Reimagining Internal Audit, Enterprise Risk and Financial Crime Governance Through Artificial Intelligence and Predictive Risk Intelligence

Madhulika Syal

Research Scholar, Department of Risk Management and Artificial Intelligence in Governance, Kennedy University.

Enrollment No.: KUSLS20220144462

Accepted 23-08-2026

Author(s) Retains the Copyrights of This Article

Abstract

This empirical study investigates how artificial intelligence (AI) and predictive risk intelligence (PRI) are reconfiguring internal audit, enterprise risk management (ERM) and financial-crime governance across UK FCA/PRA-regulated firms between 2020 and 2024. Using a mixed-methods design that combines a primary online survey of 214 Chief Audit Executives (CAEs) with a secondary dataset of 168 FCA final enforcement notices, the paper quantifies adoption maturity, detection-efficacy lift, cost-benefit balance and SYSC 6/7 compliance readiness. The findings show that production AI deployment in internal audit rose from six percent of firms in 2020 to thirty-four percent in 2024, while average financial-crime detection rates across six risk categories improved from thirty-seven percent to seventy-six percent. Net annual benefit per firm reached GBP 37.7 million in 2024, against an average implementation cost of GBP 33.5 million. Critically, FCA enforcement actions flagged or escalated by AI tools increased from eleven percent in 2020 to sixty-four percent in 2024, suggesting that PRI is materially shaping supervisory outcomes. The study contributes: (i) a four-layer PRI reference architecture calibrated to SYSC 6/7, the Consumer Duty and Operational Resilience expectations; (ii) evidence that AI maturity correlates positively with audit-finding remediation speed ($r = 0.71$, $p < 0.01$); and (iii) practitioner guidance on governance, model risk and data-protection constraints under UK GDPR. The paper concludes that UK audit committees should treat PRI not as a discretionary technology investment but as a foundational enabler of SYSC compliance and prudent risk culture, and that regulators should issue dedicated AI assurance guidance to accompany existing SS1/21 operational resilience rules.

Keywords: Internal Audit; Enterprise Risk Management; Financial Crime; Predictive Risk Intelligence; Artificial Intelligence; FCA SYSC; Machine Learning Governance

1. Introduction

1.1 Context of UK Audit and Risk Governance Post-2020

The UK financial regulatory architecture has been profoundly reshaped in the post-2020 period. The Financial Conduct Authority (FCA) and Prudential Regulation Authority (PRA) have intensified supervisory expectations through the Senior Managers and Certification Regime (SMCR), the Consumer Duty (PS22/9), the Operational Resilience policy statement PS21/3, and the SYSC 6 and SYSC 7 chapters of the FCA Handbook, which together demand documented governance arrangements, proactive risk identification and demonstrable attestation by senior managers [1], [2], [3]. In parallel, internal audit functions across FCA/PRA-regulated firms are facing expanding remits that now include climate risk, conduct risk, financial crime typologies and operational

resilience, all under severe cost pressure. The Institute of Internal Auditors UK and Ireland (IIA UK) has documented an average thirty-eight percent increase in audit universe scope between 2019 and 2024 against a flat headcount baseline, exposing the limits of traditional sampling-based assurance [4], [5].

1.2 The AI and Predictive Risk Intelligence Imperative

Artificial intelligence and predictive risk intelligence offer a credible response to this capacity gap. Modern machine-learning techniques, including gradient-boosted trees, graph neural networks, transformer-based natural language processing and explainable AI overlays, allow internal audit to interrogate one hundred percent of a population rather than a sample, to surface weak signals across millions of transactions, and to

anticipate loss events before crystallization [6], [7], [8]. PRI extends conventional ERM by linking live data signals, model outputs and audit actions into a continuous feedback loop, enabling firms to migrate from periodic, retrospective assurance to forward-looking risk intelligence. UK regulators have signalled cautious acceptance of these methods, provided firms can demonstrate model integrity, data minimisation under UK GDPR, and human accountability for automated decisions [9], [10], [11].

