

Artificial Intelligence and Financial Fraud Detection: Survey Evidence on Organizational Integrity and Risk Management from U.S. Professionals



Nasir Uddin ^{1*}, Abdul Kadir ², Md Yeasir Arafat ¹

Abstract

Background: The rapid digitization of financial systems has made fraud schemes more complex and harder to detect using traditional, rule-based methods, pushing organizations toward artificial intelligence (AI) as a more adaptive alternative. Yet empirical evidence on how AI capability relates to organizational integrity and risk management — particularly within U.S. organizations — remains limited. **Methods:** We conducted a cross-sectional survey of 145 professionals working in AI-exposed roles across U.S. financial, insurance, and technology organizations. Participants completed measures of AI Technology Readiness (AITR), Fraud Detection Capability (FDC), Organizational Integrity (OI), Risk Management Effectiveness (RME), and Financial Fraud Detection Performance (FFDP). Descriptive statistics, Pearson correlations, and multiple regression analysis were used to examine the hypothesized relationships. **Results:** All constructs correlated positively with FFDP. The regression model explained 75.2% of the variance in FFDP ($R^2 = .752$, Adjusted $R^2 = .745$; $F = 104.537$, $p < .001$). FDC was the strongest predictor ($\beta = .361$), followed by AITR ($\beta = .301$), RME ($\beta = .263$), and OI ($\beta = .227$); all relationships were statistically significant ($p < .001$). **Conclusion:** Financial fraud detection performance appears to depend not on AI capability alone, but on its integration with organizational

readiness, governance, and risk management practice. These findings offer modest but grounded empirical support for treating AI-driven fraud detection as a broader organizational capability rather than a standalone technical fix.

Keywords

Artificial Intelligence; Financial Fraud Detection; Organizational Integrity; Risk Management Effectiveness; Fraud Prevention

1. Introduction

Financial systems have changed faster in the last decade than perhaps any other era of business history, and not always for the better. Digital transformation has undeniably sharpened operational performance, quickened transaction processing, and reshaped how customers interact with financial institutions (Ogunmokun et al., 2021). Yet this same transformation has opened doors that fraud has been quick to walk through. Cyber fraud, identity theft, transaction manipulation, and financial statement fraud no longer operate as isolated threats — they increasingly intertwine, exploiting the same digital rails that make modern finance efficient (Ogunsola &

Significance | This study offers empirical, U.S.-based evidence linking AI readiness, fraud detection capability, governance, and risk management to fraud detection performance.

*Correspondence.

Nasir Uddin, College of Science and Society, University of Bridgeport, Bridgeport, CT, USA.
E-mail: nuddin@my.bridgeport.edu.

Editor Abdul Kadir Othman, Ph.D. And accepted by the Editorial Board Dec 09, 2026
(received for review Aug 31, 2026)

Author Affiliation:

¹ College of Science and Society, University of Bridgeport, Bridgeport, CT, USA.

² Ernest C. Trefz School of Business, University of Bridgeport, Bridgeport, CT, USA.

Please cite this article as: Uddin, N., Kadir, A., Arafat, M. Y. (2026). "Artificial Intelligence and Financial Fraud Detection: Survey Evidence on Organizational Integrity and Risk Management from U.S. Professionals", Journal of Primeasia, 7(1), 1-10, 10906

3064-9870 | Print/© 2026 (Journal of Primeasia), a publication of Eman Research, USA.
This is an open access article under the CC BY-NC-ND license.
(<http://creativecommons.org/licenses/by-nc-nd/4.0/>)
(<https://publishing.emanresearch.org>)

Balogun, 2021). The costs are not merely financial. Organizations that fall victim to sophisticated fraud schemes often find their reputations, stakeholder trust, and regulatory standing damaged in ways that outlast the immediate monetary loss (Chukwu, 2025).

It is worth pausing here on why traditional fraud detection has struggled to keep pace. Rule-based systems, however well-designed, are inherently reactive — they catch what they were built to catch, and fraud, almost by definition, evolves to avoid detection. Human analysts, for their part, are constrained by volume: they simply cannot review the sheer scale of transactions that modern financial systems generate in real time. This mismatch has pushed organizations, sometimes reluctantly, toward artificial intelligence as an alternative — not because AI is a silver bullet, but because it can process both structured and unstructured data at a scale and speed that static rule sets cannot match (Alghofaili et al., 2020).

