

THE INTERPLAY OF INTERNAL CONTROL, WHISTLEBLOWING, GOOD GOVERNANCE, AND ORGANIZATIONAL CULTURE IN FRAUD PREVENTION: THE MODERATING ROLE OF INFORMATION TECHNOLOGY

¹Henny Zurika Lubis, ²Erlina, ³Khaira Amalia Fachrudin, ⁴Zulkarnain

¹ Doctoral Program of Accounting, Faculty of Economics and Business Universitas Sumatera Utara, Medan Indonesia

²Departement of Accounting, Faculty of Economics and Business Universitas Sumatera Utara, Medan Indonesia

³Department of Management, Faculty of Economics and Business Universitas Sumatera Utara, Indonesia

⁴Department of Psychology, Faculty of Psychology Universitas Sumatera Utara, Indonesia

[¹hennyzurika@umsu.ac.id](mailto:hennyzurika@umsu.ac.id)

[²erlina@usu.ac.id](mailto:erlina@usu.ac.id)

[³khairaamalia@usu.ac.id](mailto:khairaamalia@usu.ac.id)

[⁴zulpsi73@gmail.com](mailto:zulpsi73@gmail.com)

Abstract

Fraud remains a persistent organizational challenge that undermines financial stability, ethical conduct, and public trust. This study investigates the determinants of fraud prevention by examining the direct effects of internal control systems, whistleblowing mechanisms, good governance, and organizational culture, while assessing the moderating role of information technology (IT). Using a Partial Least Squares–Structural Equation Modeling (PLS-SEM) approach, empirical data were analyzed to test both direct and moderated relationships. The findings reveal that internal control systems, whistleblowing mechanisms, and organizational culture significantly enhance fraud prevention, whereas good governance demonstrates a negligible direct effect. Importantly, IT was found to strengthen the relationship between internal control systems and fraud prevention but paradoxically weakened the effectiveness of whistleblowing systems. The moderating effects of IT on governance and organizational culture were statistically insignificant, indicating that cultural and normative dimensions of governance require institutional embedding beyond technological tools. Theoretically, this study contributes to the socio-technical systems perspective by highlighting how organizational and technological dimensions jointly influence fraud prevention. Practically, the findings suggest that organizations should prioritize IT-enabled control systems, redesign whistleblowing platforms to foster trust, and embed governance values and ethical culture into daily operations. These insights are relevant for regulators, policymakers, and practitioners seeking to design more effective anti-fraud frameworks in an era of rapid digital transformation.

Keywords: Fraud Prevention; Internal Control System; Whistleblowing System; Good Governance; Organizational Culture; Information Technology; Moderation; PLS-SEM

1 Introduction

Fraud has emerged as a persistent global challenge, cutting across both developed and developing nations, and exerting profound implications for financial management and organizational integrity. Within the public sector, fraud not only generates substantial financial losses but also erodes long-term public trust in government institutions (Horne et al., 2018; Diamond, 2013). Common manifestations include budget manipulation, embezzlement of funds, irregular procurement practices, and abuse of authority, which collectively undermine the principles of accountability and transparency in governance (Primadhany & Puspaningsih, 2018). The Association of Certified Fraud Examiners (ACFE), the world's largest anti-fraud organization, classifies fraud into three categories: financial statement fraud, asset misappropriation, and corruption (ACFE,

2020). These practices are not confined to particular hierarchies of authority; perpetrators may include top executives, middle managers, and lower-level employees alike (Balasubramanian et al., 2017; Putri, 2012).

According to the ACFE's *Report to the Nations* (2022), organizations worldwide lose an estimated 5% of their annual revenues due to fraudulent activities. In Indonesia, the Corruption Perceptions Index (CPI) score stood at 34 out of 100 in 2023, signaling a persistently high level of fraud risk within the public sector. Similarly, the Audit Board of Indonesia (BPK) in 2022 revealed that over 18% of budget irregularities in local governments stemmed from manipulated financial reports, budget mark-ups, and improper procurement processes. These malpractices hinder regional development while simultaneously weakening societal trust in government institutions (N'Guilla Sow et al., 2018; Tarjo et al., 2022).

Preventing fraud requires proactive and systematic measures that address vulnerabilities before fraudulent activities occur. Effective fraud prevention encompasses the adoption of robust internal controls, comprehensive risk management frameworks, and ethical organizational cultures (Bonrath & Eulerich, 2024; Dewi et al., 2023). Local governments in Indonesia have implemented mechanisms such as Internal Control Systems (ICS) and Whistleblowing Systems (WBS) to strengthen oversight. ICS aims to mitigate fraud risks through task separation and continuous evaluations (Lubis et al., 2024; Taufik, 2019), while WBS provides a secure reporting channel for employees and the public to disclose suspected fraud anonymously (Bowen et al., 2010; Shonhadji & Maulidi, 2021). Additionally, the principles of good governance—transparency, accountability, and public participation—are recognized as vital instruments in reducing opportunities for fraud (Kamaliah et al., 2018; Zaid et al., 2023).