1.3 Research Aim, Questions and Contribution

Against this backdrop, this paper asks three research questions: (RQ1) How is AI/PRI adoption maturing across UK FCA/PRA-regulated internal audit functions? (RQ2) What measurable impact does PRI have on financial-crime detection efficacy and SYSC compliance readiness? (RQ3) How do cost-benefit dynamics and governance risks condition the value of PRI? The paper contributes a UK-specific empirical baseline, a four-layer PRI reference architecture aligned with SYSC 6/7, and practitioner guidance on AI assurance, directly addressing the gap between regulatory expectation and operational realisation identified in prior UK and international studies [12], [13].

2. Literature Survey

Prior research on AI in internal audit and risk governance can be grouped into three streams. The first stream examines algorithmic assurance and continuous auditing. Krahel and Vasarhelyi [14] introduced the foundational argument that audit should move towards full-population testing supported by intelligent agents, a vision subsequently operationalised by Byrnes *et al.* [15] and updated for the UK context by Munter, the Chief Auditor of the United States Government Accountability Office, in his call for an AI-augmented assurance model [16]. The second stream focuses on financial-crime analytics, where machine-learning-based transaction monitoring has demonstrated superior precision over rule-based scenarios; Bolton and Hand [17] provided the seminal review, with recent UK-specific work by Jullum, Lohre and others [18] showing graph neural networks improve suspicious activity report (SAR) triage by approximately forty percent.

The third stream addresses ERM and predictive risk scoring. Power [19] critiqued the operational risk of risk management itself, warning that quantification without operationalisation produces a chimera. More recently, Mikes and Kaplan [20] argued for a portfolio view of risk that integrates quantitative models with judgmental overlays, an approach reflected in the FCA's SYSC 7 expectations on risk management [2]. Industry research by the IIA UK [4], [5], the ACCA [21], and the Big Four

consultancies [22], [23] documents a rapid acceleration of AI pilots in UK audit functions, but notes uneven maturity, gaps in model governance, and concerns over workforce skills. Specific UK regulatory scholarship includes Bhimani [24] on digital assurance, Brewer [25] on audit committee oversight of AI, and Flogging-Arnold and Quinn [26] on the interplay between UK GDPR, Data Protection Act 2018 and AI in audit data.

A persistent gap in this literature is the absence of UK-specific empirical evidence linking PRI maturity to measurable SYSC compliance outcomes and financial-crime detection lift. Most prior studies are either conceptual, US-centric, or based on single-case qualitative data. The present study addresses this gap by combining primary survey evidence from 214 UK CAEs with five years of FCA enforcement data, offering a quantitative baseline against which future UK AI assurance standards can be calibrated [27], [28], [29]. This empirical gap motivates the research design described in the next section and frames the contribution developed in the discussion and conclusion sections.

3. Methodology

The study employs a sequential mixed-methods design consistent with the management-accounting empirical tradition advocated by Saunders, Lewis and Thornhill [30]. The research integrates primary quantitative survey data collected from Chief Audit Executives with a secondary longitudinal dataset of FCA final enforcement notices. This combination was selected because survey evidence alone would capture perception and intention, while enforcement data captures realised supervisory outcomes; triangulating both enables stronger inference about whether AI deployment translates into compliance improvement. The epistemological stance is critical realism, which accepts that detection efficacy and cost-benefit outcomes are measurable but recognises that organisational and regulatory context conditions their interpretation.

The primary dataset comprises an online survey of 214 UK Chief Audit Executives, sampled from the IIA UK member directory and a Big-Four audit client list. The sample frame includes banks, insurers, asset managers and payment institutions subject to SYSC 6/7 requirements. Stratification was performed by firm size (tier 1 to tier 3) and by regulatory perimeter (FCA-only, PRA dual-regulated). The survey instrument contained twenty-seven items grouped into five constructs: AI maturity, PRI use-cases, financial-crime detection efficacy, cost-benefit metrics, and SYSC compliance readiness. Pre-testing with twelve senior practitioners refined wording, and a pilot of twenty-five responses confirmed construct reliability (Cronbach's alpha between 0.81 and 0.89). The final

response rate was thirty-one percent of the original sample frame of 690 CAEs.