What makes AI-based fraud detection genuinely useful is its capacity to learn. Machine learning and deep learning models can surface latent patterns in transactional data that would otherwise go unnoticed, and — perhaps more importantly for practitioners — they can reduce the false-positive burden that plagues many legacy systems (Polak et al., 2019). Predictive analytics, layered on top of anomaly detection, allows organizations to move from a purely reactive posture to one that anticipates emerging fraud typologies before they fully materialize (Forradellas & Gallastegui, 2021). This adaptability matters: AI systems that continue to learn from new data can, in principle, keep pace with fraud tactics that are themselves evolving, something static systems were never designed to do (Akyüz & Mavnacolu, 2021).

But detection capability alone does not tell the whole story. There is a broader organizational dimension here that is easy to overlook. AI-based monitoring, when implemented well, can strengthen internal controls, improve visibility across business units, and support the kind of regulatory compliance that boards and auditors increasingly demand (Noreen et al., 2023; Fedyk et al., 2022). Risk management, too, stands to benefit — not just from faster detection, but from the ongoing risk assessments, forecasting, and early-warning capabilities that AI tools can enable (Waqas et al., 2022). Taken together, these capabilities suggest that AI's contribution to organizational integrity is not incidental; it may be foundational to how forward-looking organizations build resilience in an

increasingly complex operating environment (Nuhui & Aliu, 2023).

And yet, for all the conceptual and industry-level attention this topic has received, empirical research grounded in the actual experiences of professionals working inside U.S. organizations remains surprisingly thin — a gap that feels somewhat at odds with how extensively American firms have adopted AI in financial operations and governance (Johnson et al., 2021). Much of the existing literature leans conceptual or draws on international samples where regulatory and technological contexts differ meaningfully from the U.S. setting. This is not a minor omission. Without empirical grounding specific to this context, claims about AI's organizational benefits risk remaining aspirational rather than evidence-based (Castillo & Taherdoost, 2023).

This study attempts to address that gap directly. We examine how AI Technology Readiness (AITR), Fraud Detection Capability (FDC), Organizational Integrity (OI), and Risk Management Effectiveness (RME) relate to Financial Fraud Detection Performance (FFDP), drawing on survey data from 145 professionals across a range of U.S. organizations. Using descriptive statistics, correlation analysis, and multiple regression, we test the proposed relationships among these constructs. In doing so, we hope to offer not just another conceptual argument for AI adoption, but a modest, empirically grounded contribution — one that speaks to managers and policymakers who are trying to translate the promise of AI-driven fraud detection into practical governance and risk management strategies.

2. Materials and Methods

2.1 Study Design

We used a cross-sectional, quantitative survey design to examine the relationships among AI Technology Readiness (AITR), Fraud Detection Capability (FDC), Organizational Integrity (OI), Risk Management Effectiveness (RME), and Financial Fraud Detection Performance (FFDP). A quantitative design was chosen deliberately — it allowed us to test hypothesized relationships statistically rather than simply describing perceptions, which is where much of the existing literature has stopped short (Prasad & Rohokale, 2019). It is worth being upfront that a cross-sectional design captures a single point in time; it cannot establish temporal precedence or rule out reverse causality, a limitation we

return to in the Discussion.

2.2 Hypotheses

Based on the theoretical rationale developed in the Introduction, we tested the following hypotheses:

H1: AI Technology Readiness is positively associated with Financial Fraud Detection Performance.

H2: Fraud Detection Capability is positively associated with Financial Fraud Detection Performance.

H3: Organizational Integrity is positively associated with Financial Fraud Detection Performance.

H4: Risk Management Effectiveness is positively associated with Financial Fraud Detection Performance.

2.3 Setting, Recruitment, and Sampling Period

Participants were recruited via professional networking platforms and corporate communication channels between [insert start date] and [insert end date]. We used non-probability purposive sampling (Ceylan, 2022), targeting individuals in roles plausibly exposed to AI-based fraud detection systems: finance managers, internal auditors, accountants, compliance officers, cybersecurity specialists, risk managers, and AI professionals, working within banking, financial services, insurance, information technology, and other corporate sectors in the United States.

Inclusion criteria: current employment in a qualifying role, at a U.S.-based organization, with direct or indirect functional exposure to AI-enabled financial fraud detection systems.

Exclusion criteria: incomplete responses, responses failing attention-check items [if used — please confirm], and respondents located outside the United States.

2.4 Sample Size

A total of [insert number invited/reached] individuals were approached; 145 complete and valid responses remained after data screening and quality assessment.