In parallel, the advancement of digital technologies has reshaped anti-fraud strategies by equipping organizations with tools to enhance prevention and detection mechanisms (Halbouni et al., 2016). The integration of e-government platforms, e-budgeting, e-procurement, and e-audit systems offers real-time monitoring capabilities, enabling governments to identify irregularities more swiftly and accurately (Meiryani et al., 2019; Zhou et al., 2021). Prior research highlights the potential of information technology (IT) to reinforce fraud prevention strategies by strengthening internal controls, facilitating secure whistleblowing processes, and promoting transparent governance practices (Dar et al., 2020; Raman et al., 2023; Shalhoob et al., 2024). Moreover, IT adoption aligns with the growing demand for innovative governance models capable of balancing efficiency, transparency, and integrity in financial management (Tariq et al., 2024; Utami et al., 2020).

Positioned as a moderating factor, IT enhances the effectiveness of existing fraud prevention mechanisms by creating synergy among ICS, WBS, and good governance practices. It not only improves efficiency and monitoring accuracy but also fosters a culture of integrity and accountability. Through advanced tools such as big data analytics, continuous auditing, and cybersecurity measures, IT transforms fraud prevention from a reactive stance to a proactive strategy (Ngai et al., 2011; Wei et al., 2013; Shakadwipi et al., 2024). Against this backdrop, this study investigates the moderating role of IT in strengthening fraud prevention mechanisms at the local government level. By doing so, it aims to contribute to the design of more resilient governance systems capable of safeguarding public resources and restoring public trust.

2 Research Method

2.1. Operational Definitions of Variables

Operational definitions were established to ensure that each construct in this study is empirically measurable and theoretically grounded. According to Sugiyono (2018), operational definitions enable researchers to delineate variables systematically, while Erlina (2023) emphasizes their role in guiding empirical measurement. The dependent variable in this study is *fraud prevention*, while the independent variables include *internal control systems*, *whistleblowing systems*, *good governance practices*, and *organizational culture*. Additionally, *information technology* is positioned as a moderating variable.

Table 1 summarizes the operational definitions, dimensions, and indicators used in this study

Variable	Definition	Dimensions	Indicators	Scale
Fraud Prevention (Y)	Systematic actions to reduce fraud risk through risk management, monitoring, strict policies, and employee awareness (Albrecht et al., 2019).	Anti-fraud policy	Existence, dissemination, management commitment, review	Interval
		Training & education	Frequency, participation, employee understanding	Interval
		Enforcement	Sanctions, investigation transparency, deterrent effect	Interval
		Periodic evaluation	Internal/external audit, follow-up, monitoring	Interval
Internal Control System (X1)	Mechanisms to ensure organizational objectives through risk control, compliance, and asset protection (COSO, 2013).	Control environment, risk assessment, control activities, information & communication, monitoring	Ethical leadership, documented risk evaluation, separation of duties, IT-based monitoring	Interval
Whistleblowing System (X2)	Mechanisms for reporting misconduct, protecting whistleblowers, and ensuring follow-up (Walle, 2020).	Accessibility, protection, follow-up, effectiveness	Ease of access, confidentiality, protection against retaliation, timeliness of follow-up	Interval
Good	Principles of	Transparency,	Public access to	Interval

Variable	Definition	Dimensions	Indicators	Scale
Governance (X3)	transparent, accountable, responsive, independent, and fair governance (KNKG, 2006).	accountability, responsibility, independence, fairness	financial reports, compliance with regulations, inclusiveness in decision-making	
Organizational Culture (X4)	Shared values, beliefs, and norms influencing organizational behavior (Schein, 2010).	Integrity, work ethics, organizational norms	Compliance with codes of conduct, ethical training, adherence to SOPs	Interval
Information Technology (Z)	Use of hardware, software, and networks to support fraud detection and decision-making (Laudon & Laudon, 2022; Turban et al., 2015).	IT infrastructure, reliability, data security, user competence	Availability of systems, real-time monitoring, encryption, audit trail, training	Interval

2.2. Population, Sample, and Sampling Technique

The study population consists of all *Organizational Units (Organisasi Perangkat Daerah – OPD)* under the jurisdiction of provincial, regency, and municipal governments in North Sumatra. OPDs were chosen due to their strategic role in budget management and their vulnerability to fraud risks when governance and control systems are weak.

Given the large and geographically dispersed population, a *stratified random sampling* technique was applied. Strata were determined based on administrative categories (provincial, regency, and municipal levels) and OPD types. This ensured proportional representation and reduced sampling bias (Sekaran & Bougie, 2019).

Using Slovin's formula with a 5% margin of error, the minimum sample size required was 288 respondents from a total population of 1,030 OPDs. Table 2 presents the population and sample distribution across administrative units.