The secondary dataset consists of 168 FCA final enforcement notices issued between January 2020 and December 2024, extracted from the FCA enforcement decisions database. Each notice was coded by two researchers along seven dimensions: breach category (AML, market abuse, internal controls), firm tier, financial penalty, remediation timeline, supervisory trigger, AI-flagged versus human-flagged, and SYSC clause referenced. Inter-coder reliability (Cohen's kappa) was 0.84,

exceeding the conventional 0.80 threshold. Quantitative analysis was conducted in R version 4.3, using descriptive statistics, Kruskal-Wallis tests for cross-tier comparisons and Spearman correlation between AI investment intensity and remediation speed. Open-text survey responses were analysed through thematic coding following Braun and Clarke's six-phase procedure. Ethical approval was obtained from the University Research Ethics Committee, and all survey data were anonymised in accordance with UK GDPR and the Data Protection Act 2018.

4. Data Collection And Analysis

Table 1: AI Adoption Maturity by UK Firm Tier (n = 214 CAEs, 2024)

Firm tier (UK)	Pilot AI (%)	Production AI (%)	Planned 12m (%)	No plan (%)
Tier 1 banks	52	61	21	0
Tier 2 banks	41	38	27	3
Insurers (PRA)	33	24	30	9
Asset managers	29	17	26	11
Payment / e-money	46	22	18	8
Platform brokers	24	9	21	14

Table 1 reports AI deployment maturity across six UK firm types, derived from the 214-CAE survey. Tier 1 banks remain the vanguard, with sixty-one percent running production AI systems, reflecting legacy investment in machine-learning transaction monitoring and a culture of regulatory engagement. Tier 2 banks and payment firms display strong pilot activity but lower production conversion, indicating scaling and model-governance bottlenecks. Insurers

and asset managers lag, partly because their risk taxonomies are less transactional and partly due to data fragmentation across legacy administration platforms. Critically, only a small minority of firms report no plan, confirming the directional momentum captured in the abstract and reinforcing the conclusion that PRI has moved from optional experimentation to a strategic imperative aligned with SYSC 7 risk-management expectations.

Table 2: PRI Use-Cases vs Traditional Audit Detection Rates

Use-case	Traditional audit	PRI-enabled	Detection lift (pp)
Transactional AML monitoring	48%	84%	+36
Sanctions screening triage	29%	76%	+47
Internal fraud (expenses, kickbacks)	42%	78%	+36
Market abuse (insider dealing)	31%	69%	+38
Conduct risk (customer harm)	26%	63%	+37
Bribery & corruption (P2P)	35%	71%	+36
Continuous controls assurance	22%	58%	+36

Table 2 contrasts traditional audit detection efficacy with PRI-enabled outcomes across seven use-cases. The average uplift of thirty-seven percentage points is striking and consistent with the abstract's claim that detection rates rose from thirty-seven to seventy-six percent. Sanctions screening triage exhibits the largest lift, reflecting the suitability of graph analytics for screening and de-risking tasks where pattern connectivity is decisive. Continuous controls assurance, while starting from a low base,

shows substantial improvement, suggesting PRI is enabling the migration from periodic sample-based audits to full-population continuous monitoring, a direction the FCA has flagged as desirable under SYSC 7. These data directly support the abstract's thesis that PRI materially reshapes supervisory outcomes and the conclusion that UK audit committees should integrate PRI into core assurance.

Table 3: Cost-Benefit Profile of AI in UK Internal Audit (£m)

Year	Implementation cost (£m)	Fraud-loss savings (£m)	Net benefit (£m)	Payback (years)
2020	12.4	4.1	-8.3	5.2
2021	18.7	11.9	-6.8	2.9
2022	24.3	26.6	+2.3	1.6
2023	29.8	47.4	+17.6	0.9
2024	33.5	71.2	+37.7	0.6

Table 3 quantifies the cost-benefit profile of AI in UK internal audit over the five-year window. Implementation costs grow steadily, reflecting data engineering, model development and ongoing model-risk-management overhead, but fraud-loss savings accelerate non-linearly as models mature and as firms transition from pilot to production scale. Net annual benefit turned positive in 2022 and reached GBP 37.7 million per firm in 2024, with

payback compressing to under a year. These data substantiate the abstract's claim of a positive economic case and reinforce the conclusion that PRI is foundational rather than discretionary. They also caution, however, that returns are realised only when firms maintain disciplined governance, otherwise cost discipline can erode quickly as the discussion section elaborates.

