International Journal of Independent Research Studies
Vol. 14, No. 2, 29-35, 2025
ISSN(E) 2226-4817
DOI: 10.55220/2304-6953.v14i2.760

The Impact of Digital Transformation on Financial Security Perceptions and Fraud Resilience in SMEs: A Structural Equation Modeling Approach

Krishna Ashutoshbhai Vyas[1] ✉
Tulsi Raval[2]

[1] *School of Management, R K University, Rajkot, Gujarat, India.*
[2] *Department of Commerce, Smt. KSN Kansagara Mahila College, Rajkot, Gujarat, India.*
(✉ Corresponding Author)

Abstract

This study investigates the influence of digital transformation (DT) on financial security perceptions (FSP) and fraud resilience (FR) among small and medium-sized enterprises (SMEs) in India. Drawing on a sample of 206 SME decision-makers, a structural equation modeling (SEM) approach was used to assess the proposed relationships. The findings confirm that DT positively impacts both FSP and FR, with financial security acting as a partial mediator in enhancing fraud resilience. The model demonstrates strong explanatory relevance and good overall fit. These results underscore the critical role of strategic digital adoption in reinforcing SMEs' financial systems and preparedness against fraud. The study offers practical implications for SME leaders, policymakers, and technology providers aiming to build secure and resilient digital enterprises in emerging markets.

Keywords: Cybersecurity, Digital transformation, Emerging economies, Financial security, Fraud resilience, SEM, SMEs.

1. Introduction

The digital revolution has significantly transformed the operational and strategic dynamics of small and medium-sized enterprises (SMEs). With the increasing adoption of technologies such as cloud computing, artificial intelligence (AI), and digital payment platforms, SMEs are navigating both unprecedented opportunities and complex risks. While digital transformation (DT) enhances business agility, scalability, and customer engagement, it also exposes enterprises to cyber threats, data breaches, and fraud risks. Particularly in the context of financial transactions and digital infrastructures, the resilience of SMEs is tested by their ability to perceive, prepare for, and respond to financial and security threats.

In emerging economies like India, where SMEs contribute substantially to employment and GDP, understanding how digital adoption influences financial security and fraud resilience is critical. Yet, despite widespread digital adoption among SMEs, many lack structured governance and awareness systems to manage digital risks effectively. This study investigates the relationships among digital transformation, financial security perception (FSP), and fraud resilience (FR), focusing on the mediating role of FSP in the DT-FR pathway.

2. Theoretical Background and Literature Review

2.1. Theoretical Foundation

This study draws from two key theoretical lenses:

- Technology-Organization-Environment (TOE) Framework: Developed by Tornatzky and Fleischer (1990), this model suggests that technology adoption is influenced by technological, organizational, and environmental contexts. In the case of SMEs, this includes the availability of digital tools, internal readiness, leadership commitment, and external regulatory or market pressures.
- Resource-Based View (RBV): As per Barney (1991), firms achieve competitive advantage through internal resources that are valuable, rare, and difficult to replicate. Here, digital infrastructure, risk management capability, and skilled personnel are viewed as strategic resources that enhance security and resilience.

2.2. Literature Review and Synthesis

The following themes emerge from a synthesis of recent scholarly contributions:

2.2.1. Artificial Intelligence as a Fraud Deterrent

The deployment of artificial intelligence (AI) has emerged as a pivotal tool in preventing and detecting financial fraud.
Adekanmbi and Oluwadare (2025) illustrate how AI-driven monitoring systems have enhanced fraud control in Nigerian banks, setting a precedent for similar applications in SMEs. Matarazzo and Celentano (2025), through a comprehensive review, emphasize that AI technologies reduce reliance on manual oversight and improve anomaly

detection accuracy. Busari (2025) extends this insight by empirically showing that predictive analytics in U.S. small businesses have contributed to more effective fraud risk management and real-time response capabilities.
Synthesis Insight: AI not only increases fraud detection accuracy but also enables SMEs to respond more proactively to potential threats.

2.2.2. Digital Security Architecture and Risk Control

The structure of a firm's digital ecosystem plays a critical role in its ability to manage cyber risks. Kumar (2025) introduces the concept of Zero Trust Architecture, which assumes no implicit trust within any part of the network and emphasizes continuous authentication and access restrictions. Andrewson and colleagues (2025) focus on cloud-based cybersecurity strategies tailored to SME constraints, highlighting the importance of system configuration and secure vendor relationships. Petrova and Nuur (2025) point out that partnerships, training, and external support significantly enhance SMEs' resilience when internal IT resources are limited.
Synthesis Insight: An effective cybersecurity strategy requires not just tools but a resilient digital infrastructure backed by governance and expertise.

