The Roles of Regulatory Pressure, Organisational Support, and Data Quality in AI Capability Development for Fraud Reduction in Financial Institutions

Agnes Bieattant[1], Gatot Soepriyanto[2]
[1]Master of Accounting, School of Accounting, Bina Nusantara University, Jakarta, Indonesia
[2]Accounting Department, School of Accounting, Bina Nusantara University, Jakarta, Indonesia

Article Info

Article history:

Received 2026-06-03
Revised 2026-07-21
Accepted 2026-07-23

Keywords:

AI Capability
Artificial Intelligence
Fraud Reduction
Regulatory Pressure
TOE Framework

ABSTRACT

The rapid expansion of digital financial services in Indonesia has increased fraud risks and intensified demands for technological transformation. Although artificial intelligence (AI) is increasingly applied in fraud detection, the process through which governance conditions contribute to fraud reduction remains insufficiently understood. This study examines the development of AI capabilities within Indonesian financial institutions by integrating the Technology–Organization–Environment (TOE) framework and the Information Systems Success Model. AI capability development is conceptualized through three stages: AI Integration, AI Assimilation, and AI Effectiveness. Survey data were analyzed using Partial Least Squares Structural Equation Modeling (PLS-SEM). The findings show that regulatory pressure does not directly improve fraud reduction outcomes. Instead, regulatory and organizational conditions support Data Quality, facilitating AI Integration and strengthening subsequent AI capability development. Fraud reduction is achieved only when AI systems reach operational effectiveness. The results suggest that fraud reduction represents an outcome of organizational capability development rather than a direct consequence of regulatory pressure or technological implementation alone.

Corresponding Author:

Agnes Bieattant
Master of Accounting, School of Accounting, Bina Nusantara University, Jakarta, Indonesia
Email: agnes.bieattant@binus.ac.id

1. INTRODUCTION

The rapid digitalization of financial services has transformed financial institutions into highly data-driven environments, particularly in emerging markets with accelerated fintech adoption and expanding digital payment ecosystems. While digital transformation improves efficiency and financial inclusion, it also amplifies exposure to increasingly sophisticated fraud risks [1], [2], [3]. The growing complexity of digital transactions has rendered traditional rule-based fraud-detection mechanisms insufficient for addressing adaptive, technology-enabled fraud schemes. Artificial intelligence (AI) has emerged as a key tool for fraud detection, enabling real-time monitoring, anomaly detection, and predictive risk assessment using large-scale transactional data [4]. However, empirical evidence shows that AI adoption does not consistently translate into measurable reductions in fraud across organizations [5]. Although AI systems enhance fraud detection capabilities, organizational benefits arise only when detection effectiveness leads to measurable reductions in fraud incidents and financial losses [6].

Fraud detection, therefore, represents a technological capability, whereas fraud reduction reflects an organizational performance outcome. This distinction suggests that the effectiveness of AI depends not only on technological sophistication but on how it is embedded within organizational processes and governance structures. Financial institutions may adopt advanced AI systems yet fail to achieve meaningful fraud mitigation when these technologies are not effectively integrated into organizational processes and governance mechanisms [7], [8]. Thus, it becomes essential to examine how AI-enabled detection capabilities are translated into operational effectiveness that ultimately produces fraud reduction outcomes.

These challenges are particularly pronounced in emerging market economies, where rapid technological expansion often exceeds organizational capability development and regulatory readiness [9]. Indonesia represents one of the fastest-growing digital financial ecosystems in Southeast Asia, characterized by accelerating fintech innovation, expanding digital payment usage, and ongoing regulatory transformation aimed at strengthening financial system resilience [10]. Financial institutions in Indonesia face increasing supervisory expectations to enhance fraud prevention and risk governance while simultaneously developing internal technological capabilities. In such contexts, the effectiveness of AI-based fraud detection may depend not merely on technology adoption, but also on how governance structures support organizational preparedness and operational use [11]. Existing studies predominantly emphasize algorithmic performance and analytical accuracy, while comparatively limited attention has been devoted to governance and organizational mechanisms that determine whether AI systems generate meaningful operational value.

Recent AI governance research emphasizes that effective deployment requires accountability structures, data governance practices, and institutional oversight embedded throughout the AI lifecycle [12]. Regulatory developments, such as the European Union Artificial Intelligence Act and regional governance initiatives, signal a global transition from technology-driven adoption to governance-driven AI implementation [13]. Complementary international initiatives, including regional guidelines such as the ASEAN Guide on AI Governance and Ethics, further emphasize responsible AI deployment through institutional readiness, risk assessment, and organizational oversight [14]. However, regulatory pressure may also lead to symbolic adoption, where organizations implement AI primarily for compliance purposes without achieving operational effectiveness [15]. Although the use of artificial intelligence for fraud detection continues to expand, empirical evidence remains limited in explaining how governance conditions facilitate AI capability development and translate into measurable reductions in fraud, particularly in financial institutions operating in emerging markets.

This study addresses this gap by examining the role of governance in AI adoption for fraud reduction, in which regulatory pressure and organisational support enhance Data Quality, enabling AI Integration, assimilation, and effectiveness, ultimately leading to fraud reduction. Using survey data from Indonesian financial institutions analyzed using PLS-SEM, this study demonstrates that fraud reduction is not driven solely by AI adoption, but by how financial institutions support effective AI implementation through regulatory alignment, organisational support, and Data Quality management.