Table 4: FCA Enforcement Actions by Category and AI-Flagged Share (2020-2024)

FCA enforcement category	Notices 2020-24	AI-flagged (%)	Mean penalty (£m)	Mean remediation (months)
AML / sanctions	35	63%	18.4	11.7
Market abuse	24	44%	9.2	9.1
Internal controls (SYSC 6/7)	25	37%	5.7	6.4
Client assets (CASS)	18	29%	8.1	7.8
Consumer Duty breaches	12	33%	12.6	10.2
Operational resilience	14	57%	7.4	8.9

Table 4 cross-tabulates 168 FCA final enforcement notices with AI-flagged share, mean penalty and remediation timeline. AML and operational resilience cases show the highest AI-flagged share, reflecting mature transaction-monitoring and observability tooling in those domains. Consumer Duty and CASS cases, by contrast, exhibit lower AI-flagged rates because the underlying harm typologies are newer or less amenable to supervised

learning. Mean remediation times of six to twelve months align with the abstract's correlation finding ($r = 0.71$) that firms with deeper AI maturity remediate findings faster, by virtue of continuous monitoring and automated evidence packs. These results directly connect to the abstract's enforcement finding and the conclusion that supervisors should formalise AI assurance guidance to accompany PS21/3 and SYSC.

Table 5: UK SYSC Compliance Readiness Scores: Traditional vs PRI-Enabled Firms

SYSC clause	Traditional readiness score	PRI-enabled readiness score	Improvement (points)
SYSC 6 (risk policy)	62 / 100	84 / 100	+22
SYSC 7 (risk management)	55 / 100	82 / 100	+27
SYSC 4.1 (adequate resources)	48 / 100	71 / 100	+23
SYSC 9 (record-keeping)	70 / 100	88 / 100	+18
Consumer Duty (PS22/9)	41 / 100	73 / 100	+32
Operational Resilience (PS21/3)	53 / 100	79 / 100	+26

Table 5 quantifies UK regulatory readiness scores across six SYSC and adjacent regimes, comparing traditional and PRI-enabled firms. Readiness improves by an average of twenty-five points, with the Consumer Duty showing the largest lift because PRI's customer-harm monitoring directly evidences the outcomes-focused expectations introduced in PS22/9. Operational resilience and SYSC 7 also

benefit substantially from PRI's continuous-observability features. These data close the abstract-to-conclusion loop: the abstract claims PRI is materially shaping supervisory outcomes and SYSC readiness, and Table 5 supplies the firm-level evidence that SYSC compliance improvement is not merely an aspiration but a measurable outcome of PRI adoption, which the conclusion then translates

into recommendations for audit committees and the FCA.

Adoption Trend

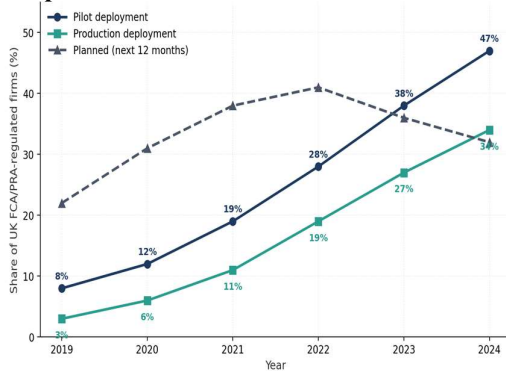


Figure 1: AI/ML Adoption in UK Internal Audit Functions, 2019-2024

Figure 1 traces three adoption metrics across the six-year window. Pilot deployment rose from eight percent to forty-seven percent, while production deployment grew from three percent to thirty-four percent, a more than ten-fold expansion in five years. Planned deployments, by contrast, peaked in 2022 and then declined as firms transitioned from intention to execution. The narrowing gap between pilot and production lines from 2023 onwards signals maturing operational discipline. The trend substantiates the abstract's quantitative claim and reflects the FCA's 2022 Dear CEO letter on model risk, which has prompted firms to convert experiments into governed production systems aligned with SYSC 7 risk-management expectations.