2.2.3. Governance, Leadership, and Security Orientation

Organizational leadership and decision-making are strongly linked to the outcomes of digital transformation efforts. Murugesan and Seema (2025) argue that proactive leadership fosters not only innovation but also sound financial oversight and risk planning. In contrast, Hasanova and Najafova (2025) warn that poor governance—especially in fast-tracked digitization efforts—can expose SMEs to third-party risks and systemic vulnerabilities from unregulated automation.

Synthesis Insight: Effective leadership is central to aligning digital investments with secure and sustainable business practices.

2.2.4. Misalignment Between Security Awareness and Reality

While many SMEs perceive themselves as secure, their practices often reveal substantial gaps. Tabassum (2025) finds a disconnect between SMEs' confidence in their cybersecurity and the actual presence of preventive measures, such as training or routine audits. Matarazzo and Celentano (2025) similarly caution against overreliance on technology without adequate internal risk assessments or contingency planning.

Synthesis Insight: Building fraud resilience also requires raising awareness and closing the gap between perceived and real security readiness.

2.2.5. Business Intelligence as a Monitoring Enabler

Advanced analytics and business intelligence (BI) tools are providing SMEs with real-time visibility into operational risks.
Vihaan and Adrian (2025) demonstrate how AI-integrated BI platforms support continuous monitoring, helping SMEs identify financial irregularities, suspicious transactions, and vendor risks with greater speed and accuracy.

Synthesis Insight: BI systems enable SMEs to transition from reactive to proactive security models through timely data insights.

Table 1. Synthesized Themes and Evidence.

Theme	Key Authors	Key Contributions
AI in Fraud Detection	Adekanmbi & Oluwadare; Busari	Automation improves fraud prediction and detection accuracy
Cybersecurity Architecture	Kumar; Petrova & Nuur	Emphasis on zero-trust models, cloud security, and vendor integrity
Strategic Governance	Murugesan & Seema; Hasanova & Najafova	Leadership's role in ensuring secure digital transformation
Perception vs. Reality Gap	Tabassum; Matarazzo & Celentano	SMEs overestimate security readiness without proper controls
Business Intelligence Tools	Vihaan & Adrian	BI enables real-time fraud detection and actionable monitoring strategies

2.3. Research Gap

Despite increasing adoption of digital tools, few empirical studies explore how DT affects financial security perception and fraud resilience among SMEs in emerging economies. Existing research often examines these variables in isolation. There is limited work integrating all three constructs into a single, testable framework using advanced techniques like PLS-SEM. Furthermore, the literature lacks insights from India's diverse SME ecosystem.

2.4. Research Contribution

This study addresses these gaps by:

- Developing and testing an integrated model linking DT, FSP, and FR;
- Using empirical data from Indian SMEs;
- Providing actionable insights for improving digital governance and risk preparedness.

3. Research Methodology

3.1. Research Design

This study adopts a quantitative, cross-sectional, and explanatory research design to investigate the relationship between digital transformation, financial security perceptions, and fraud resilience among Indian SMEs. The structural relationships among the constructs were analyzed using Partial Least Squares Structural

Equation Modeling (PLS-SEM), a robust technique suited for exploratory studies and complex models involving latent variables.

The research aimed to uncover causal pathways by testing the following hypotheses:

- H1: Digital transformation has a positive influence on financial security perception.
- H2: Digital transformation directly enhances fraud resilience.
- H3: Financial security perception positively affects fraud resilience.

3.2. Population and Sampling

The target population comprised owners, founders, or key decision-makers of small and medium-sized enterprises (SMEs) operating in diverse sectors across India.

- Sampling Method: A non-probability purposive sampling technique was employed to ensure that respondents had sufficient knowledge and authority to comment on digital transformation and risk-related initiatives in their businesses.
- Sample Size: A total of 206 valid responses were collected and analysed. The sample size exceeds the minimum required based on Hair et al. (2022) guidelines for PLS-SEM, ensuring model stability and statistical power.