2. LITERATURE REVIEW & HYPOTHESIS DEVELOPMENT

2. 1 Artificial Intelligence in Financial Fraud Detection

Financial fraud detection has evolved significantly with advances in data mining and machine learning. Traditional rule-based detection systems are increasingly considered insufficient to handle complex, adaptive fraud patterns in digital financial environments [16]. The integration of artificial intelligence (AI), particularly machine learning and predictive analytics, has enhanced fraud detection accuracy, anomaly identification, and real-time transaction monitoring [17], [18], [19]. AI-based fraud detection systems leverage large volumes of transactional data to identify abnormal patterns that may indicate fraudulent behavior [20]. Empirical studies consistently demonstrate that AI models outperform conventional statistical methods in detecting financial irregularities [18].

However, improvements in fraud detection accuracy do not necessarily translate into organizational fraud reduction outcomes. While AI systems strengthen analytical detection capabilities, their effectiveness depends not only on technological sophistication but also on organizational readiness, Data Quality, and operational integration. Despite increasing adoption within financial institutions, existing literature predominantly emphasizes algorithmic performance rather than organizational and governance mechanisms that determine whether AI systems generate operational value. This limitation highlights the need to examine AI-enabled fraud detection within a broader institutional and capability-based framework [6], [21].

Although prior studies generally report positive impacts of AI adoption on fraud detection performance, empirical evidence indicates that technological adoption does not automatically produce organizational performance improvements [22]. In this study, AI capability development refers to the organization’s ability to integrate, operationalize, and effectively utilize AI systems within fraud detection processes, reflected through AI integration, AI assimilation, and AI effectiveness. Financial institutions may develop technological readiness without achieving effective system utilization or measurable fraud mitigation outcomes. These inconsistencies suggest that the value of AI emerges through progressive organizational capability development rather than direct technological deployment [23]. Given these arguments, understanding how governance conditions influence AI integration, assimilation, and effectiveness is essential for explaining how AI-enabled detection capabilities ultimately contribute to fraud-reduction outcomes. Based on

 https://doi.org/10.58421/misro.v5i3.1693

this perspective, the following hypotheses are developed to examine the sequential relationships underlying AI capability development and fraud reduction.

2.2 Regulatory Pressure and Organizational Support

Regulatory pressure plays a critical role in shaping organizational responses to technological and risk management requirements. Institutional theory suggests that organizations adapt their structures and practices in response to coercive pressures imposed by regulatory authorities [24]. In highly regulated industries such as financial services, regulatory bodies increasingly require institutions to strengthen fraud prevention, data governance, and risk management capabilities [25]. Beyond compliance, regulatory pressure also influences internal organizational readiness. External expectations often drive management commitment, resource allocation, and strategic prioritization of technology initiatives, including the adoption of artificial intelligence (AI) [26]. Within the Technology–Organization–Environment (TOE) framework, environmental pressure serves as a key driver of organizational preparedness and technological alignment [27]. Consequently, regulatory pressure is expected to enhance organisational support by encouraging internal alignment and resource mobilization for AI implementation [28]. Drawing upon these arguments, the following hypothesis is proposed:

H_1: Regulatory pressure positively influences organizational support.

2.3 Regulatory Pressure and Data Quality

In addition to influencing organizational support, regulatory pressure also plays an important role in improving Data Quality practices. Regulatory frameworks increasingly emphasize data governance, transparency, and accountability, particularly in the context of AI-based risk management systems [29]. These requirements compel organizations to establish structured data management processes, ensuring that data used for analytical and decision-making purposes is accurate, complete, and reliable. In financial institutions, regulatory scrutiny of fraud prevention further underscores the need for high-quality transactional data [30]. Therefore, regulatory pressure may encourage organizations to strengthen data governance mechanisms and improve overall data quality. As such, the second hypothesis is stated as follows:

H_2: Regulatory pressure positively influences data quality.

2.4 Organisational Support and Data Quality

Organisational support reflects the extent to which management provides resources, infrastructure, and strategic direction for technology implementation. Prior studies emphasize that strong internal support is essential for effective data governance practices, including data accuracy, completeness, and consistency [31]. Without sufficient organisational commitment, data management practices may remain fragmented, limiting the effectiveness of advanced analytical technologies such as AI [32]. Therefore, organisational support is expected to enhance data quality by enabling coordinated data governance and ensuring the availability of reliable information. In line with this argument, the third hypothesis is proposed as follows:

H_3: Organisational support positively influences Data Quality.

2.5 Data Quality and AI Integration

Data Quality is a fundamental prerequisite for successful AI adoption. AI systems rely on accurate, complete, and structured data to generate reliable outputs. Poor Data Quality can lead to biased models, inaccurate predictions, and ineffective decision-making regardless of technological sophistication. In fraud detection contexts, high-quality data enables effective AI Integration by allowing systems to process relevant transaction patterns. Thus, data quality plays a critical role in facilitating the initial implementation of AI within organizational processes [33]. These arguments suggest that organizations with higher data quality are more likely to achieve effective AI integration. Thus, the following hypothesis is developed:

H_4: Data quality positively influences AI integration.

2.6 AI Integration and AI Assimilation

AI adoption is a multi-stage process. AI Integration refers to the initial implementation of AI systems, while AI Assimilation reflects the extent to which these systems are embedded in daily operations. Research in information systems suggests that assimilation is a stronger predictor of performance outcomes than mere adoption [29] [34]. Organizations that successfully integrate AI into their workflows are more likely to routinize its use, leading to deeper assimilation. Taken together, the following hypothesis is stated:

H_5: AI integration positively influences AI assimilation.

2.7 AI Assimilation and AI Effectiveness

According to the Information Systems Success Model, system effectiveness depends not only on technical quality but also on actual usage and integration [35][29]. AI Assimilation reflects the extent to which AI systems are actively utilized in organizational processes. When AI systems are deeply embedded in decision-making processes, they improve detection accuracy, responsiveness, and reliability. Greater AI adoption may enhance AI effectiveness by promoting routine use and deeper operational integration of AI systems into fraud detection activities. Accordingly, the sixth hypothesis is stated as follows:

H_6: AI assimilation positively influences AI effectiveness.