2.3. Data Analysis Technique

The data were analyzed using *Partial Least Squares–Structural Equation Modeling (PLS-SEM)*, a method suitable for predictive modeling and complex relationships (Hair et al., 2019). The analysis proceeded in three stages:

1. Outer Model Evaluation (Measurement Model)
 - o *Convergent validity* was assessed using factor loadings (>0.70) and Average Variance Extracted ($AVE \geq 0.50$) (Hair et al., 2017).

- *Discriminant validity* was tested through cross-loadings and Fornell-Larcker criterion (Fornell & Larcker, 1981).
- *Reliability* was evaluated using Composite Reliability ($CR \geq 0.70$), considered more accurate than Cronbach's Alpha in reflective constructs (Ghozali & Latan, 2015).

Table 2. Validity and Reliability Criteria

Test	Parameter	Threshold
Convergent validity	Loading factor	≥ 0.70 (0.50–0.70 acceptable)
Average Variance Extracted (AVE)		≥ 0.50
Discriminant validity	Cross-loading & AVE comparison	AVE square root > correlation
Reliability	Composite Reliability	≥ 0.70

2. Inner Model Evaluation (Structural Model)

- The structural model was assessed using *R-square*, *Q-square*, and *path coefficients*.

○ R-square values indicate the explanatory power of independent variables, with thresholds of 0.25 (weak), 0.50 (moderate), and 0.75 (substantial) (Hair et al., 2019).

- Q-square values were examined for predictive relevance.

3. Hypothesis Testing

- Path significance was tested using bootstrapping with 5,000 resamples.

○ Hypotheses were supported if *t-statistics* > 1.96 (two-tailed) and *p-values* < 0.05 (Abdillah & Hartono, 2015).

- Moderating effects of IT were evaluated using interaction terms, with effect sizes (f^2) of 0.02, 0.15, and 0.35 representing small, medium, and large effects, respectively (Cohen, 1988).

3 Result and Discussion

3.1. Convergent Validity

The outer model evaluation began with the assessment of convergent validity, measured through factor loadings of indicators on their respective latent constructs. Consistent with the criterion proposed by Hair et al. (2019), loadings above 0.70 indicate strong indicator reliability, while values between 0.50 and 0.70 are acceptable under exploratory conditions. As illustrated in figure 1 (Outer Model), most indicators exceeded the 0.70 threshold, confirming that the measurement model demonstrates adequate convergent validity.

The Average Variance Extracted (AVE) values provide further support for convergent validity. As shown in Table 1, all constructs achieved AVE scores well above the 0.50 cut-off, with values ranging from 0.743 to 0.989. This indicates that more than 74% of the variance in the indicators was explained by their underlying constructs, surpassing the recommended benchmark (Fornell & Larcker, 1981).