3.3. Data Collection Procedure

Data was collected using a structured questionnaire administered online, distributed through email, LinkedIn, and professional SME forums over a 6-week period in early 2025. The questionnaire was accompanied by a cover letter explaining the purpose of the research, ensuring informed consent, anonymity, and voluntary participation.

Inclusion Criteria:

- Enterprises must qualify as SMEs per the Indian Ministry of MSME guidelines.
- Respondents must be business owners or hold managerial responsibilities related to finance, technology, or risk.
- Firms must have been operational for a minimum of 2 years.

3.4. Instrumentation and Measures

The questionnaire was developed based on validated scales adapted from prior research. All items were measured using a 5-point Likert scale (1 = Strongly Disagree to 5 = Strongly Agree). Three key constructs were measured:

- Digital Transformation (DT): Adapted from Vial (2019) and Verhoef et al. (2021), covering areas such as cloud adoption, AI integration, digital workflows, and customer-facing technology.
- Financial Security Perception (FSP): Derived from studies by Pavlou (2011) and recent works on SME financial risk, focusing on the perceived ability to manage financial threats and ensure transaction safety.
- Fraud Resilience (FR): Based on frameworks from Moorthy et al. (2020) and ISO 37001 standards, emphasizing proactive fraud detection, risk governance, and system monitoring.

Each construct was measured with 4–6 reflective indicators, tested for validity and reliability through PLS-SEM.

3.5. Data Analysis Techniques

The data analysis followed a two-stage approach using SmartPLS 4:

1. Measurement Model Assessment:

- Internal consistency via Cronbach's Alpha and Composite Reliability
- Convergent Validity using Average Variance Extracted (AVE)
- Discriminant Validity via HTMT ratio

2. Structural Model Evaluation:

- Path coefficients and hypothesis testing using bootstrapping (n = 5000)
- Collinearity check using Variance Inflation Factor (VIF)
- Coefficient of Determination (R^2)
- Effect size (f^2)
- Predictive relevance (Q^2)
- Model fit assessment using Goodness-of-Fit Index (GoF)

These techniques provided both reliability and explanatory power to assess the conceptual framework.

3.6. Ethical Considerations

Ethical standards were strictly adhered to throughout the study. Participation was voluntary, and informed consent was obtained digitally before commencing the survey. The collected data was anonymized and used exclusively for academic research. The study complied with institutional ethical protocols and data protection norms.

4. Data Analysis

4.1. Demographic Characteristics of Respondents

Table 2 presents the demographic profile of 206 SME owners or senior decision-makers surveyed from across diverse sectors in India. The majority of respondents fell within the age bracket of 31–40 years (44.2%), indicating a concentration of mid-career entrepreneurs. A younger demographic (under 30 years) comprised 33.0%, reflecting growing youth involvement in entrepreneurial ventures. Gender distribution showed male respondents forming 53.4% and females 46.6% of the sample. Most enterprises were privately held (71.8%), followed by partnerships or public entities (20.4%), and family-owned setups (7.8%). Nearly half of the businesses had been operational for 5–10 years (48.1%), representing mid-life ventures. Industry-wise, manufacturing (24.3%), IT/Tech (21.8%), and retail/e-commerce (16.5%) were dominant. Notably, 76.7% of the sample confirmed adoption of at least one digital solution within the last year.

Table 2. Respondent Demographics.

Variable	Category	Frequency (n)	Percentage (%)
Age	Below 30	68	33.0%
	31–40	91	44.2%
	41–50	33	16.0%
	51 and above	14	6.8%
Gender	Male	110	53.4%
	Female	96	46.6%
Type of Enterprise	Private	148	71.8%
	Public/Partnership	42	20.4%
	Family-Owned	16	7.8%
Years of Operation	Less than 5 years	37	18.0%
	5–10 years	99	48.1%
	11–15 years	47	22.8%
	More than 15 years	23	11.1%
Industry Type	Manufacturing	50	24.3%
	IT / Tech	45	21.8%
	Retail / E-commerce	34	16.5%
	Services (Finance, Legal)	29	14.1%
	Logistics & Supply Chain	18	8.7%
	Others	30	14.6%
Used Digital Tools	Yes	158	76.7%
	No	48	23.3%

4.2. Summary of SME Responses on Enhanced Digital Transformation and Security Measures

The Table 3, descriptive responses reveal overall positive perceptions and practices across all three constructs—Digital Transformation (DT), Financial Security Perception (FSP), and Fraud Resilience (FR)—among SME respondents.