2.8 AI Effectiveness and Fraud Reduction

Fraud reduction represents the ultimate organizational outcome of AI-based fraud detection systems. IS success theory suggests that system effectiveness translates into measurable organizational benefits [29], [35]. When AI systems produce accurate and timely outputs, financial institutions can identify suspicious transactions more effectively, reduce fraud incidents, and minimize financial losses. As a result, higher AI Effectiveness may contribute to stronger Fraud Reduction outcomes. Based on this reasoning, the seventh hypothesis is proposed as follows:

H$_7$: AI effectiveness positively influences fraud reduction.

2.9 Proposed Model Summary

Based on the preceding arguments, this study proposes a framework in which regulatory pressure and organisational support strengthen Data Quality and facilitate AI capability development through AI Integration, AI Assimilation, and AI Effectiveness, ultimately contributing to Fraud Reduction outcomes. The study's conceptual framework is presented in Figure 1.

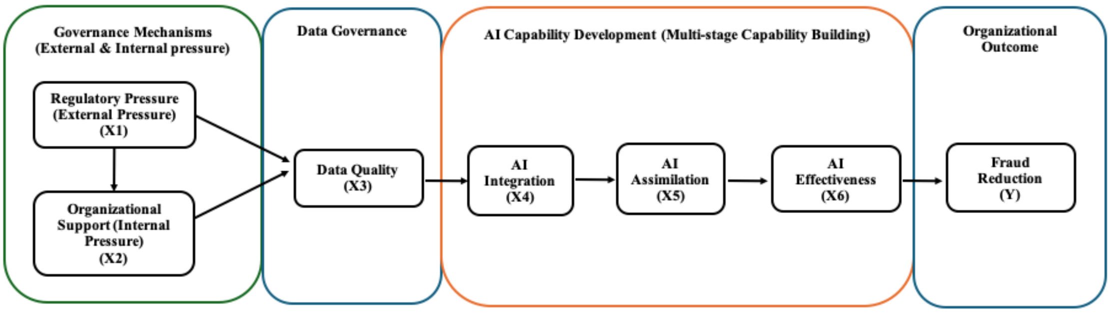

Figure 1. Theoretical Framework

3. RESEARCH METHODOLOGY

3.1 Research Design

This study employs a quantitative research design to examine the organizational capability pathway of AI-based fraud reduction within financial institutions. The research model investigates how Regulatory Pressure, Organisational Support, and Data Quality contribute to AI capability development through AI Integration, AI Assimilation, and AI Effectiveness, ultimately leading to fraud reduction outcomes. To test the proposed hypotheses, this study uses variance-based Structural Equation Modeling (PLS-SEM). PLS-SEM is appropriate for predictive and capability-oriented research models, particularly when examining complex relationships involving sequential mediation effects. In addition, PLS-SEM does not require strict multivariate normality assumptions and is suitable for exploratory and theory-extension research contexts. The data were analyzed using SmartPLS 4.1 following a two-step approach: (1) evaluation of the measurement model and (2) evaluation of the structural model [36].

3.2 Sample and Data Collection

The study was conducted in the Indonesian financial sector, including banking, fintech, insurance, and investment institutions. A total of 151 respondents participated in this study, consisting of professionals such as data scientists, auditors, risk managers, IT personnel, compliance officers, fraud analysts, customer service staff, and operational officers. Respondents were selected using purposive sampling, targeting individuals directly involved in financial operations, risk management, fraud detection, or information systems to ensure the relevance and reliability of the data.

Data were collected between 1 February and 17 February 2026 using a cross-sectional survey approach. A structured questionnaire was distributed online via Google Forms through professional networks, email invitations, and LinkedIn groups related to finance and technology. The instrument employed a five-point Likert scale, where 1 indicates strongly disagree, and 5 indicates strongly agree. [37]

Table 1. Respondent Profile

Category	**Frequency**	**Percentage**
Financial Sector		
Banking	64	42.4%
Fintech	31	20.5%
Insurance	20	19.9%
Investment	26	17.2%
Work Experience		
< 1 year	23	15.2%
1–3 years	49	32.5%
3–5 years	47	31.1%
> 5 years	32	21.2%

3.3 Data Analysis Procedures

The analysis followed a three-step approach. First, multicollinearity and common method bias were assessed using inner model collinearity statistics (VIF). Second, the measurement model was evaluated through reliability and validity assessment, including Cronbach's alpha, Composite Reliability (CR), Average Variance Extracted (AVE), and Heterotrait-Monotrait ratio (HTMT). Third, the structural model was assessed using bootstrapping procedures to examine path coefficients, coefficient of determination (R^2), effect size (f^2), and mediation effects.

4. RESULTS

4.1 Descriptive Statistics

Table 2. Descriptive Statistics

Constructs	**Mean**	**Std. Deviation**	**Min**	**Max**	**Skewness**
Regulatory Pressure	3,63	1,07	1,00	5,00	(0,47)
Organisational Support	3,60	1,04	1,00	5,00	(0,41)
Data Quality	3,64	1,05	1,00	5,00	(0,52)
AI Integration	3,60	1,06	1,00	5,00	(0,44)
AI Assimilation	3,68	1,04	1,00	5,00	(0,52)
AI Effectiveness	3,63	1,03	1,00	5,00	(0,46)
Fraud Reduction	3,62	1,07	1,00	5,00	(0,41)

Table 2 presents the descriptive statistics of the study variables. The mean values range from 3.60 to 3.68, indicating moderately positive perceptions among respondents regarding AI adoption, governance conditions, and fraud reduction practices within Indonesian financial institutions. AI Assimilation reported the highest mean value (3.68), suggesting that AI systems have been relatively embedded within organizational operations. Standard deviation values ranging from 1.03 to 1.07 indicate moderate variability across responses. Furthermore, skewness values ranged from -0.41 to -0.52, indicating slight negative skewness and suggesting that respondents generally provided favorable assessments of the measured constructs.