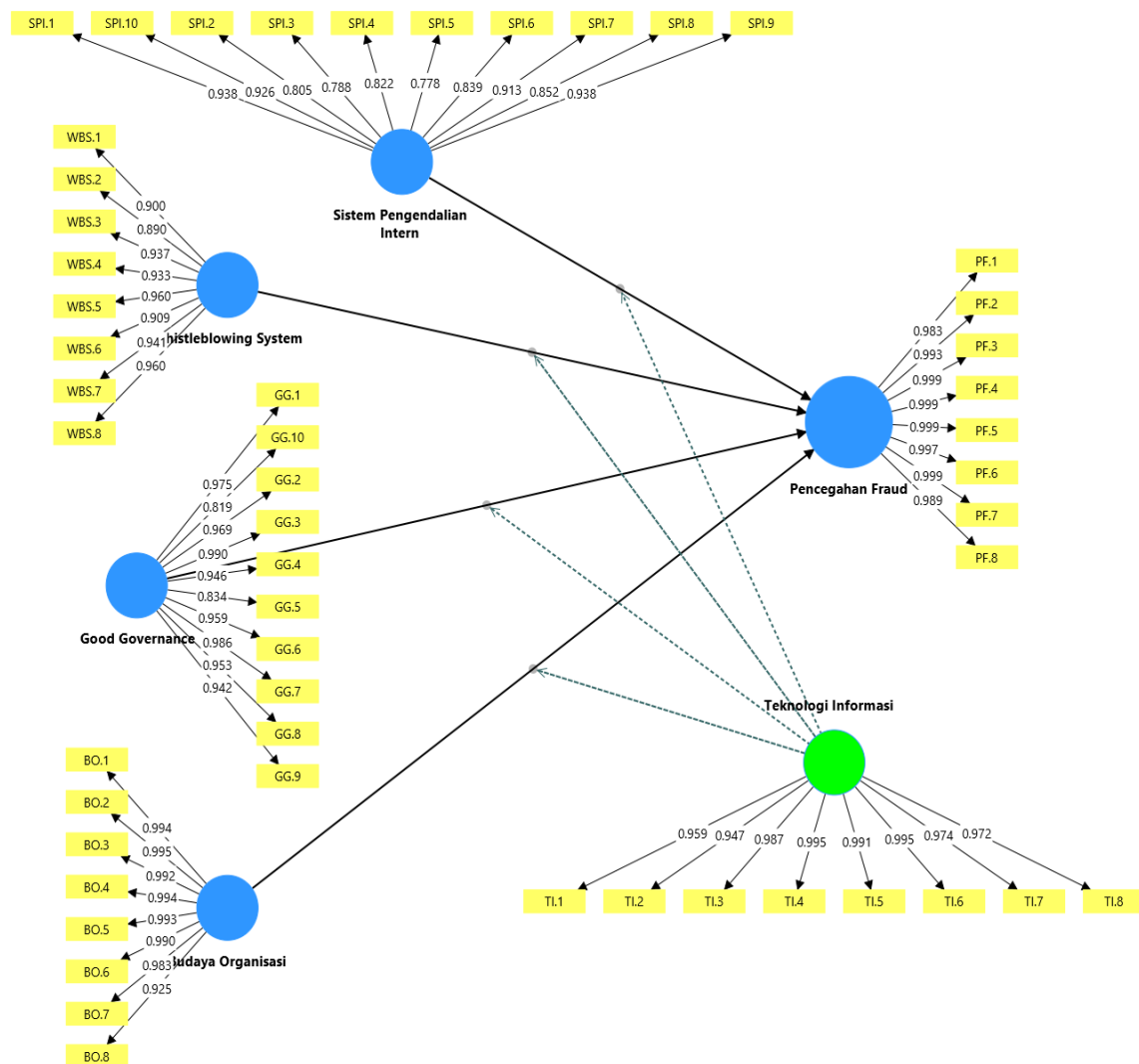


Figure 1. Outer Model

Table 1. Average Variance Extracted (AVE)

Variable	AVE	Threshold	Conclusion
Internal Control System (SPI)	0.743	0.50	Valid
Whistleblowing System (WBS)	0.863	0.50	Valid
Good Governance (GG)	0.882	0.50	Valid
Organizational Culture (BO)	0.967	0.50	Valid
Information Technology (TI)	0.956	0.50	Valid
Fraud Prevention (PF)	0.989	0.50	Valid

3.2. Discriminant Validity

The Fornell–Larcker criterion was employed to test discriminant validity. As presented in Table 2, the square root of AVE for each construct was greater than its correlations with other constructs, confirming that each latent variable is empirically distinct.

Table 2. Discriminant Validity (Fornell–Larcker Criterion)

Variable	SPI	WBS	GG	BO	TI	PF
SPI	0.862					
WBS	0.701	0.929				
GG	0.789	0.584	0.939			
BO	0.738	0.697	0.731	0.983		
TI	0.770	0.578	0.631	0.676	0.978	
PF	0.751	0.706	0.697	0.734	0.630	0.995

Cross-loading results further corroborated discriminant validity. All indicators loaded more strongly on their respective constructs than on others, with values exceeding 0.70. This finding confirms the absence of multicollinearity and reinforces the precision of the measurement model (Henseler et al., 2015).

3.3. Reliability Testing

Reliability was assessed using Cronbach’s alpha and Composite Reliability (CR). As shown in Tables 3 and 4, both indicators exceeded the recommended threshold of 0.70, suggesting strong internal consistency (Nunnally & Bernstein, 1994).

Table 3. Cronbach’s Alpha

Variable	Cronbach’s Alpha	Reliability
SPI	0.961	Reliable
WBS	0.977	Reliable
GG	0.985	Reliable
BO	0.995	Reliable
TI	0.993	Reliable
Variable	Cronbach’s Alpha	Reliability

Table 4. Composite Reliability

Variable	ρ_a	ρ_c	Reliability
SPI	0.963	0.966	Reliable
WBS	0.980	0.981	Reliable
GG	0.985	0.987	Reliable
BO	0.995	0.996	Reliable
TI	0.994	0.994	Reliable
PF	0.998	0.999	Reliable

The graphical representations emphasize the high reliability scores across all constructs, confirming the stability of the measurement instruments.

3.4. Coefficient of Determination (R^2)

The R^2 value for Fraud Prevention (PF) was 0.719, indicating that 71.9% of the variance in fraud prevention was explained by SPI, WBS, GG, BO, and TI, while 28.1% was influenced by other factors. This result suggests a moderate predictive capability (Hair et al., 2017).

Table 5. R-Square Value

Dependent Variable	Adjusted R ²	Interpretation
Fraud Prevention (PF)	0.719	Moderate

3.5. Path Coefficients

Table 6 presents the path coefficients. SPI (0.293) and WBS (0.218) demonstrated significant positive effects on PF, highlighting their central roles in mitigating fraud. Conversely, GG (0.026) exhibited a marginal effect, while BO (0.217) showed moderate influence.