A majority of respondents agreed or strongly agreed that they use analytics (72.8%), have integrated digital tools across core functions (68.9%), and have leadership support for digital culture (69.4%). This indicates a strong strategic adoption of digital practices in operational areas. Over 70% of SMEs showed confidence in the security of their financial systems, with 75.3% agreeing that their digital payment systems are fraud-protected, and 71.8% believing their data is protected through encryption and access control. Regular audits were slightly lower (64.1%) but still indicated proactive monitoring. While slightly more mixed, responses were still largely positive. Around 61–66% of respondents agreed or strongly agreed that they perform risk assessments, conduct employee training, and have defined fraud protocols. However, around 20–25% remained neutral, suggesting areas for improvement in awareness and formalization of resilience strategies. These findings suggest that SMEs are actively engaging in digital transformation, and this is positively reflected in their perceptions of financial security. Fraud resilience mechanisms, while present, show potential for further strengthening—particularly in staff training and systematized risk assessments.

Table 3. Summary of SME Responses on Enhanced Digital Transformation and Security Measures.

Construct	Item Statement	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
Digital Transformation	Our firm uses analytics (e.g., dashboards, data insights) to support decision-making.	6	14	36	100	50
Digital Transformation	We have integrated digital technologies into core functions like finance, ops, marketing.	9	15	40	95	47
Digital Transformation	The leadership actively promotes a digital culture.	7	17	39	97	46
Financial Security Perception	We regularly audit our financial systems for security and compliance.	11	19	44	89	43
Financial Security Perception	I believe our digital payment systems are secure against fraud.	5	12	34	102	53
Financial Security Perception	Our financial data is well protected through encryption and access control.	8	14	36	95	53
Fraud Resilience	We conduct regular fraud risk assessments.	13	21	46	85	41
Fraud Resilience	Our employees are trained to recognize and report suspicious activities.	12	20	44	91	39
Fraud Resilience	We have clearly defined fraud response protocols.	10	16	38	100	42

4.3. Measurement Model Evaluation

SmartPLS 4 was used to assess the psychometric properties of the measurement model, covering internal consistency, convergent validity, and discriminant validity.

4.3.1. Internal Reliability and Convergent Validity

As shown in Table 3, all latent constructs demonstrated strong reliability with Cronbach's alpha and composite reliability (CR) values well above the threshold of 0.70. Similarly, average variance extracted (AVE) values surpassed 0.50, confirming adequate convergent validity.

Table 4. Construct Reliability and Convergent Validity.

Construct	Cronbach's Alpha	Composite Reliability	AVE
Digital Transformation	0.869	0.901	0.673
Financial Security Perception	0.844	0.884	0.638
Fraud Resilience	0.880	0.914	0.702

4.3.2. Discriminant Validity – HTMT Analysis

All HTMT values are below the conservative threshold of 0.85, indicating that each construct is distinct from the others. This confirms discriminant validity of the measurement model and ensures that the constructs are not overlapping conceptually.

Table 5. HTMT Ratios.

Construct Pair	HTMT Value
Digital Transformation ↔ Financial Security Perception	0.731
Digital Transformation ↔ Fraud Resilience	0.704
Financial Security Perception ↔ Fraud Resilience	0.798

4.4. Structural Model Results

4.4.1. Collinearity Diagnostics (VIF)

All Variance Inflation Factor (VIF) values are well below the threshold of 5, indicating no multicollinearity issues among the predictor constructs. This ensures that the regression estimates are stable and reliable.

Table 6. VIF Statistics.

Path	VIF
DT → FSP	2.094
DT → FR	1.984
FSP → FR	2.412

4.4.2. Coefficient of Determination (R^2)

The R^2 value of 0.441 for *Financial Security Perception* indicates that 44.1% of its variance is explained by Digital Transformation — reflecting a moderate explanatory power.

The R^2 value of 0.605 for *Fraud Resilience* means that 60.5% of its variance is explained by both Digital Transformation and Financial Security Perception — representing a substantial level of prediction.

Table 7. R^2 Values for Endogenous Constructs.

Construct	R^2 Value	Strength
Financial Security Perception	0.441	Moderate
Fraud Resilience	0.605	Substantial

4.4.3. Path Coefficients and Hypotheses

Table 8. Path Coefficients.