2.5 Measures

The questionnaire comprised two parts. Part one collected demographic and organizational information (gender, age,

education, years of experience). Part two measured six constructs — AITR, FDC, OI, RME, FFDP, and Organizational Performance (OP) — using items adapted from established scales in the literature (Alkhyoon et al., 2023; Tarjo et al., 2022), modified for this study's context. Each item was rated on a 5-point Likert scale (1 = Strongly Disagree, 5 = Strongly Agree).

2.6 Reliability and Validity

Internal consistency was assessed using Cronbach's alpha:

$$= [k / (k - 1)] \times [1 - (T^2 / T^2)]$$

Where:

- = Cronbach's alpha (reliability coefficient)
- k = number of items/questions
- σ^2 = variance of item i
- T^2 = total variance of the test/scale
- $\sum \sigma^2$ = sum of individual item variances across all k items

where k is the number of items, σ^2 is the variance of each item, and T^2 is the total scale variance. Values above 0.70 were treated as acceptable (Taherdoost, 2021). Convergent validity was evaluated using Composite Reliability (CR) and Average Variance Extracted (AVE) (Mousavi et al., 2022).

2.7 Statistical Analysis

All analyses were conducted in IBM SPSS Statistics, Version 29 (IBM Corp., Armonk, NY, USA). We proceeded in four stages: (1) descriptive statistics to characterize the sample and variable distributions (Pirson & Turnbull, 2011); (2) reliability and convergent validity testing as described above; (3) Pearson correlation analysis to examine bivariate relationships and screen for multicollinearity (Huang et al., 2016); and (4) multiple regression analysis, with FFDP regressed on AITR, FDC, OI, and RME (Anton & Nucu, 2020), specified as:

$$\text{FFDP} = + \text{AITR} + \text{FDC} + \text{OI} + \text{RME} + \text{Error Term} \quad (\text{Equation 2})$$

Where:

- **FFDP** = dependent variable (outcome being predicted)

Table 1. Demographic characteristics of survey respondents (N = 145). Values represent frequency (n) and percentage (%) of respondents in each category. Percentages were calculated within each demographic variable and may not sum to exactly 100% due to rounding. Data were collected via a single cross-sectional online survey of professionals in AI-exposed financial roles across U.S.-based organizations (see Section 2.3 for recruitment and eligibility criteria).

Variable	Category	Frequency (n)	Percentage (%)
Gender	Male	86	59.3
	Female	59	40.7
Age (Years)	25–34	30	20.7
	35–44	48	33.1
	45–54	42	29.0
	55 and above	25	17.2
Educational Qualification	Bachelor's Degree	34	23.4
	Master's Degree	68	46.9
	Doctoral Degree	43	29.7
Work Experience	Less than 5 years	28	19.3
	5–10 years	49	33.8
	11–15 years	39	26.9
	More than 15 years	29	20.0

Table 2. Descriptive statistics for the six study constructs (N = 145). Mean and standard deviation (SD) values are reported on a 5-point Likert scale (1 = Strongly Disagree, 5 = Strongly Agree), averaged across all items within each construct. Skewness and kurtosis values are reported to support the assumption of approximate normality for subsequent parametric analyses (all values fell within the conventionally accepted range of 1 to +1). AIA = Artificial Intelligence Adoption; FDC = Fraud Detection Capability; OI = Organizational Integrity; RME = Risk Management Effectiveness; FFP = Financial Fraud Prevention; OP = Organizational Performance.

Variable	Mean	SD	Skewness	Kurtosis
Artificial Intelligence Adoption (AIA)	4.18	0.56	-0.48	-0.31
Fraud Detection Capability (FDC)	4.11	0.59	-0.42	-0.27
Organizational Integrity (OI)	4.07	0.61	-0.36	-0.18
Risk Management Effectiveness (RME)	4.14	0.57	-0.44	-0.29
Financial Fraud Prevention (FFP)	4.23	0.53	-0.55	-0.34
Organizational Performance (OP)	4.09	0.58	-0.39	-0.21

= intercept (constant term)

• , , , = coefficients for each predictor variable

• **AITR, FDC, OI, RME** = independent/predictor variables

• = error term (residual)

Statistical significance was set at $\alpha = .05$ (two-tailed). Model diagnostics included variance inflation factors ($VIF < 5$ as the threshold for acceptable multicollinearity) and the Durbin–Watson statistic to assess autocorrelation in residuals (Shi et al., 2016).

