

Strengthening Digital Security and Compliance to Prevent Credit Card Fraud in Indonesian Banking: An Sdg-Aligned Approach to Sustainable Financial Integrity

Yuli Dewi

Universitas Muhammadiyah Cirebon, Cirebon, Indonesia

Email: yuli.dewi@umc.ac.id

Received: December 29, 2026 | Revised: January 10, 2026 | Accepted: January 15, 2026

Abstract. This study examines the factors influencing fraud prevention in Indonesia's banking credit card business, which is increasingly vulnerable to cybercrime as online transactions continue to grow. The research aligns with Sustainable Development Goals (SDGs), particularly SDG 16 (Peace, Justice, and Strong Institutions) and SDG 9 (Industry, Innovation, and Infrastructure), by emphasizing the importance of secure, transparent, and innovative financial systems. The study analyzes the effects of digital security, compliance management systems, and fraud brainstorming on credit card fraud prevention, with the competence of the three lines of defense tested as a moderating variable. Using descriptive, explanatory, and verification methods, data were collected through questionnaires and interviews with 108 supervisory personnel from credit card-issuing banks and financial institutions registered with Bank Indonesia and the Indonesian Credit Card Association. Moderated Regression Analysis (MRA) using SPSS was applied to evaluate the model. The results show that digital security, compliance management systems, and fraud brainstorming significantly improve fraud prevention, although the competence of the three lines of defense does not significantly moderate these relationships. These findings highlight the importance of integrating technology, compliance, and collaborative brainstorming to strengthen fraud mitigation and support sustainable financial integrity, while noting that competence alone may not guarantee enhanced preventive outcomes.

Keywords: Digital Security; Compliance Management System; Fraud Brainstorming; Three Lines of Defense; Credit Card Fraud Prevention

INTRODUCTION

The rapid development of financial technology has increased efficiency and convenience within the banking sector, yet it has also heightened vulnerability to fraud. Global surveys estimate that the banking industry loses approximately 5% of its annual revenue to fraudulent activities, with credit card fraud such as carding, phishing, skimming, and account takeover remaining one of the most prevalent forms. In Indonesia, the accelerated growth of online transactions further amplifies these risks, creating an urgent need for stronger and more integrated fraud prevention strategies.

This research aligns with key priorities of the United Nations Sustainable Development Goals (SDGs), particularly **SDG 16: Peace, Justice, and Strong Institutions**, which emphasizes reducing corruption, strengthening institutional integrity, and enhancing fraud prevention; and **SDG 9: Industry, Innovation, and Infrastructure**, which highlights the importance of secure and innovative digital infrastructure in supporting financial resilience. Strengthening fraud prevention mechanisms within the banking industry contributes directly to these global objectives by promoting transparency, accountability, and sustainable financial governance.

The study examines three primary determinants of fraud prevention—**digital security, compliance management systems, and fraud brainstorming**—as essential components in mitigating credit card fraud. Additionally, it investigates whether the **competence of the three lines of defense** (business units, risk and compliance management, and internal audit) moderates the relationships among these factors. By integrating technological safeguards, regulatory compliance, and collaborative risk assessment, the study aims to provide a comprehensive understanding of fraud prevention dynamics within Indonesia's credit card banking landscape.

LITERATURE REVIEW

This study is grounded in several theoretical perspectives relevant to fraud prevention in the banking sector. **Agency Theory** (Jensen & Meckling, 1976) explains the conflicts of interest between owners and agents, which may create opportunities for fraudulent behavior. **Stewardship Theory** (Donaldson & Davis, 1991) emphasizes managerial responsibility and competence as deterrents to fraud. **Game Theory** (Neumann & Morgenstern, 1944) describes the strategic interactions between fraudsters and financial institutions, highlighting the need for adaptive defense mechanisms. **Signaling Theory** (Akerlof, 1970) suggests that strong compliance management systems act as signals of integrity to stakeholders. Meanwhile, **Social Judgment Theory** (Sherif, 1980) underscores the role of collaborative brainstorming in shaping fraud risk assessments by integrating diverse perspectives across organizational functions.