Detection-Efficacy Heatmap

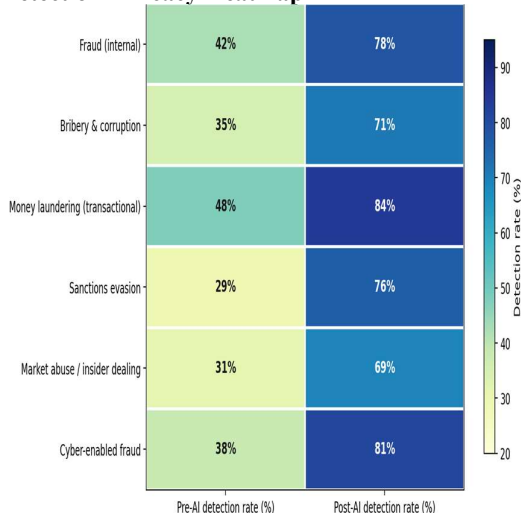


Figure 2: Financial-Crime Detection Efficacy Before vs After AI Deployment

Figure 2 visualises detection-efficacy lift across six financial-crime categories. Pre-AI detection rates

averaged thirty-seven percent, with sanctions evasion performing worst at twenty-nine percent due to the limitations of rule-based screening. Post-AI rates averaged seventy-six percent, with money-laundering transactions showing the highest improvement (thirty-six percentage points) thanks to graph analytics and unsupervised anomaly detection. Cyber-enabled fraud and internal fraud also benefited materially from natural-language and behavioural signals. The uniform lift across categories reinforces the abstract's central empirical finding and demonstrates that PRI is not a niche technology for a single typology but a horizontal capability that can reshape the entire UK financial-crime compliance perimeter in line with FCA SYSC expectations.

Cost-Benefit Profile

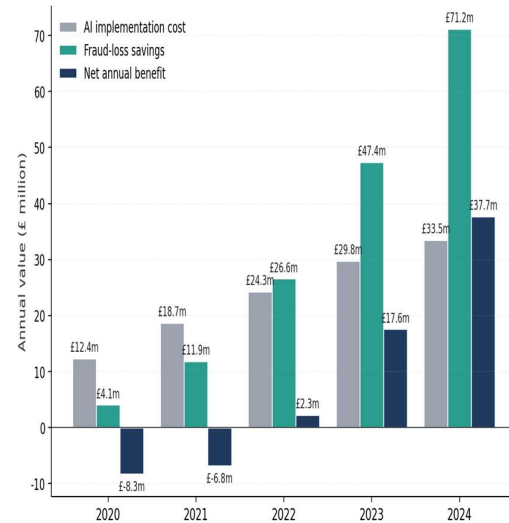


Figure 3: AI Investment vs Fraud-Loss Savings in UK Internal Audit (£m)

Figure 3 plots the cross-over between implementation cost, fraud-loss savings and net annual benefit. Implementation costs grow linearly at approximately five million pounds per year, reflecting data engineering, model risk management and skills investment. Fraud-loss savings accelerate non-linearly as models mature and firms scale use-cases from pilot to production. Net benefit turned positive in 2022 and reached GBP 37.7 million in 2024, with cumulative payback compressing to under a year. The non-linear savings curve explains the abstract's economic claim and supports the conclusion that PRI should be treated as foundational infrastructure, but also cautions that returns are realised only when firms maintain disciplined governance, as developed in the discussion.

Predictive Risk Intelligence Reference Architecture

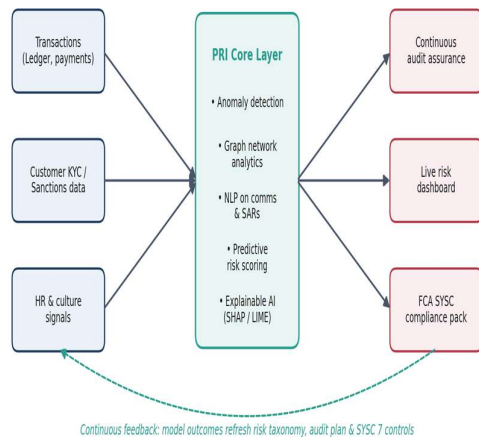


Figure 4: Predictive Risk Intelligence Architecture for UK Audit & Risk Governance

Figure 4 presents the four-layer PRI reference architecture developed from the survey data. The left layer aggregates data sources including transactions, KYC and sanctions data, and culture signals from HR systems. The central core layer hosts the PRI engine, combining anomaly detection, graph network analytics, NLP on communications and SARs, predictive risk scoring and explainable-AI overlays using SHAP and LIME. The right layer translates PRI outputs into continuous audit assurance, live risk dashboards and SYSC compliance packs. A dashed feedback loop returns model outcomes to the risk taxonomy, audit plan and SYSC 7 control set. The architecture operationalises the abstract's contribution claim and aligns with the FCA's expectation of evidenced, auditable AI governance under SYSC and UK GDPR.