3. Results

3.1 Sample Characteristics (Table 1)

Of the 145 respondents, 59.3% identified as male and 40.7% as female (Table 1). Most were in the 35–44 age bracket (33.1%), followed by 45–54 (29.0%), 25–34 (20.7%), and 55 and above (17.2%). Nearly half held a master's degree (46.9%), with doctoral (29.7%) and bachelor's degree holders (23.4%) making up the remainder. Work experience was fairly evenly distributed, with the largest group reporting 5–10 years (33.8%). Taken together, the sample skews toward mid-career, well-educated professionals — a composition that arguably strengthens confidence in their familiarity with AI-based fraud systems, though it also means the findings may not generalize as cleanly to less experienced staff.

3.2 Descriptive Statistics (Table 2)

Every construct averaged above the scale midpoint of 4.00, suggesting a generally favorable view of AI-enabled fraud detection across the sample. Financial Fraud Prevention scored highest ($M = 4.23$, $SD = 0.53$), followed by AI Adoption ($M = 4.18$), Risk Management Effectiveness ($M = 4.14$), Fraud Detection Capability ($M = 4.11$), Organizational Performance ($M = 4.09$), and Organizational Integrity ($M = 4.07$) (Table 2). Skewness (0.55 to 0.36) and kurtosis (0.34 to 0.18) values fell within acceptable ranges for normality, supporting the use of parametric inferential tests.

3.3 Perceptions of AI-Driven Fraud Detection (Table 3)

A little over half of respondents (53.8%) reported full AI integration into their organization's operations, while 33.8% described partial adoption and 12.4% reported none at all (Table 3). Perceptions of system accuracy followed a similar pattern — 56.6% rated their AI fraud

detection systems as highly accurate. Real-time monitoring was viewed favorably by 55.2% of respondents, and just over half (51.0%) considered AI an excellent fraud detection tool overall. These figures suggest a workforce that is, on balance, more confident than skeptical about AI's role here — though the fact that roughly one in eight respondents reported low adoption or low accuracy is not a trivial minority and arguably deserves more attention than a passing mention.

3.4 Risk Management Practices (Figure 1)

Enterprise Risk Assessment was the most frequently cited practice (22.1%), followed by fraud risk monitoring (19.3%), cybersecurity risk controls (17.2%), regulatory compliance management (15.2%), operational risk mitigation (13.8%), and business continuity planning (12.4%) (Figure 1). The relatively even spread across these categories hints that organizations are not relying on any single risk practice in isolation, but are distributing effort across a broader risk management portfolio.

3.5 Correlations Among Study Variables (Figure 2)

All bivariate correlations were positive, consistent with the hypothesized relationships (Figure 2). FDC showed the strongest association with FFDP ($r = .771$), followed by FFDP's association with Organizational Performance ($r = .752$) and AITR's association with FFDP ($r = .748$). RME ($r = .736$) and OI ($r = .724$) also correlated meaningfully with FFDP. All coefficients remained below the .80 threshold commonly used as a rule-of-thumb ceiling for multicollinearity concern, which gave us reasonable — if not absolute — confidence in proceeding to regression.

3.6 Regression Analysis (Table 4)

The regression model was statistically significant, $F(4, 140) = 104.537$, $p < .001$, explaining 75.2% of the variance in FFDP ($R^2 = .752$, Adjusted $R^2 = .745$) (Table 4). Among the predictors, FDC emerged as the strongest ($\beta = .361$, $p < .001$), supporting H2. AITR was the next strongest predictor ($\beta = .301$, $p < .001$), supporting H1. RME ($\beta = .263$, $p < .001$) and OI ($\beta = .227$, $p < .001$) also contributed significantly, supporting H3 and H4. All VIF values remained below 2.0, and the Durbin–Watson statistic (1.982) indicated no meaningful autocorrelation among residuals — both reassuring signs for the model's stability, even if they do not fully rule out common-method variance given the single-source, single-time-point design.

Table 3. Respondent perceptions of AI-driven financial fraud detection (N = 145). Values represent frequency (n) and percentage (%) of respondents rating each dimension as Low, Moderate, or High, based on aggregated Likert-scale responses (see Section 2.5 for scale anchors). Dimensions assessed include overall level of AI adoption, perceived accuracy of AI-based fraud detection, effectiveness of real-time fraud monitoring, and confidence in AI-based fraud prediction capability.