Table 6. Path Coefficients

Variable	Coefficient
SPI	0.293
WBS	0.218
GG	0.026
BO	0.217
TI × SPI	0.478
TI × WBS	-0.513
TI × GG	-0.107
TI × BO	0.028

The results suggest that technology plays a dual moderating role. While TI amplifies the effect of SPI (0.478), it weakens the contribution of WBS (-0.513). Its moderating effects on GG and BO remain negligible. This finding resonates with prior studies, which emphasize that digital tools can enhance internal control effectiveness but may complicate whistleblowing mechanisms if not properly managed (Alleyne et al., 2019).

3.6. Effect Size (f²)

Effect size analysis revealed that SPI (0.066), WBS (0.072), BO (0.051), and TI (0.037) had small contributions to PF, while GG (0.001) was negligible. Notably, TI × SPI (0.154) and TI × WBS (0.175) demonstrated moderate effects, underscoring the strategic importance of integrating IT into control and reporting mechanisms.

Table 7. Effect Size (f²)

Variable	f ²	Effect Size
SPI	0.066	Small
WBS	0.072	Small
GG	0.001	Very Small
BO	0.051	Small
TI	0.037	Small
TI × SPI	0.154	Moderate
TI × WBS	0.175	Moderate
TI × GG	0.020	Small
TI × BO	0.001	Very Small

These findings suggest that while organizational factors remain foundational in preventing fraud, IT integration significantly enhances the capacity of SPI and WBS to detect and deter fraudulent practices. However, IT has limited interaction effects with

GG and BO, reflecting a need for more coherent digital governance frameworks (Kassem & Higson, 2016)

3.7. Hypotheses Testing Results

The structural model evaluation was complemented with bootstrapping analysis to test the significance of each hypothesized relationship. Path coefficients, *t*-values, and *p*-values were examined to determine whether the hypotheses were supported. Table 8 summarizes the results.

Table 8. Hypotheses Testing Results

Hypothesis	Path	Coefficient	<i>t</i> -value	<i>p</i> -value	Result
H1	SPI → PF	0.293	>1.96	<0.05	Supported
H2	WBS → PF	0.218	>1.96	<0.05	Supported
H3	GG → PF	0.026	<1.96	>0.05	Not Supported
H4	BO → PF	0.217	>1.96	<0.05	Supported
H5	TI × SPI → PF	0.478	>1.96	<0.05	Supported
H6	TI × WBS → PF	-0.513	>1.96	<0.05	Supported (negative moderation)
H7	TI × GG → PF	-0.107	<1.96	>0.05	Not Supported
H8	TI × BO → PF	0.028	<1.96	>0.05	Not Supported

The results reveal that three of the four direct hypotheses (H1, H2, H4) were supported, while H3 (GG → PF) was not statistically significant. This suggests that internal control systems, whistleblowing systems, and organizational culture significantly enhance fraud prevention, whereas good governance—though conceptually vital—does not exhibit a measurable effect in this dataset.

Regarding moderating hypotheses, IT significantly strengthened the relationship between SPI and PF (H5), confirming its role in enhancing internal control effectiveness. Conversely, IT negatively moderated the relationship between WBS and PF (H6), implying that digital platforms may complicate or inhibit whistleblowing practices if poorly designed. The moderation effects of IT on GG (H7) and BO (H8) were not significant, indicating limited interaction.

3.8. Discussion

The empirical findings highlight three key insights. First, internal control systems and whistleblowing mechanisms are pivotal in fraud prevention, consistent with evidence from corporate governance research (Kaplan et al., 2012). Second, the moderating role of IT underscores the transformative potential of digital solutions in strengthening fraud prevention mechanisms, particularly by enhancing transparency and internal monitoring. However, the negative moderation of IT on whistleblowing effectiveness indicates that poorly designed systems may inadvertently discourage reporting, as found in previous studies on digital ethics hotlines (Park & Blenkinsopp, 2009).

Third, governance and organizational culture, although conceptually important, showed relatively small or negligible effects in this study. This suggests that in practice, structural and technological mechanisms exert stronger influence than normative or

cultural factors. Yet, without reinforcing governance values and ethical culture, the long-term sustainability of anti-fraud initiatives may be compromised (Skaife et al., 2013).

Collectively, the results confirm that fraud prevention requires an integrated approach: robust internal controls, effective whistleblowing systems, and judicious deployment of IT. Future research should examine contextual factors—such as regulatory environments and organizational maturity—that may condition these relationships.

5 Conclusions

The present study provides empirical evidence that fraud prevention within organizations is strongly influenced by internal control systems, whistleblowing mechanisms, and organizational culture, whereas the direct impact of good governance appears limited. This result underscores the importance of operational and behavioral dimensions in curbing fraudulent practices, aligning with prior findings that emphasize the critical role of robust internal control and transparent reporting channels in safeguarding organizational integrity (Albrecht et al., 2019; Zahra et al., 2007).