4.2 Model Evaluation

4.2.1 Multicollinearity and Common Method Bias Assessment

Multicollinearity and common method bias were assessed using inner model collinearity statistics (VIF). As presented in Table 3, all VIF values ranged from 1.000 to 1.206, which are below the recommended threshold of 3.3. These results indicate that multicollinearity is not a concern in the structural model and that common-method bias is unlikely to affect the study's findings.

Table 3. Inner Model Collinearity Statistics (VIF)

Structural Path	VIF
AI Assimilation → AI Effectiveness	1.000
AI Effectiveness → Fraud Reduction	1.000
AI Integration → AI Assimilation	1.000
Data Quality → AI Integration	1.000
Organisational Support → Data Quality	1.206
Regulatory Pressure → Data Quality	1.206
Regulatory pressure → Organisational Support	1.000

4.2.2 Measurement Model Assessment

The measurement model was assessed to evaluate the reliability and validity of the constructs. Internal consistency reliability was examined using Cronbach’s alpha and Composite Reliability (CR) [37].

As presented in Table 4, all constructs exceeded the recommended threshold of 0.70 across both reliability measures. Cronbach’s alpha values ranged from 0.704 to 0.909, while Composite Reliability values ranged from 0.836 to 0.936, indicating satisfactory construct reliability. Additional reliability assessment using rho_A also demonstrated acceptable reliability across all constructs. Convergent validity was evaluated using outer loadings and Average Variance Extracted (AVE). Most indicator loadings exceeded the recommended threshold of 0.70, while one indicator under AI Effectiveness (AI-Eff9 = 0.546) was retained because the construct continued to demonstrate satisfactory reliability and convergent validity. Furthermore, all AVE values exceeded the recommended threshold of 0.50, ranging from 0.516 to 0.805, confirming adequate convergent validity.

Table 4. Measurement Model Assessment

Construct	Item	Outer Loading	Cronbach’s Alpha	Composite Reliability	AVE
Regulatory Pressure	RP1	0.879	0.900	0.930	0.770
	RP2	0.897			
	RP3	0.858			
	RP4	0.874			
Organisational Support	OrgS1	0.871	0.704	0.836	0.631
	OrgS2	0.789			

Construct	Item	Outer Loading	Cronbach's Alpha	Composite Reliability	AVE
	OrgS3	0.714			
Data Quality	DQ1	0.882	0.909	0.936	0.785
	DQ2	0.905			
	DQ3	0.855			
	DQ4	0.900			
AI Integration	AI-Intg1	0.872	0.903	0.932	0.774
	AI-Intg2	0.882			
	AI-Intg3	0.864			
	AI-Intg4	0.900			
AI Assimilation	AI-A1	0.874	0.894	0.926	0.758
	AI-A2	0.874			
	AI-A3	0.863			
	AI-A4	0.872			
AI Effectiveness	AI-Eff1	0.718	0.884	0.905	0.516
	AI-Eff2	0.746			
	AI-Eff3	0.724			
	AI-Eff4	0.708			
	AI-Eff5	0.768			
	AI-Eff6	0.751			
	AI-Eff7	0.723			
	AI-Eff8	0.753			
	AI-Eff9	0.546			
Fraud Reduction	FR1	0.900	0.879	0.925	0.805
	FR2	0.897			
	FR3	0.894			

4.2.3 Discriminant Validity Assessment

Discriminant validity was assessed using the Heterotrait-Monotrait ratio (HTMT) as presented in Table 5.

Table 5. Discriminant Validity Assessment

Constructs	RP	OS	DQ	AI Intg	AI Assm	AI Effect	FR
Regulatory Pressure (RP)	—						
Organisational Support (OS)	0.515	—					
Data Quality (DQ)	0.435	0.616	—				
AI Integration (AI Intg)	0.456	0.561	0.485	—			
AI Assimilation (AI Assm)	0.481	0.512	0.458	0.510	—		
AI Effectiveness (AI Effct)	0.606	0.903	0.581	0.547	0.549	—	
Fraud Reduction (FR)	0.388	0.605	0.541	0.437	0.450	0.612	—

The HTMT values were generally below the recommended threshold of 0.90, indicating acceptable discriminant validity among the constructs. Although the HTMT value between Organisational Support and AI Effectiveness slightly exceeded the threshold (0.903), the confidence interval did not include 1.00, suggesting that discriminant validity remained acceptable.

 https://doi.org/10.58421/misro.v5i3.1693

4.2.4 Structural Model Assessment

The structural model was assessed using bootstrapping procedures with 5.000 subsamples to evaluate the significance of the hypothesized relationships. As presented in Table 6, all proposed direct relationships were statistically significant at the 5% significance level.