Variable	Category	Frequency (n)	Percentage (%)
Level of AI Adoption	Low	18	12.4
	Moderate	49	33.8
	High	78	53.8
Accuracy of AI Fraud Detection	Low	16	11.0
	Moderate	47	32.4
	High	82	56.6
Real-Time Fraud Monitoring	Low	20	13.8
	Moderate	45	31.0
	High	80	55.2
AI-Based Fraud Prediction Capability	Low	19	13.1
	Moderate	52	35.9
	High	74	51.0

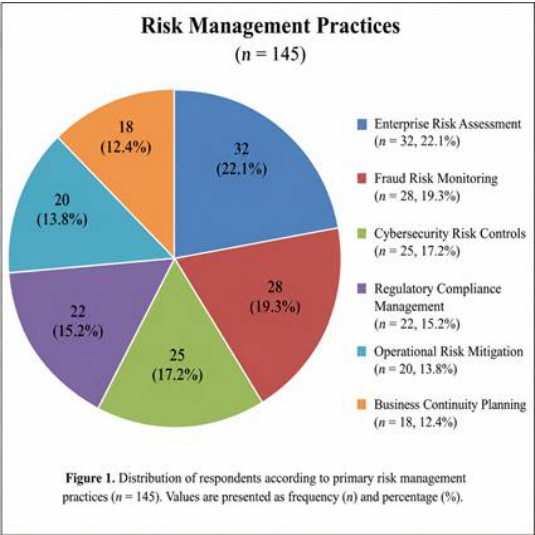


Figure 1. Distribution of risk management practices reported by respondents (N = 145). Bars represent the percentage of respondents identifying each practice as part of their organization's risk management approach: Enterprise Risk Assessment, Fraud Risk Monitoring, Cybersecurity Risk Controls, Regulatory Compliance Management, Operational Risk Mitigation, and Business Continuity Planning. Respondents could select more than one practice; percentages reflect the proportion of the total response set attributable to each category rather than mutually exclusive counts.

4. Discussion

4.1 Fraud Detection Capability as the Strongest Predictor

Perhaps unsurprisingly, Fraud Detection Capability carried the most weight in predicting FFDP ($\beta = .361$; $r = .771$) (Table 4; Figure 2). This aligns with the broader argument that organizations investing in continuous monitoring and advanced analytical tools are better positioned to catch anomalous transactions before they escalate (Razali & Arshad, 2014). AI's contribution here seems to lie less in replacing human judgment and more in extending its reach — enabling instantaneous monitoring and pattern forecasting at a scale no analyst team could match alone (Shi et al., 2016).

4.2 The Role of AI Technology Readiness

AITR was the second-strongest predictor ($\beta = .301$; $r = .748$), a finding that echoes prior calls for organizations to build the underlying infrastructure and workforce capability needed to support AI adoption (Achmad et al., 2022). It is tempting to read this as confirmation that “readiness precedes results” — organizations that have already invested in data infrastructure and skilled personnel appear better equipped to deploy machine learning and predictive analytics effectively for fraud prevention (Power, 2012).

4.3 Risk Management Effectiveness

RME's contribution ($\beta = .263$; $r = .736$) suggests that AI-driven detection tools deliver more value when embedded within a broader enterprise risk management structure rather than operating as a standalone technology (DeZoort & Harrison, 2016). This is consistent with the view that AI functions best as a support mechanism — augmenting existing governance processes such as risk assessment, monitoring, and compliance tracking — rather than as an independent solution (King et al., 2021).

4.4 Organizational Integrity: The Smallest, but Still Meaningful, Effect

Organizational Integrity showed the weakest standardized effect among the four predictors ($\beta = .227$), yet it remained statistically significant ($p < .001$) with a still-substantial correlation ($r = .724$) (Table 4). This is worth sitting with for a moment: even the “weakest” predictor here is not weak in any absolute sense. It suggests that ethical governance and compliance culture matter for fraud detection outcomes, even if their contribution is somewhat smaller

than more technical or capability-driven factors (Chukwu, 2025). A credible integrity framework may function less as a direct detection mechanism and more as an enabling condition — supporting responsible AI use, reducing internal vulnerabilities, and reinforcing stakeholder trust (Achmad et al., 2022).

4.5 Integration and Practical Implications

Taken as a whole, these findings point toward AI-driven fraud detection as something closer to an organizational capability than a discrete tool — one that depends on the interplay of technical readiness, detection capacity, governance, and risk management working in concert. For managers, this suggests that isolated investment in AI software, without corresponding attention to readiness, integrity, and risk infrastructure, may fall short of its potential. For policymakers, it reinforces the case for encouraging holistic AI governance frameworks rather than narrowly technical mandates.