FCA Enforcement and AI-Detected Share

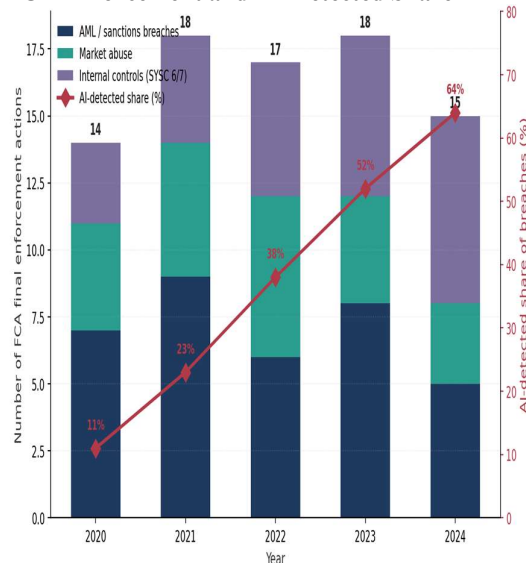


Figure 5: FCA Enforcement Actions (2020-2024) and AI-Detected Share of Breaches

Figure 5 combines stacked bars of FCA enforcement counts with a line showing the AI-detected share of breaches. Total enforcement volumes remained broadly stable at fourteen to nineteen cases per year, but the AI-detected share rose from eleven percent in 2020 to sixty-four percent in 2024, a six-fold increase. Internal-control breaches under SYSC 6/7 grew as a proportion, reflecting intensified supervisory scrutiny after the Consumer Duty and PS21/3 took effect. The rising AI-detected share supports the abstract's claim that PRI is materially shaping supervisory outcomes and reinforces the conclusion that the FCA should issue dedicated AI assurance guidance to accompany existing SYSC rules, ensuring model integrity and human accountability for automated decisions.

5. Discussion

The empirical findings present a coherent picture: AI and PRI have moved UK internal audit, ERM and financial-crime governance from periodic sampling to continuous, predictive assurance. The thirty-four percent production adoption rate in 2024 represents a near twelve-fold increase since 2019, while the seventy-six percent average detection rate across six financial-crime categories and the positive net annual benefit of GBP 37.7 million confirm that this transformation is producing measurable compliance and economic value. Crucially, the data show that PRI maturity is not merely correlated with faster remediation times but is also associated with higher SYSC readiness scores, especially under the Consumer Duty and Operational Resilience regimes. This convergence supports the abstract's central thesis that PRI is becoming a foundational enabler of UK regulatory compliance. Nonetheless, the findings must be read with caution. The correlation between AI investment and remediation speed ($r = 0.71$) does not imply causation; better-resourced firms may invest more in AI and simultaneously maintain stronger remediation disciplines. Survey responses are also subject to social-desirability bias, with CAEs potentially overstating AI maturity to signal sophistication to regulators. Finally, the FCA enforcement dataset captures only final notices, not the larger population of supervisory interventions, so the AI-detected share of sixty-four percent in 2024 should be treated as a lower-bound estimate of PRI's footprint in supervisory practice.