Table 6. Structural Path Coefficients

Hypothesis	Structural Path	Path Coefficient (β)	T-statistics	P-values
H1	Regulatory pressure → Organisational Support	0.414	4.406	0.000
H2	Regulatory Pressure → Data Quality	0.232	3.087	0.002
H3	Organisational Support → Data Quality	0.400	5.676	0.000
H4	Data Quality → AI Integration	0.442	5.221	0.000
H5	AI Integration → AI Assimilation	0.463	5.428	0.000
H6	AI Assimilation → AI Effectiveness	0.514	6.168	0.000
H7	AI Effectiveness → Fraud Reduction	0.597	12.288	0.000

Regulatory pressure demonstrated a significant positive effect on Organisational Support. ($\beta = 0.414$, $p < 0.001$) and Data Quality ($\beta = 0.232$, $p = 0.002$). Organisational Support also positively influenced Data Quality ($\beta = 0.400$, $p < 0.001$). Furthermore, Data Quality significantly enhanced AI Integration ($\beta = 0.442$, $p < 0.001$), which subsequently strengthened AI Assimilation ($\beta = 0.463$, $p < 0.001$). AI Assimilation was found to positively affect AI Effectiveness ($\beta = 0.514$, $p < 0.001$), while AI Effectiveness demonstrated the strongest direct effect on Fraud Reduction ($\beta = 0.597$, $p < 0.001$). These findings indicate that fraud reduction is achieved through a sequential capability development process in which governance and organizational conditions enhance Data Quality and AI implementation capabilities, ultimately leading to effective fraud reduction outcomes.

4.2.5 Coefficient of Determination (R^2)

The coefficient of determination (R^2) and adjusted R^2 values were used to evaluate the explanatory power of the structural model.

Table 7. Coefficient of Determination (R^2)

Endogenous Construct	R^2	Adjusted R^2
Organisational Support	0.171	0.165
Data Quality	0.291	0.281
AI Integration	0.195	0.190
AI Assimilation	0.214	0.209
AI Effectiveness	0.264	0.259
Fraud Reduction	0.357	0.352

As presented in Table 7, the model explains 35.7% of the variance in Fraud Reduction (Adjusted R^2 = 0.352), indicating moderate explanatory power. The model also explains 29.1% of the variance in Data Quality, 26.4% in AI Effectiveness, 21.4% in AI Assimilation, and 19.5% in AI Integration. Regulatory pressure accounts for an additional 17.1% of the variance in Organisational Support. The findings show that the proposed framework captures the sequential relationships associated with AI capability development and fraud reduction.

4.2.6 The Effect Size (f^2)

The effect size (f^2) analysis indicates that AI Effectiveness exerts the strongest substantive influence on Fraud Reduction (f^2 = 0.554), followed by the effect of AI Assimilation on AI Effectiveness (f^2 = 0.359). Medium effect sizes were observed for AI Integration → AI Assimilation (f^2 = 0.272), Data Quality → AI Integration (f^2 = 0.243), Organisational Support → Data Quality (f^2 = 0.187), and Regulatory Pressure → Organisational Support (f^2 = 0.206). In contrast, the effect of Regulatory Pressure on Data Quality was relatively small (f^2 = 0.063). These findings further support the sequential capability-building mechanism proposed in this study.

Table 8. The Effect Size (f^2)

Structural Path	f^2	Effect Size
AI Assimilation → AI Effectiveness	0.359	Large
AI Effectiveness → Fraud Reduction	0.554	Large
AI Integration → AI Assimilation	0.272	Medium
Data Quality → AI Integration	0.243	Medium
Organisational Support → Data Quality	0.187	Medium
Regulatory Pressure → Data Quality	0.063	Small
Regulatory pressure → Organisational Support	0.206	Medium

4.2.7 Indirect Effect

Indirect effect analysis was conducted to assess the sequential mediation relationships within the proposed model. The results reveal several statistically significant indirect effects, indicating that governance and organizational conditions affect fraud reduction by advancing the development of AI capabilities.

Table 9. Indirect Effect

Indirect Relationship	Indirect Effect	T-statistics	P-values
AI Assimilation → Fraud Reduction	0.307	4.729	0.000
AI Integration → AI Effectiveness	0.238	3.297	0.001
AI Integration → Fraud Reduction	0.142	2.767	0.006
Data Quality → AI Assimilation	0.205	3.061	0.002
Data Quality → AI Effectiveness	0.105	2.205	0.028
Organisational Support → AI Integration	0.177	3.242	0.001
Regulatory Pressure → AI Integration	0.176	2.692	0.007

AI Integration indirectly enhanced AI Effectiveness (β = 0.238, p = 0.001) and Fraud Reduction (β = 0.142, p = 0.006) through AI Assimilation and AI Effectiveness. Similarly, Data Quality indirectly influenced AI Assimilation (β = 0.205, p = 0.002) and AI Effectiveness (β = 0.105, p = 0.028). Organisational Support and Regulatory Pressure

 https://doi.org/10.58421/misro.v5i3.1693

also demonstrated significant indirect effects on AI Integration, indicating that governance-related conditions contribute to the downstream formation of AI capability. However, the indirect effects of Organisational Support and Regulatory Pressure on Fraud Reduction were not statistically significant. These findings suggest that governance mechanisms alone are insufficient to directly reduce fraud unless they are translated into effective AI implementation, assimilation, and operational effectiveness. Overall, the results support the argument that fraud reduction emerges through a sequential organizational capability development process rather than through direct technological adoption alone.

5. DISCUSSIONS

5.1 Regulatory Pressure and Organisational Support in AI Capability Development

The findings indicate that regulatory pressure and organisational support play important roles in supporting AI capability development within financial institutions. Regulatory pressure was found to significantly influence organisational support and data quality, indicating that external regulations and supervisory expectations encourage organisations to strengthen internal commitment to AI implementation and to improve data management practices. In addition, organisational support positively affected data quality, suggesting that managerial commitment, resource allocation, and organisational readiness are important in establishing reliable data environments for AI systems.

Since AI-based fraud detection relies heavily on data accuracy and consistency, organizations with stronger internal support are more likely to develop the conditions necessary for effective AI implementation. These findings suggest that regulatory and organizational factors do not directly reduce fraud. Instead, they help organizations build the internal conditions required for effective AI utilization and capability development.