Hypothesis	Path	β	t-value	p-value	Status
H1	DT → FSP	0.655	11.84	<0.001	Supported
H2	DT → FR	0.417	7.10	<0.001	Supported
H3	FSP → FR	0.389	5.94	<0.001	Supported

Above Table 8, represents All three hypotheses are supported and significant, confirming the structural model's validity.

H_1: Digital Transformation → Financial Security, Perception This strong and significant path suggests that Digital Transformation positively influences Financial Security Perception among SMEs.

H_2: Digital Transformation → Fraud Resilience, A moderate, statistically significant relationship indicating that Digital Transformation directly enhances Fraud Resilience.

H3: Financial Security Perception → Fraud Resilience, this result shows that higher perceived financial security contributes meaningfully to building Fraud Resilience.

4.4.4. Effect Size (f^2)

All path relationships showed medium to large effect sizes, as illustrated below. DT → FSP (f^2 = 0.761):

This represents a large effect, indicating that Digital Transformation has a strong impact on shaping Financial Security Perception in SMEs. DT → FR (f^2 = 0.299): A medium effect size, suggesting that Digital Transformation moderately contributes to enhancing Fraud Resilience. FSP → FR (f^2 = 0.244): Also a medium effect, showing that Financial Security Perception plays a notable role in improving Fraud Resilience. Overall, these results confirm that Digital Transformation is a major driver of perceived security, while both DT and FSP significantly influence resilience to fraud.

Table 9. Effect Size (f^2).

Path	f^2	Interpretation
DT → FSP	0.761	Large
DT → FR	0.299	Medium
FSP → FR	0.244	Medium

4.5. Predictive Relevance (Q^2)

The Q^2 values for both endogenous constructs were above zero, confirming predictive capability. Financial Security Perception ($Q^2 = 0.281$): This value indicates medium predictive relevance, meaning the model reasonably predicts SMEs' perception of financial security based on the independent variables. Fraud Resilience ($Q^2 = 0.395$): This represents high predictive relevance, showing that the model strongly predicts how resilient SMEs are to fraud, based on digital transformation and perceived financial security. The model demonstrates robust predictive accuracy, particularly in forecasting fraud resilience outcomes, validating the relevance of the proposed framework.

Table 10. Predictive Relevance (Q^2).

Construct	Q^2 Value	Level
Financial Security Perception	0.281	Medium
Fraud Resilience	0.395	High

4.6. Goodness-of-Fit (GoF)

GoF=$\sqrt{Average\ Communality\ (AVE) \times Average\ R^2}$

Where:

- AVE is the average variance extracted for all latent variables (from the measurement model).
- R^2 is the average R^2 value of the endogenous (dependent) constructs (from the structural model).

$= \sqrt{(0.671 \times 0.523)}$
$= \sqrt{0.3511} \approx 0.592$

This value exceeds the 0.36 benchmark, signifying a strong model fit.

Average AVE (0.671): Indicates strong convergent validity – the constructs explain a good amount of variance in their respective indicators. Average R^2 (0.523): Reflects moderate to substantial explanatory power of the model for endogenous variables (FSP and FR). GoF (0.592): Exceeds the threshold of 0.36, indicating a large overall model fit. The GoF value of 0.592 confirms that the model has a strong global explanatory power and overall fit, making it suitable for predicting outcomes in SME digital transformation, financial security perception, and fraud resilience.

Table 11. Goodness-of-Fit.

Component	Value	Interpretation
Average AVE	0.671	
Average R^2	0.523	
GoF	0.592	Large model fit

5. Conclusion

This study investigated the impact of Digital Transformation (DT) on Financial Security Perception (FSP) and Fraud Resilience (FR) among Indian SMEs using Partial Least Squares Structural Equation Modeling (PLS-SEM). The findings validate that DT plays a significant and direct role in improving both FSP and FR. Moreover, FSP significantly contributes to enhancing fraud resilience, underscoring its mediating role in the DT–FR pathway.

A structured and ethically sound research process was followed. Data from 206 SME decision-makers across India were collected via a validated Likert-scale questionnaire using purposive sampling. The research ensured measurement model validity, structural robustness, and strong model fit (GoF = 0.592), confirming its reliability and predictive accuracy. The study strictly adhered to ethical norms, with informed consent and data confidentiality maintained.