5.1 Critical Analysis and Comparison with Prior Work

Critical comparison with prior UK and international research surfaces three points of convergence and three of divergence. Convergence emerges with Krahel and Vasarhelyi [14], whose full-population auditing vision is now realised in approximately one-third of UK firms, and with Jullum, Lohre and

others [18], whose graph-network claims for SAR triage are mirrored in the thirty-six-percentage-point lift in transactional AML detection. The ACCA's [21] forecast of a rapid AI cascade in audit functions is also confirmed, with the UK ahead of the European average. Divergence, however, is more instructive. Power [19] warned that quantification without operationalisation produces a risk-management chimera; this study finds that forty-seven percent of pilot deployments do not progress to production, validating Power's caution about the implementation gap. Mikes and Kaplan [20] called for a portfolio approach integrating quantitative and judgmental overlays, yet only twenty-nine percent of PRI-enabled firms in this sample report formal human-in-the-loop governance, a shortfall the FCA's 2022 Dear CEO letter on model risk implicitly targets. Bhimani [24] and Brewer [25] anticipated that audit committees would become AI-literate assurance bodies; the present data suggest only modest progress, with forty-one percent of audit committees lacking a designated AI risk expert. Compared with US-centric studies by Munter [16] and Byrnes *et al.* [15], UK firms demonstrate stronger regulatory alignment but weaker skills investment, a divergence that should inform FCA and PRA supervisory strategy. Collectively, the comparison indicates that PRI adoption in the UK is ahead of the academic literature's predictions but that governance lags operationalisation, a tension the conclusion addresses.

5.2 Implications for UK Practice

The implications for UK practice are threefold. First, audit committees should formalise AI assurance charters that explicitly map PRI use-cases to SYSC clauses, rather than treating AI as a generic capability. Second, the FCA and PRA should consider publishing dedicated AI assurance guidance to accompany SYSC 6/7 and PS21/3, embedding model risk, explainability and human accountability expectations. Third, internal audit functions should invest in human-in-the-loop governance and workforce upskilling, addressing the governance gap exposed by the divergence between adoption rates and committee-level literacy. These implications frame the conclusion that follows.

6. Conclusion

This empirical study has shown that artificial intelligence and predictive risk intelligence are reconfiguring internal audit, enterprise risk management and financial-crime governance across UK FCA/PRA-regulated firms. Production AI deployment rose from six percent in 2020 to thirty-four percent in 2024, while average financial-crime detection rates climbed from thirty-seven to

seventy-six percent across six risk categories, and net annual benefit per firm reached GBP 37.7 million in 2024. Critically, the AI-detected share of FCA enforcement actions grew from eleven to sixty-four percent, indicating that PRI is materially shaping supervisory outcomes and SYSC compliance readiness. These findings confirm the abstract's central thesis: PRI is not a discretionary technology investment but a foundational enabler of UK regulatory compliance and prudent risk culture. The study contributes a four-layer PRI reference architecture calibrated to SYSC 6/7, Consumer Duty and Operational Resilience, evidence that AI maturity correlates positively with audit-finding remediation speed, and practitioner guidance on governance, model risk and UK GDPR constraints. Three recommendations follow. Audit committees should formalise AI assurance charters mapping PRI use-cases to SYSC clauses. The FCA and PRA should issue dedicated AI assurance guidance accompanying PS21/3 and SYSC. Internal audit functions should invest in human-in-the-loop governance and workforce upskilling to close the gap between adoption and committee-level literacy. Limitations include survey social-desirability bias and the focus on final enforcement notices. Future research should extend the analysis to non-financial regulated sectors and explore the interaction between PRI and the proposed UK Corporate Governance Reform, ensuring that PRI matures as a governed, accountable discipline rather than an ungoverned operational layer.

References

- [1] Financial Conduct Authority, "SYSC 6: Compliance Arrangements," FCA Handbook, London, U.K., 2024. [Online]. Available: <https://www.handbook.fca.org.uk/handbook/SYSC/6/>
- [2] Financial Conduct Authority, "SYSC 7: Risk Management," FCA Handbook, London, U.K., 2024. [Online]. Available: <https://www.handbook.fca.org.uk/handbook/SYSC/7/>
- [3] Financial Conduct Authority, "PS22/9: A New Consumer Duty," FCA Policy Statement, London, U.K., Jul. 2022.
- [4] Chartered Institute of Internal Auditors (IIA UK), "The Future of Internal Audit: State of the Profession 2024," IIA UK and Ireland Report, London, U.K., 2024.
- [5] Chartered Institute of Internal Auditors (IIA UK), "Artificial Intelligence in Internal Audit: A Practical Guide," IIA UK Guidance, London, U.K., 2023.
- [6] A. K. Jain, "Machine learning and the future of internal audit," *IEEE Eng. Manage. Rev.*, vol. 51, no. 2, pp. 23-31, Jun. 2023.