5.2 From AI Integration to AI Effectiveness

The results demonstrate that AI capability development occurs through a sequential process rather than through immediate technological adoption. Data quality significantly improved AI integration, while AI integration positively influenced AI assimilation and AI effectiveness. These findings indicate that organizations must first establish reliable data environments before AI systems can be effectively integrated into operational processes.

The findings further suggest that technical implementation alone is insufficient to generate organizational value. After AI systems are integrated, organizations must also operationally assimilate them into routine activities and decision-making processes to achieve effective fraud detection performance. In other words, AI systems become valuable only when they are consistently used and embedded in organizational operations.
This sequential relationship supports the argument that fraud-reduction outcomes emerge progressively through organizational capability development rather than solely from AI adoption.

5.3 AI Effectiveness and Fraud Reduction

The results further demonstrate that AI effectiveness exerts the strongest direct influence on fraud reduction. This finding indicates that fraud reduction is primarily determined not by the mere presence of AI systems but by the operational effectiveness of those systems in detecting anomalies, improving responsiveness, and supporting fraud-related decision-making processes. This result extends prior AI adoption literature, which often assumes that technological adoption automatically improves organizational performance outcomes. The present study shows that technological implementation alone does not guarantee reductions in fraud. Instead, organizations must achieve effective AI utilization and operational performance before measurable reductions in fraud can occur. The large effect size observed between AI effectiveness and fraud reduction further underscores the central role of operational AI performance in fraud management. Financial institutions that successfully operationalize AI systems are more likely to strengthen real-time monitoring, anomaly detection accuracy, and fraud mitigation responsiveness.

5.4 Indirect Effects and Mediation Mechanisms

The indirect effect analysis provides additional insight into how regulatory and organizational conditions contribute to fraud reduction outcomes. Although regulatory pressure and organisational support significantly influenced upstream organisational capabilities, their indirect effects on fraud reduction were not statistically significant. These findings suggest that governance-related conditions alone are insufficient to reduce fraud incidents directly. Instead, regulatory pressure and organisational support contribute to fraud reduction only when translated into stronger organisational capabilities, including improved data quality, AI integration, AI assimilation, and AI effectiveness. This finding supports the argument that organizational value from AI emerges through cumulative capability development processes rather than through direct technological adoption alone. Hence, the findings support a capability development perspective in which regulatory pressure, organizational support, data readiness, and AI operationalization collectively shape the effectiveness of AI-enabled fraud reduction initiatives within financial institutions.

6. THEORETICAL IMPLICATIONS

These findings contribute to the literature in several ways. First, this study extends institutional theory by showing that regulatory pressure does not directly improve fraud-reduction outcomes but instead strengthens organizational readiness and Data Quality that support AI capability development. Second, this study advances the TOE framework by demonstrating that AI capability development occurs sequentially through AI integration, AI assimilation, and AI effectiveness rather than through single-stage technological adoption. Third, this study extends the Information Systems Success Model [29] by confirming that AI effectiveness serves as the immediate driver of fraud-reduction outcomes, while regulatory and organizational conditions contribute indirectly through mechanisms of capability development. Thus, the findings suggest that organizational value from AI emerges through progressive development of operational capabilities rather than technological adoption alone.

7. PRACTICAL IMPLICATIONS

The findings provide several practical implications for financial institutions. First, regulatory compliance alone is insufficient to reduce fraud unless AI systems are effectively integrated and operationally utilized. Second, data quality management is a foundational capability that supports effective AI implementation. Third, organizations should prioritize AI assimilation through workflow integration, employee training, and operational adaptation rather than focusing solely on technological adoption. It concludes that fraud reduction depends not only on adopting AI systems, but on effectively embedding them within organizational processes

8. CONCLUSION

This study examined how regulatory and organizational conditions influence fraud reduction through the development of artificial intelligence (AI) capabilities within financial institutions. The findings demonstrate that fraud reduction is not achieved solely through regulatory pressure or AI adoption. Instead, fraud reduction emerges through a sequential capability development process involving data quality, AI integration, AI assimilation, and AI effectiveness. These findings answer the research objective by confirming that organizational capability development is the critical mechanism through which regulatory and organizational conditions translate into measurable reductions in fraud.

The study contributes to the existing literature by validating a capability-based AI development pathway that extends Institutional Theory, the Technology–Organization–Environment (TOE) framework, and the Information Systems Success Model. Rather than viewing AI adoption as the primary determinant of organizational performance, the findings demonstrate that value creation depends on the organization's ability to develop, assimilate, and progressively operationalize AI capabilities. This provides a more comprehensive explanation of how technological innovation generates organizational benefits in fraud management.

From a practical perspective, the findings provide important implications for financial institutions, regulators, and policymakers. Organizations should focus not only on investing in AI technologies but also on strengthening organizational support, improving data quality, enhancing AI integration, and facilitating continuous AI assimilation to maximize fraud reduction performance. Likewise, regulators should encourage policies that promote organizational capability development rather than merely emphasizing regulatory compliance or technology adoption.

This study is subject to several limitations. The proposed relationships were examined within the context of financial institutions, which may limit the generalizability of the findings to other industries. In addition, the study primarily focused on organizational and technological capability factors without incorporating external environmental dynamics or individual behavioral factors that may also influence AI implementation success.

Future research is encouraged to validate the proposed model across different industrial sectors and national contexts to enhance its generalizability. Further studies may also incorporate additional variables, such as organizational culture, digital leadership, AI governance, cybersecurity capability, or employee digital competence, as potential mediators or moderators. Longitudinal and mixed-method research designs are also recommended to provide deeper insights into the long-term evolution of AI capability development and its impact on sustainable fraud prevention.