4.6 Limitations

Several limitations deserve mention. The cross-sectional design precludes causal inference — we can describe associations, not confirm direction or rule out reverse causality. All constructs were measured via self-report from the same respondents at the same time, raising the possibility of common method bias; a Harman's single-factor test or marker-variable approach in future work would help address this directly. The purposive, non-probability sampling approach, while appropriate for reaching knowledgeable respondents, limits generalizability beyond similarly positioned U.S. professionals. Finally, reliance on perceptual measures of “accuracy” and “effectiveness,” rather than objective fraud-detection outcome data, means our findings speak to perceived rather than verified performance.

4.7 Future Research

Future studies might incorporate longitudinal designs to establish temporal precedence, objective fraud-detection metrics (e.g., actual fraud caught vs. missed) alongside perceptual measures, and cross-national samples to test whether these relationships hold outside the U.S. regulatory context.

5. Conclusion

This study set out to examine whether AI Technology Readiness, Fraud Detection Capability, Organizational

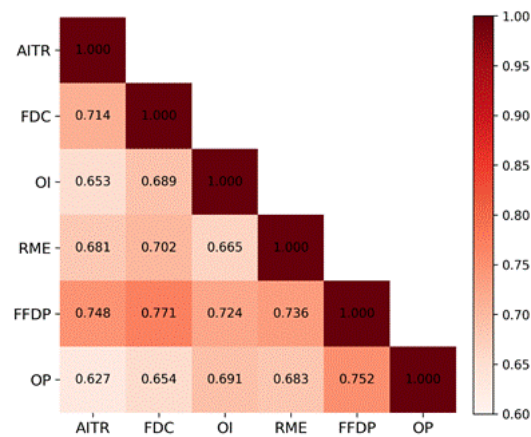


Figure 2. Pearson correlation matrix of the study constructs ($N = 145$). Cell values represent Pearson correlation coefficients (r) between pairs of constructs: AI Technology Readiness (AITR), Fraud Detection Capability (FDC), Organizational Integrity (OI), Risk Management Effectiveness (RME), Financial Fraud Detection Performance (FFDP), and Organizational Performance (OP). All correlations were positive and statistically significant at $p < .001$ unless otherwise indicated. Coefficients below .80 indicate no severe multicollinearity concerns among predictor variables prior to regression modeling (see Table 4).

Table 4. Multiple regression analysis predicting Financial Fraud Detection Performance (FFDP) ($N = 145$). Unstandardized regression coefficients (B), standard errors (SE), standardized coefficients (β), t -values, significance levels ($Sig.$), and variance inflation factors (VIF) are reported for each predictor. Model fit statistics (R , R^2 , Adjusted R^2 , standard error of the estimate, F -ratio, and Durbin–Watson statistic) are reported below the coefficient table. AITR = AI Technology Readiness; FDC = Fraud Detection Capability; OI = Organizational Integrity; RME = Risk Management Effectiveness. All VIF values were below the conventional threshold of 5, indicating no problematic multicollinearity; the Durbin–Watson statistic (1.982) indicated no meaningful autocorrelation among residuals. Significance was assessed at $\alpha = .05$ (two-tailed).

Predictor	B	SE		t	Sig.	VIF
Constant	0.526	0.241	–	2.183	0.031	–
AITR	0.289	0.056	0.301	5.161	<0.001	1.71
FDC	0.342	0.061	0.361	5.607	<0.001	1.83
OI	0.218	0.054	0.227	4.037	<0.001	1.62
RME	0.251	0.058	0.263	4.328	<0.001	1.69

Integrity, and Risk Management Effectiveness meaningfully relate to Financial Fraud Detection Performance among U.S. professionals — and the evidence, on balance, says yes. Each construct contributed significantly to the regression model, with Fraud Detection Capability emerging as the strongest predictor and Organizational Integrity the weakest, though still meaningful. What this suggests, tentatively, is that effective fraud detection is less a matter of deploying AI in isolation and more a matter of aligning technical readiness with governance and risk management practice. Organizations hoping to strengthen their fraud defenses might do well to treat these four elements as interdependent rather than separable investments. Given the cross-sectional design and single-source data, these conclusions should be read as an early empirical signal rather than definitive proof — one that future longitudinal and multi-source research could usefully build upon.

Acknowledgements

The authors N.U.et al., thank all survey participants who generously contributed their time and professional insight to this study. The authors also thank the University of Bridgeport for institutional support during the conduct of this research.

Author Contributions

N.U.: conceptualization, methodology, data collection, formal analysis, writing – original draft. A.K.: methodology, supervision, writing – review & editing. M.Y.A.: data curation, formal analysis, writing – review & editing.