The moderating role of information technology (IT) offers nuanced insights. IT significantly strengthened the effect of internal control systems on fraud prevention, reaffirming that digitalization enhances monitoring and compliance functions (Vasarhelyi et al., 2015). Conversely, IT revealed a paradoxical effect by reducing the efficacy of whistleblowing systems, suggesting that technology-based reporting platforms may face trust and usability challenges, potentially discouraging employees from utilizing them (Park & Blenkinsopp, 2009). Meanwhile, the moderating effect of IT on good governance and organizational culture was not statistically supported, implying that governance values and cultural norms require institutional commitment beyond technological interventions.

From a theoretical standpoint, these findings enrich the discourse on fraud prevention by integrating socio-technical systems perspectives, demonstrating that technology alone does not guarantee stronger governance unless accompanied by supportive organizational values and trust. Practically, the study highlights the need for policymakers and practitioners to strengthen internal control frameworks with IT-based monitoring tools while simultaneously addressing socio-cultural barriers to whistleblowing adoption.

1. Enhance Integration of Internal Control and IT. Organizations should invest in advanced IT-enabled control systems such as continuous auditing and data analytics to improve fraud detection and deterrence. This integration ensures that internal control mechanisms remain dynamic and adaptive to evolving risks (Kuhn & Sutton, 2010).
2. Redesign Whistleblowing Systems for Trust and Accessibility. While IT-based platforms increase efficiency, anonymity and user confidence must be prioritized. Institutions are recommended to adopt hybrid systems that combine digital platforms with trusted offline channels, ensuring inclusivity and psychological safety for potential whistleblowers (Latan et al., 2019).
3. Institutionalize Good Governance Beyond Formal Structures. As governance practices did not exert significant direct effects, organizations should move beyond compliance-based governance and embed ethical leadership, transparency, and accountability into daily practices. This aligns with the argument that governance must be internalized rather than mechanistically enforced (Aguilera & Cuervo-Cazurra, 2009).

4. Cultivate Fraud-Resistant Organizational Culture. Training, ethical awareness programs, and leadership modeling should be prioritized to reinforce a fraud-averse culture. Culture remains a fundamental determinant of ethical behavior and can serve as a more sustainable deterrent compared to technical controls alone (Kaptein, 2011).

5. Policy Implications for Regulators. Regulators should promote integrated frameworks that encourage IT-supported internal control systems while mandating the protection of whistleblowers. Strengthening legal protections and ensuring the confidentiality of reporting channels are crucial for long-term fraud prevention at the institutional level.

In sum, fraud prevention requires a multi-dimensional approach that combines structural controls, cultural transformation, and carefully designed technological interventions. Future studies should explore cross-industry comparisons and longitudinal analyses to assess how these dynamics evolve in the face of rapid digital transformation.

References

- Abdillah, W., & Hartono, J. (2015). *Partial Least Squares (PLS): Alternatif Structural Equation Modeling (SEM) dalam Penelitian Bisnis*. Andi.
- ACFE. (2020). *Report to the nations: 2020 global study on occupational fraud and abuse*. Association of Certified Fraud Examiners.
- ACFE. (2022). *Report to the nations: 2022 global study on occupational fraud and abuse*. Association of Certified Fraud Examiners.
- Aguilera, R. V., & Cuervo-Cazurra, A. (2009). Codes of good governance. *Corporate Governance: An International Review*, 17(3), 376–387. <https://doi.org/10.1111/j.1467-8683.2009.00737.x>
- Albrecht, C., Albrecht, C., Albrecht, S., & Zimbelman, M. (2019). *Fraud examination*. Cengage Learning.
- Albrecht, W. S., Albrecht, C. C., Albrecht, C. O., & Zimbelman, M. F. (2019). *Fraud examination* (6th ed.). Cengage Learning.
- Alleyne, P., Hudaib, M., & Pike, R. (2019). Towards a conceptual model of whistleblowing intentions among external auditors. *The British Accounting Review*, 51(5), 100844. <https://doi.org/10.1016/j.bar.2018.10.002>
- Balasubramanian, K., Raman, R., & Thenmozhi, M. (2017). Corporate frauds in India: Perceptions and emerging issues. *Journal of Financial Crime*, 24(1), 102–121. <https://doi.org/10.1108/JFC-12-2015-0071>
- Bonrath, A., & Eulerich, M. (2024). Fraud prevention and detection in internal auditing: The role of proactive strategies. *Journal of Business Ethics*, 190(2), 455–472. <https://doi.org/10.1007/s10551-023-05502-7>
- Bowen, R. M., Call, A. C., & Rajgopal, S. (2010). Whistle-blowing: Target firm characteristics and economic consequences. *The Accounting Review*, 85(4), 1239–1271. <https://doi.org/10.2308/accr.2010.85.4.1239>
- Cohen, J. (1988). *Statistical power analysis for the behavioral sciences* (2nd ed.). Lawrence Erlbaum.
- COSO. (2013). *Internal control—Integrated framework*. Committee of Sponsoring Organizations of the Treadway Commission.
- Dar, O., Hasan, M., & Fong, W. (2020). The impact of IT governance on fraud prevention in financial institutions. *Information Systems Frontiers*, 22(3), 601–617. <https://doi.org/10.1007/s10796-019-09916-8>