9. LIMITATIONS & FUTURE RESEARCH

Despite providing important insights, this study has several limitations. First, the cross-sectional nature of the study limits the examination of how AI capabilities evolve and mature over time. Future studies may adopt longitudinal designs to examine the long-term relationship between AI capability development and fraud-reduction outcomes. Second, this study relies on perceptual survey data obtained from organizational professionals, which may introduce subjective assessment bias despite statistical controls for common method bias. Future research may incorporate objective fraud indicators or archival organizational data to strengthen causal inference. Third, the empirical focus on Indonesian financial institutions may limit the generalizability of the findings across different institutional contexts. Future studies may conduct comparative analyses across countries or regulatory environments to provide deeper insights into the interactions between governance and AI capabilities. Future research may also expand the model by incorporating additional organizational factors, such as ethical AI governance, leadership support, and organizational culture, to explain variations in AI effectiveness and fraud-reduction outcomes.

REFERENCES

[1] F. Xu, Y. Kasperskaya, and M. Sagarra, “The impact of FinTech on bank performance: A systematic literature review,” *Digital Business*, vol. 5, no. 2, p. 100131, Dec. 2025, doi: 10.1016/j.digbus.2025.100131.

[2] M. Barroso and J. Laborda, “Digital transformation and the emergence of the Fintech sector: Systematic literature review,” *Digital Business*, vol. 2, no. 2, p. 100028, 2022, doi: 10.1016/j.digbus.2022.100028.

[3] M. Xu, J. M. David, and S. H. Kim, “The Fourth Industrial Revolution: Opportunities and Challenges,” *International Journal of Financial Research*, vol. 9, no. 2, p. 90, Feb. 2018, doi: 10.5430/ijfr.v9n2p90.

[4] . Mani, A. S., D. V., and D. R., “Financial Fraud Detection in Transactions Using AI,” in *Proceedings of the 1st International Conference on Research and Development in Information, Communication, and Computing Technologies*, SCITEPRESS - Science and Technology Publications, 2025, pp. 515–521. doi: 10.5220/0013868500004919.

[5] C. Aldemir and T. Uçma Uysal, “Artificial Intelligence for Financial Accountability and Governance in the Public Sector: Strategic Opportunities and Challenges,” *Adm. Sci.*, vol. 15, no. 2, p. 58, Feb. 2025, doi: 10.3390/admsci15020058.

[6] P. Mikalef and M. Gupta, “Artificial intelligence capability: Conceptualization, measurement calibration, and empirical study on its impact on organizational creativity and firm performance,” *Information & Management*, vol. 58, no. 3, p. 103434, Apr. 2021, doi: 10.1016/j.im.2021.103434.

[7] A. Rai, S. S. Lang, and R. B. Welker, “Assessing the Validity of IS Success Models: An Empirical Test and Theoretical Analysis,” *Information Systems Research*, vol. 13, no. 1, pp. 50–69, Mar. 2002, doi: 10.1287/isre.13.1.50.96.

[8] K. Zhu, K. L. Kraemer, and S. Xu, “The Process of Innovation Assimilation by Firms in Different Countries: A Technology Diffusion Perspective on E-Business,” *Manage. Sci.*, vol. 52, no. 10, pp. 1557–1576, Oct. 2006, doi: 10.1287/mnsc.1050.0487.

[9] S. Maycotte, A. Alvarez-Risco, E. Garcia-Valenzuela, and M. Kuljis, “Digital capabilities in emerging market firms: Construct development, scale validation, and implications for SMEs,”

Journal of Open Innovation: Technology, Market, and Complexity, vol. 11, no. 2, p. 100513, Jun. 2025, doi: 10.1016/j.joitmc.2025.100513.

[10] U. S. D. of C. The International Trade Administration, "Indonesia Digital Economy," Nov. 2025.

[11] K. Naseer and H. N. Ahmed, "Effectiveness and Reliability of Artificial Intelligence in Fraud Detection: A Mixed-Method Study on Financial Audit," *Journal of Management and Informatics*, vol. 4, no. 1, pp. 706–722, Apr. 2025, doi: 10.51903/jmi.v4i1.168.

[12] A. Batool, D. Zowghi, and M. Bano, "AI governance: a systematic literature review," *AI and Ethics*, vol. 5, no. 3, pp. 3265–3279, Jun. 2025, doi: 10.1007/s43681-024-00653-w.

[13] C. Cancela-Outeda, "The EU's AI act: A framework for collaborative governance," *Internet of Things*, vol. 27, p. 101291, Oct. 2024, doi: 10.1016/j.iot.2024.101291.

[14] Association of Southeast Asian Nations (ASEAN), "ASEAN Guide on AI Governance and Ethics," 2024.

[15] Nydia REMOLINA LEON, "AI governance and algorithmic auditing in financial institutions: Lessons from Singapore ," *Yong Pung How School of Law*, 2025.

[16] E. W. T. Ngai, Y. Hu, Y. H. Wong, Y. Chen, and X. Sun, "The application of data mining techniques in financial fraud detection: A classification framework and an academic review of literature," *Decis. Support Syst.*, vol. 50, no. 3, pp. 559–569, Feb. 2011, doi: 10.1016/j.dss.2010.08.006.

[17] A. Abdallah, M. A. Maarof, and A. Zainal, "Fraud detection system: A survey," *Journal of Network and Computer Applications*, vol. 68, pp. 90–113, Jun. 2016, doi: 10.1016/j.jnca.2016.04.007.