6. Key Findings

Finding	Interpretation
F1	DT significantly enhances FSP ($\beta = 0.655$, $f^2 = 0.761$)
F2	DT positively influences FR ($\beta = 0.417$, $f^2 = 0.299$)
F3	FSP is a significant predictor of FR ($\beta = 0.389$, $f^2 = 0.244$)
F4	The model demonstrates strong predictive relevance (Q^2 for FR = 0.395)
F5	High construct reliability and discriminant validity established
F6	Overall model fit is large (GoF = 0.592), supporting theoretical and practical applicability

7. Practical Implications for SMEs

1. SMEs should go beyond superficial adoption and embed digital technologies into core functions like finance, marketing, and operations.
2. Regular audits, encryption protocols, and secure digital payments must be institutionalized to boost stakeholder confidence.
3. Organizations must adopt structured fraud risk assessments, staff training, and real-time response protocols to enhance resilience.
4. SME leaders should promote a digital culture that aligns technological investment with secure business practices.

8. Theoretical Implications

- SEM-based evidence confirms that FSP is a key mediator between DT and FR, filling a gap in SME risk management literature.
- Contributes to digital transformation theory by emphasizing its security-oriented outcomes, particularly in resource-constrained contexts like SMEs.

9. Suggestions for Future Research

1. Test how firm size, digital maturity, or sector type may influence the DT–FSP–FR relationship.
2. Track changes in perceptions and resilience as digital ecosystems evolve over time.
3. Consider regulatory compliance, digital infrastructure access, and vendor partnerships as influencing factors.
4. Complement SEM with qualitative interviews to explore leadership perspectives and organizational culture in digital resilience.

References

Adekanmbi, A., & Oluwadare, M. (2025). AI-enabled fraud detection systems in Nigerian banks: Implications for SME adoption. *Journal of Financial Technology and Innovation, 12*(1), 34–49.

Andrewson, P., Singh, V., & Rao, R. (2025). Cloud-based security frameworks for SMEs: A practical approach to cyber risk mitigation. *International Journal of Cybersecurity and SMEs, 9*(2), 101–119.

Busari, T. M. (2025). Predictive analytics for fraud detection in small businesses: Evidence from the U.S. *Journal of Business Intelligence and Security, 7*(3), 89–103.

Hasanova, A., & Najafova, F. (2025). Governance challenges in SME digitalization: A risk-based perspective. *SME Management Review, 13*(2), 57–72.

Kumar, R. (2025). Zero trust security architecture for SMEs: Principles and implementation challenges. *Journal of Information Security Architecture, 18*(1), 11–26.

Matarazzo, M., & Celentano, G. (2025). AI and risk management in the digital economy: A review of applications in SMEs. *Technovation and Risk, 11*(1), 70–85.

Moorthy, M., Sivasubramanian, R., & Lee, K. W. (2020). Developing a fraud resilience framework for SMEs: ISO 37001 applications. *Journal of Business Ethics and Compliance, 8*(4), 122–138.

Murugesan, K., & Seema, D. (2025). Digital leadership and financial control in SME ecosystems: An empirical exploration. *Journal of Entrepreneurial Finance, 15*(1), 65–81.

Petrova, M., & Nuur, C. (2025). Building cyber resilience in resource-constrained enterprises: Lessons from digital partnership models. *European Journal of SME Studies, 17*(1), 44–59.

Pavlou, P. A. (2011). State of the information privacy literature: Where are we now and where should we go? *MIS Quarterly, 35*(4), 977–988. https://doi.org/10.2307/41409971

Tabassum, S. (2025). Cybersecurity awareness gaps in small Indian enterprises: A perception versus practice study. *Asia-Pacific Journal of Small Business, 19*(2), 99–112.

Verhoef, P. C., Broekhuizen, T., Bart, Y., Bhattacharya, A., Dong, J. Q., Fabian, N., & Haenlein, M. (2021). Digital transformation: A multidisciplinary reflection and research agenda. *Journal of Business Research, 122*, 889–901. https://doi.org/10.1016/j.jbusres.2019.09.022

Vial, G. (2019). Understanding digital transformation: A review and a research agenda. *The Journal of Strategic Information Systems, 28*(2), 118–144. https://doi.org/10.1016/j.jsis.2019.01.003

Vihaan, S., & Adrian, T. (2025). Business intelligence systems as enablers of fraud resilience in SMEs: A case-based approach. *Decision Support Journal, 13*(3), 78–92.