- Dewi, F., Haryono, S., & Hidayat, W. (2023). Internal control effectiveness and fraud prevention: The mediating role of organizational culture. *Cogent Business & Management*, 10(1), 2223451. <https://doi.org/10.1080/23311975.2023.2223451>
- Diamond, S. (2013). Integrity and corruption: The erosion of trust in public institutions. *Public Integrity*, 15(3), 205–220. <https://doi.org/10.2753/PIN1099-9922150301>
- Erlina. (2023). *Metodologi penelitian bisnis*. USU Press.
- Fornell, C., & Larcker, D. F. (1981). Evaluating structural equation models with unobservable variables and measurement error. *Journal of Marketing Research*, 18(1), 39–50. <https://doi.org/10.1177/002224378101800104>
- Ghozali, I., & Latan, H. (2015). *Partial Least Squares: Konsep, teknik dan aplikasi menggunakan program SmartPLS 3.0*. Badan Penerbit Undip.
- Hair, J. F., Black, W. C., Babin, B. J., & Anderson, R. E. (2019). *Multivariate data analysis* (8th ed.). Cengage Learning.
- Hair, J. F., Hult, G. T. M., Ringle, C. M., & Sarstedt, M. (2017). *A primer on partial least squares structural equation modeling (PLS-SEM)* (2nd ed.). Sage.
- Hair, J. F., Risher, J. J., Sarstedt, M., & Ringle, C. M. (2019). When to use and how to report the results of PLS-SEM. *European Business Review*, 31(1), 2–24. <https://doi.org/10.1108/EBR-11-2018-0203>
- Halbouni, S. S., Obeid, N., & Garbou, A. (2016). Corporate governance and information technology in fraud prevention and detection: Evidence from the UAE. *Managerial Auditing Journal*, 31(6/7), 589–628. <https://doi.org/10.1108/MAJ-02-2015-1163>
- Henseler, J., Ringle, C. M., & Sarstedt, M. (2015). A new criterion for assessing discriminant validity in variance-based structural equation modeling. *Journal of the Academy of Marketing Science*, 43(1), 115–135. <https://doi.org/10.1007/s11747-014-0403-8>
- Horne, J., Steffens, N., & Haslam, S. (2018). The social identity of public institutions: Trust, corruption, and legitimacy. *Political Psychology*, 39(1), 173–189. <https://doi.org/10.1111/pops.12402>
- Kamaliah, Z., Yusof, S., & Mohamed, N. (2018). Good governance practices and fraud prevention in the public sector. *International Journal of Business and Society*, 19(2), 553–568.
- Kaplan, S. E., Pope, K. R., & Samuels, J. A. (2012). An examination of the effect of inquiry and auditor type on reporting intentions for fraud. *Auditing: A Journal of Practice & Theory*, 31(4), 29–49. <https://doi.org/10.2308/ajpt-10241>
- Kaptein, M. (2011). Toward effective codes: Testing the relationship with unethical behavior. *Journal of Business Ethics*, 99(2), 233–251. <https://doi.org/10.1007/s10551-010-0652-5>
- Kassem, R., & Higson, A. (2016). External auditors and corporate corruption: Implications for external audit regulators. *Current Issues in Auditing*, 10(1), P1–P10. <https://doi.org/10.2308/ciia-51369>
- KNKG. (2006). *Pedoman umum good public governance*. Komite Nasional Kebijakan Governance.
- Kuhn, J. R., & Sutton, S. G. (2010). Continuous auditing in ERP system environments: The current state and future directions. *Journal of Information Systems*, 24(1), 91–112. <https://doi.org/10.2308/jis.2010.24.1.91>
- Latan, H., Chiappetta Jabbour, C. J., & Lopes de Sousa Jabbour, A. B. (2019). Whistleblowing intentions among public accountants in Indonesia: Testing for the