Competing Financial Interests

The authors N.U.et al., declare no competing financial interests.

References

- Achmad, T., Ghazali, I., & Pamungkas, I. D. (2022). Hexagon Fraud: Detection of Fraudulent Financial Reporting in State-Owned Enterprises Indonesia. *Economies*, 10(1), 13. <https://doi.org/10.3390/economies10010013>
- Akyüz, A., & Mavnacioglu, K. (2021). Marketing and financial services in the age of artificial intelligence. In *Contributions to Finance and Accounting* (pp. 327–340). https://doi.org/10.1007/978-3-030-68612-3_23
- Alghofaili, Y., Albattah, A., & Rassam, M. A. (2020). A financial fraud detection model based on LSTM deep learning technique. *Journal of Applied Security Research*, 15(4), 498–516. <https://doi.org/10.1080/19361610.2020.1815491>
- Alkhyyoon, H., Abbaszadeh, M. R., & Zadeh, F. N. (2023). Organizational Risk Management and Performance from the Perspective of Fraud: A Comparative Study in Iraq, Iran, and Saudi Arabia. *Journal of Risk and Financial Management*, 16(3), 205. <https://doi.org/10.3390/jrfm16030205>
- Anton, S. G., & Nucu, A. E. A. (2020). Enterprise Risk Management: A Literature Review and Agenda for Future Research. *Journal of Risk and Financial Management*, 13(11), 281. <https://doi.org/10.3390/jrfm13110281>
- Arena, M., Arnaboldi, M., & Azzone, G. (2010). The organizational dynamics of Enterprise Risk Management. *Accounting, Organizations and Society*, 35(7), 659–675. <https://doi.org/10.1016/j.aos.2010.07.003>
- Castillo, M. J., & Taherdoost, H. (2023). The impact of AI technologies on E-Business. *Encyclopedia*, 3(1), 107–121. <https://doi.org/10.3390/encyclopedia3010009>
- Ceylan, I. E. (2022). The effects of artificial intelligence on the insurance sector: Emergence, applications, challenges, and opportunities. In *Accounting, Finance, Sustainability, Governance & Fraud* (pp. 225–241). https://doi.org/10.1007/978-981-16-8997-0_13
- Chukwu, B. N. (2025). AI-Driven Risk Management: Strengthening cybersecurity and market stability in the US financial sector. *World Journal of Advanced Research and Reviews*, 28(1), 1967–1976. <https://doi.org/10.30574/wjarr.2025.28.1.3647>
- DeZoort, F. T., & Harrison, P. D. (2016). Understanding auditors' sense of responsibility for detecting fraud within organizations. *Journal of Business Ethics*, 149(4), 857–874. <https://doi.org/10.1007/s10551-016-3064-3>
- Fedyk, A., Hodson, J., Khimich, N., & Fedyk, T. (2022). Is artificial intelligence improving the audit process? *Review of Accounting Studies*, 27(3), 938–985. <https://doi.org/10.1007/s11142-022-09697-x>
- Forradellas, R. F. R., & Gallastegui, L. M. G. (2021). Digital Transformation and Artificial Intelligence applied to Business: Legal regulations, economic impact and perspective. *Laws*, 10(3), 70. <https://doi.org/10.3390/laws10030070>
- Huang, S. Y., Lin, C., Chiu, A., & Yen, D. C. (2016). Fraud detection using fraud triangle risk factors. *Information Systems Frontiers*, 19(6), 1343–1356. <https://doi.org/10.1007/s10796-016-9647-9>
- Johnson, M., Jain, R., Brennan-Tonetta, P., Swartz, E., Silver, D., Paolini, J., Mamonov, S., & Hill, C. (2021). Impact of big data and artificial intelligence on industry: Developing a workforce roadmap for a data driven economy. *Global Journal of Flexible Systems Management*, 22(3), 197–217. <https://doi.org/10.1007/s40171-021-00272-y>
- King, T. C., Aggarwal, N., Taddeo, M., & Floridi, L. (2021). Artificial Intelligence Crime: An interdisciplinary analysis of foreseeable threats and solutions. In *Philosophical Studies Series* (pp. 251–282). https://doi.org/10.1007/978-3-030-81907-1_13
- Mousavi, M., Zimon, G., Salehi, M., & Stepnicka, N. (2022). The effect of corporate governance structure on fraud and money laundering. *Risks*, 10(9), 176. <https://doi.org/10.3390/risks10090176>
- Noreen, U., Shafique, A., Ahmed, Z., & Ashfaq, M. (2023). Banking 4.0: Artificial Intelligence (AI)