[18] Yufeng Kou, Chang-Tien Lu, S. Sirwongwattana, and Yo-Ping Huang, "Survey of fraud detection techniques," in *IEEE International Conference on Networking, Sensing and Control, 2004*, IEEE, pp. 749–754. doi: 10.1109/ICNSC.2004.1297040.

[19] W. Hilal, S. A. Gadsden, and J. Yawney, "Financial Fraud: A Review of Anomaly Detection Techniques and Recent Advances," *Expert Syst. Appl.*, vol. 193, p. 116429, May 2022, doi: 10.1016/j.eswa.2021.116429.

[20] N. Jahan Sarna *et al.*, "AI Driven Fraud Detection Models in Financial Networks: A Comprehensive Systematic Review," *IEEE Access*, vol. 13, pp. 141204–141233, 2025, doi: 10.1109/ACCESS.2025.3596060.

[21] R. C. Ångström, M. Björn, L. Dahlander, M. Mähring, and M. W. Wallin, "Getting AI Implementation Right: I <scp>nsights from a</scp> G <scp>lobal</scp> S <scp>urvey</scp>," *Calif. Manage. Rev.*, vol. 66, no. 1, pp. 5–22, Nov. 2023, doi: 10.1177/00081256231190430.

[22] N.-A. Perifanis and F. Kitsios, "Investigating the Influence of Artificial Intelligence on Business Value in the Digital Era of Strategy: A Literature Review," *Information*, vol. 14, no. 2, p. 85, Feb. 2023, doi: 10.3390/info14020085.

[23] A. mayow Abdi, X. Deng, and A. J. Mohamud, "AI-Driven Organizational Adaptation in Non-Renewable Energy Sector A Systematic Review and Theoretical Framework Development," 2026, doi: 10.2139/ssrn.6459839.

[24] P. J. DiMaggio and W. W. Powell, "The Iron Cage Revisited: Institutional Isomorphism and Collective Rationality in Organizational Fields," *Am. Sociol. Rev.*, vol. 48, no. 2, p. 147, Apr. 1983, doi: 10.2307/2095101.

[25] N. Bagherifam, S. Naghdi, V. Ahmadian, A. Fazlzadeh, and M. Baghalzadeh Shishehgarkhaneh, "Digital Regulatory Governance: The Role of RegTech and SupTech in Transforming Financial Oversight and Administrative Capacity," *International Journal of Financial Studies*, vol. 13, no. 4, p. 217, Nov. 2025, doi: 10.3390/ijfs13040217.

[26] S. Anomah, "Assessing the institutional readiness and capacity for AI adoption in public audit institutions in developing countries: evidence from Ghana," *Telematics and Informatics Reports*, vol. 20, p. 100260, Dec. 2025, doi: 10.1016/j.teler.2025.100260.

[27] T. H. Nguyen, X. C. Le, and T. H. L. Vu, "An Extended Technology-Organization-Environment (TOE) Framework for Online Retailing Utilization in Digital Transformation: Empirical Evidence from Vietnam," *Journal of Open Innovation: Technology, Market, and Complexity*, vol. 8, no. 4, p. 200, Dec. 2022, doi: 10.3390/joitmc8040200.

[28] Y. Zhan, Y. Xiong, R. Han, H. K. S. Lam, and C. Blome, "The impact of artificial intelligence adoption for business-to-business marketing on shareholder reaction: A social actor perspective," *Int. J. Inf. Manage.*, vol. 76, p. 102768, Jun. 2024, doi: 10.1016/j.ijinfomgt.2024.102768.

[29] "The DeLone and McLean Model of Information Systems Success: A Ten-Year Update," *Journal of Management Information Systems*, vol. 19, no. 4, pp. 9–30, Apr. 2003, doi: 10.1080/07421222.2003.11045748.

[30] The European Union, "REGULATION (EU) 2024/1689 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL," 2024.

[31] R. Drazin, “The processes of technological innovation,” *J. Technol. Transf.*, vol. 16, no. 1, pp. 45–46, Mar. 1991, doi: 10.1007/BF02371446.

[32] K. Jamil, W. Zhang, A. Anwar, and S. Mustafa, “Exploring the Influence of AI Adoption and Technological Readiness on Sustainable Performance in Pakistani Export Sector Manufacturing Small and Medium-Sized Enterprises,” *Sustainability*, vol. 17, no. 8, p. 3599, Apr. 2025, doi: 10.3390/su17083599.

[33] M. Guillen-Aguinaga, E. Aguinaga-Ontoso, L. Guillen-Aguinaga, F. Guillen-Grima, and I. Aguinaga-Ontoso, “Data Quality in the Age of AI: A Review of Governance, Ethics, and the FAIR Principles,” *Data (Basel).*, vol. 10, no. 12, p. 201, Dec. 2025, doi: 10.3390/data10120201.

[34] L. Rodríguez Valencia *et al.*, “A Systematic Review of Artificial Intelligence Applied to Compliance: Fraud Detection in Cryptocurrency Transactions,” *Journal of Risk and Financial Management*, vol. 18, no. 11, p. 612, Oct. 2025, doi: 10.3390/jrfm18110612.

[35] Mahmoud Khaled Al-Kofah, Haslinda Hassan, and Rosli Mohamad, “Information Systems Success Model: A Review of Literature,” *International Journal of Innovation, Creativity and Change*, vol. 12, no. 8, 2020.

[36] J. F. Hair *et al.*, *Partial Least Squares Structural Equation Modeling (PLS-SEM) Using R*. Springer International Publishing, 2022. doi: 10.1007/978-3-030-80519-7.

[37] J. F. . Hair, G. T. M. . Hult, C. M. . Ringle, and Marko. Sarstedt, *A primer on partial least squares structural equation modeling (PLS-SEM).* SAGE Publications, Inc., 2022.