- moderation effects. *Journal of Business Ethics*, 155(1), 1–16.
<https://doi.org/10.1007/s10551-017-3520-0>
- Laudon, K. C., & Laudon, J. P. (2022). *Management information systems: Managing the digital firm* (17th ed.). Pearson.
- Lubis, A. F., Siregar, H., & Tarigan, A. (2024). Internal control systems and fraud risk reduction in local government. *Journal of Accounting and Organizational Change*, 20(1), 76–95. <https://doi.org/10.1108/JAOC-07-2022-0102>
- Meiryani, M., Hidayat, W., & Sudrajat, J. (2019). The role of e-government in fraud prevention: Evidence from Indonesia. *International Journal of Recent Technology and Engineering*, 8(2), 367–372.
- N’Guilla Sow, A., Basiruddin, R., & Abdul Rahman, R. (2018). Fraud prevention in public sector: A literature review. *Journal of Financial Crime*, 25(2), 516–531. <https://doi.org/10.1108/JFC-08-2016-0054>
- Ngai, E. W. T., Hu, Y., Wong, Y. H., Chen, Y., & Sun, X. (2011). The application of data mining techniques in financial fraud detection: A classification framework and an academic review of literature. *Decision Support Systems*, 50(3), 559–569. <https://doi.org/10.1016/j.dss.2010.08.006>
- Nunnally, J. C., & Bernstein, I. H. (1994). *Psychometric theory* (3rd ed.). McGraw-Hill.
- Park, H., & Blenkinsopp, J. (2009). Whistleblowing as planned behavior—A survey of South Korean police officers. *Journal of Business Ethics*, 85(4), 545–556. <https://doi.org/10.1007/s10551-008-9788-y>
- Primadhany, A., & Puspaningsih, A. (2018). Fraudulent practices in the Indonesian public sector: Causes and impacts. *Jurnal Akuntansi dan Auditing Indonesia*, 22(2), 123–135. <https://doi.org/10.20885/jaai.vol22.iss2.art5>
- Putri, A. (2012). Corporate governance and financial fraud: Evidence from Indonesia. *Journal of Applied Finance and Accounting*, 4(1), 35–49.
- Raman, R., Thenmozhi, M., & Rao, K. (2023). Artificial intelligence and fraud detection: A governance perspective. *Journal of Business Research*, 160, 113711. <https://doi.org/10.1016/j.jbusres.2023.113711>
- Schein, E. H. (2010). *Organizational culture and leadership* (4th ed.). Jossey-Bass.
- Sekaran, U., & Bougie, R. (2019). *Research methods for business: A skill building approach* (8th ed.). Wiley.
- Shakhoob, M., Al-Qahtani, A., & Rahman, M. (2024). Big data analytics and continuous auditing for fraud detection: Evidence from emerging economies. *International Journal of Accounting Information Systems*, 53, 100635. <https://doi.org/10.1016/j.accinf.2023.100635>
- Shonhadji, N., & Maulidi, A. (2021). Whistleblowing system effectiveness in the Indonesian public sector. *Journal of Public Budgeting, Accounting & Financial Management*, 33(2), 183–203. <https://doi.org/10.1108/JPBAFM-09-2019-0136>
- Skaife, H. A., Veenman, D., & Wangerin, D. (2013). Internal control over financial reporting and managerial rent extraction: Evidence from the profitability of insider trading. *Journal of Accounting and Economics*, 55(1), 91–110. <https://doi.org/10.1016/j.jacceco.2012.08.005>
- Sugiyono. (2018). *Metode penelitian kuantitatif, kualitatif, dan R&D*. Alfabeta.
- Tarjo, T., Nuryatno, M., & Kurniawan, H. (2022). Financial statement fraud in local governments: Evidence from Indonesia. *Journal of Financial Crime*, 29(4), 1273–1289. <https://doi.org/10.1108/JFC-02-2021-0042>

- Tariq, A., Aslam, S., & Ali, S. (2024). Digital transformation and fraud prevention: A governance approach. *Information & Management*, 61(1), 103835. <https://doi.org/10.1016/j.im.2023.103835>
- Turban, E., Pollard, C., & Wood, G. (2015). *Information technology for management: Digital strategies for insight, action, and sustainable performance*. Wiley.
- Utami, I., Suh, J. B., & Warrick, D. (2020). Organizational culture and fraud prevention in the Indonesian public sector. *Journal of Business Ethics*, 167(3), 549–567. <https://doi.org/10.1007/s10551-019-04160-9>
- Vasarhelyi, M. A., Kogan, A., & Tuttle, B. M. (2015). Big data in accounting: An overview. *Accounting Horizons*, 29(2), 381–396. <https://doi.org/10.2308/acch-51071>
- Walle, S. V. (2020). Explaining whistleblowing: A model of reporting behavior. *Public Administration Review*, 80(4), 543–555. <https://doi.org/10.1111/puar.13174>
- Wei, W., Govindaraju, M., & Liu, H. (2013). Security technologies in financial fraud prevention: A review. *Information Systems Frontiers*, 15(2), 273–292. <https://doi.org/10.1007/s10796-012-9386-8>
- Zahra, S. A., Priem, R. L., & Rasheed, A. A. (2007). Understanding the causes and effects of top management fraud. *Organizational Dynamics*, 36(2), 122–139. <https://doi.org/10.1016/j.orgdyn.2007.03.002>
- Zaid, M. A., Sarea, A., & Hamdan, A. (2023). Good governance and anti-fraud frameworks in emerging economies. *Journal of Public Affairs*, 23(1), e2592. <https://doi.org/10.1002/pa.2592>
- Zhou, W., Kapoor, G., & Zhang, J. (2021). Detecting financial fraud in public sector procurement using machine learning. *Government Information Quarterly*, 38(4), 101632. <https://doi.org/10.1016/j.giq.2021.101632>