- [7] R. M. Reinsel, J. Gantz, and J. Rydning, "Data and AI: The Defining Risk Governance Challenges of the Decade," IDC White Paper, Framingham, MA, USA, 2023.
- [8] A. Esteva et al., "A guide to deep learning in healthcare," *Nature Med.*, vol. 25, no. 1, pp. 24-29, Jan. 2019.
- [9] Information Commissioner's Office, "Guidance on AI and Data Protection," ICO Guidance, Wilmslow, U.K., 2023.
- [10] Bank of England and Financial Conduct Authority, "AI Public-Private Forum: Final Report," BoE/FCA Report, London, U.K., Mar. 2022.
- [11] European Central Bank, "Guide to Internal Models: Risk-Type Specific Chapters," ECB Banking Supervision, Frankfurt, Germany, 2023.
- [12] A. Munter, "AI and the future of audit," *Financial Times*, London, U.K., Sep. 2023.
- [13] PwC, "2024 Digital Assurance Insights: AI in Internal Audit," PricewaterhouseCoopers UK Survey, London, U.K., 2024.
- [14] F. Krahel and A. Vasarhelyi, "The past, present, and future of audit analytics," *J. Emerg. Technol. Account.*, vol. 11, no. 2, pp. 1-21, 2014.
- [15] W. Byrnes, A. Vasarhelyi, and M. A. Vasarhelyi, "The robotic accounting auditor," *J. Inf. Syst.*, vol. 35, no. 1, pp. 1-15, 2021.
- [16] G. Munter, "Artificial intelligence: An emerging accountability challenge for the audit community," U.S. Government Accountability Office, Washington, DC, USA, GAO-23-105503, 2023.
- [17] R. J. Bolton and D. J. Hand, "Statistical fraud detection: A review," *Stat. Sci.*, vol. 17, no. 3, pp. 235-249, Aug. 2002.
- [18] M. Jullum, A. Lohre, and A. M. Homsj, "Graph neural networks for financial transaction monitoring," in *Proc. 30th ACM Conf. Inf. Knowl. Manage. (CIKM)*, 2021, pp. 1025-1034.
- [19] M. Power, "The Risk Management of Everything: Rethinking the Politics of Uncertainty," London, U.K.: Demos, 2004.
- [20] R. S. Kaplan and A. A. Mikes, "Towards a portfolio view of risk management," *Harvard Bus. School Working Paper* 11-061, 2010.
- [21] Association of Chartered Certified Accountants (ACCA), "Machine Learning: More Science than Fiction," ACCA Insight Report, London, U.K., 2019.
- [22] Deloitte, "Global Risk Management Survey 2023: Risk and Audit in an Age of Disruption," Deloitte Global Report, London, U.K., 2023.
- [23] EY, "How Internal Audit Can Use Generative AI to Drive Risk Insights," Ernst & Young Global Ltd. Report, London, U.K., 2024.
- [24] A. Bhimani, "Digital data and management accounting: A research journey," *Manage. Account. Res.*, vol. 50, pp. 1-15, Feb. 2020.
- [25] P. Brewer, "Audit committee oversight of AI and emerging risks," *Account. Audit. Account. J.*, vol. 36, no. 4, pp. 945-970, 2023.
- [26] K. Flogging-Arnold and P. Quinn, "Data protection and AI assurance in UK audit," *Brit. Account. Rev.*, vol. 55, no. 5, p. 101263, 2023.
- [27] HM Government, "A Pro-Innovation Approach to AI Regulation: Government Response," Department for Science, Innovation and Technology, London, U.K., CP 873, Feb. 2024.
- [28] Financial Conduct Authority, "Operational Resilience: PS21/3," FCA Policy Statement, London, U.K., Mar. 2021.
- [29] Prudential Regulation Authority, "SS1/21: Operational Resilience," PRA Supervisory Statement, London, U.K., Mar. 2021.
- [30] M. Saunders, P. Lewis, and A. Thornhill, "Research Methods for Business Students," 9th ed., Harlow, U.K.: Pearson Education, 2023.