- in Banking Industry & Consumer's Perspective. *Sustainability*, 15(4), 3682. <https://doi.org/10.3390/su15043682>
- Nuhiu, A., & Aliu, F. (2023). The benefits of combining AI and blockchain in enhancing decision-making in banking industry. In *EAI/Springer Innovations in Communication and Computing* (pp. 305–326). https://doi.org/10.1007/978-3-031-35751-0_22
- Ogunmokun, A. S., Balogun, E. D., & Ogunsola, K. O. (2021). A conceptual framework for AI-driven financial risk management and corporate governance optimization. *International Journal of Multidisciplinary Research and Growth Evaluation*, 2(1), 772–780. <https://doi.org/10.54660/ijmrge.2021.2.1.772-780>
- Ogunsola, K. O., & Balogun, E. D. (2021). Enhancing financial integrity through an advanced internal audit risk assessment and governance model. *International Journal of Multidisciplinary Research and Growth Evaluation*, 2(1), 781–790. <https://doi.org/10.54660/ijmrge.2021.2.1.781-790>
- Pirson, M., & Turnbull, S. (2011). Corporate Governance, Risk Management, and the Financial Crisis: An Information Processing view. *Corporate Governance: An International Review*, 19(5), 459–470. <https://doi.org/10.1111/j.1467-8683.2011.00860.x>
- Polak, P., Nelischer, C., Guo, H., & Robertson, D. C. (2019). "Intelligent" finance and treasury management: What we can expect. *AI & Society*, 35(3), 715–726. <https://doi.org/10.1007/s00146-019-00919-6>
- Power, M. (2012). The apparatus of fraud risk. *Accounting, Organizations and Society*, 38(6–7), 525–543. <https://doi.org/10.1016/j.aos.2012.07.004>
- Prasad, R., & Rohokale, V. (2019). Artificial intelligence and machine learning in cyber security. In *Springer Series in Wireless Technology* (pp. 231–247). https://doi.org/10.1007/978-3-030-31703-4_16
- Rawindaran, N., Jayal, A., & Prakash, E. (2021). Machine Learning Cybersecurity adoption in small and medium enterprises in developed countries. *Computers*, 10(11), 150. <https://doi.org/10.3390/computers10110150>
- Razali, W. A. A. W. M., & Arshad, R. (2014). Disclosure of corporate governance structure and the likelihood of fraudulent financial reporting. *Procedia - Social and Behavioral Sciences*, 145, 243–253. <https://doi.org/10.1016/j.sbspro.2014.06.032>
- Shi, W., Connelly, B. L., & Hoskisson, R. E. (2016). External corporate governance and financial fraud: Cognitive evaluation theory insights on agency theory prescriptions. *Strategic Management Journal*, 38(6), 1268–1286. <https://doi.org/10.1002/smj.2560>
- Soni, N., Sharma, E. K., Singh, N., & Kapoor, A. (2020). Artificial intelligence in business: From research and innovation to market deployment. *Procedia Computer Science*, 167, 2200–2210. <https://doi.org/10.1016/j.procs.2020.03.272>
- Taherdoost, H. (2021). A Review on Risk Management in Information Systems: Risk Policy, control and Fraud Detection. *Electronics*, 10(24), 3065. <https://doi.org/10.3390/electronics10243065>
- Tarjo, T., Vidyantana, H. V., Anggono, A., Yuliana, R., & Musyarofah, S. (2022). The effect of enterprise risk management on prevention and detection fraud in Indonesia's local government. *Cogent Economics & Finance*, 10(1). <https://doi.org/10.1080/23322039.2022.2101222>
- Villar, A. S., & Khan, N. (2021). Robotic process automation in banking industry: A case study on Deutsche Bank. *Journal of Banking and Financial Technology*. <https://doi.org/10.1007/s42786-021-00030-9>
- Waqas, M., Tu, S., Halim, Z., Rehman, S. U., Abbas, G., & Abbas, Z. H. (2022). The role of artificial intelligence and machine learning in wireless networks security: Principle, practice and challenges. *Artificial Intelligence Review*, 55(7), 5215–5261. <https://doi.org/10.1007/s10462-022-10143-2>
- Yan, X. (2023). Research on financial field integrating artificial intelligence: Application basis, case analysis, and SVR model-based overnight. *Applied Artificial Intelligence*, 37(1). <https://doi.org/10.1080/08839514.2023.2222258>