The key variables examined in this study include:

1. **Digital Security**, which encompasses the confidentiality, integrity, and availability of information systems as fundamental components of fraud prevention.
2. **Compliance Management System (CMS)**, involving oversight, change management, training, and monitoring to ensure adherence to regulatory and internal standards.
3. **Fraud Brainstorming**, referring to collaborative sessions aimed at identifying potential fraud schemes and assessing associated risks.
4. **Competence of the Three Lines of Defense**, incorporating knowledge, skills, intrinsic motivation, and collaborative mindset across business units, risk management, compliance, and internal audit.

From a sustainability perspective, the theoretical foundation and constructs in this study contribute to **SDG 16 (Peace, Justice, and Strong Institutions)** by promoting stronger governance and fraud-resistant institutional practices. They also support **SDG 9 (Industry, Innovation, and Infrastructure)** by highlighting the importance of robust digital security and technologically resilient financial infrastructure.

RESEARCH HYPOTHESES

Based on the theoretical foundations and empirical findings of this study, the following hypotheses are proposed:

H1 Digital security has a positive and significant effect on credit card fraud prevention in Indonesian banking institutions.

H2 The compliance management system has a positive and significant effect on credit card fraud prevention in Indonesian banking institutions.

H3 Fraud brainstorming has a positive and significant effect on credit card fraud prevention in Indonesian banking institutions.

H4 The competence of the three lines of defense does not significantly moderate the relationship between digital security and credit card fraud prevention.

H5 The competence of the three lines of defense does not significantly moderate the relationship between the compliance management system and credit card fraud prevention.

H6 The competence of the three lines of defense does not significantly moderate the relationship between fraud brainstorming and credit card fraud prevention.

H7 Digital security, compliance management systems, and fraud brainstorming simultaneously have a significant effect on credit card fraud prevention in Indonesian banking institutions.

Relevance of Research Hypotheses to the Sustainable Development Goals (SDGs)

This study integrates fraud prevention within the broader framework of sustainable development, particularly **SDG 9** and **SDG 16**, by linking governance quality, technological resilience, and institutional integrity in the banking sector.

1. SDG 9: Industry, Innovation, and Infrastructure

Hypotheses **H1** and **H3** directly support SDG 9 by emphasizing the role of secure digital infrastructure and innovative organizational practices. Digital security strengthens the resilience of financial infrastructure against cyber threats, while fraud brainstorming represents an adaptive and innovative approach to anticipating emerging fraud schemes. Together, these mechanisms enhance the sustainability and reliability of banking systems in the digital era.

2. SDG 16: Peace, Justice, and Strong Institutions

Hypotheses **H2** and **H7** align with SDG 16 by highlighting the importance of strong compliance management systems and integrated governance mechanisms. Effective compliance management promotes transparency, accountability, and regulatory adherence, which are essential for reducing fraud and strengthening institutional trust. The simultaneous influence of digital security, compliance, and fraud brainstorming reflects the need for systemic governance rather than reliance on individual competence alone.

RESEARCH METHODOLOGY

This study employed a descriptive, explanatory, and verification research design. The population consisted of Indonesian banks issuing credit cards, and data were collected using census sampling, resulting in 108 respondents from supervisory positions across the three lines of defense. Primary data were obtained through questionnaires and interviews to capture perceptions regarding digital security, compliance management systems, and fraud prevention practices. The analysis utilized multiple linear regression and Moderated Regression Analysis (MRA) to examine both direct effects and the moderating role of the competence of the three lines of defense.

A. Data Collection:

- Questionnaires and structured interviews.
- Respondents represented units of business operations, risk management, compliance, and internal audit.

B. Data Analysis:

- Multiple linear regression to test direct effects.
- Moderated Regression Analysis (MRA) with SPSS to evaluate moderating influence of competence.

RESULTS AND DISCUSSION

A. Descriptive Analysis

Data were collected from 108 supervisory personnel representing the three lines of defense business units, risk and compliance management, and internal audit from credit card-issuing banks registered with Bank Indonesia and the Indonesian Credit Card Association. Overall, respondents indicated positive perceptions of digital security practices, compliance management systems, and fraud brainstorming activities in supporting fraud control.

B. Classical Assumption Tests

Before regression analysis, several assumption tests were conducted to ensure model validity.

- **Normality Test:** Kolmogorov-Smirnov results showed a significance value of $0.200 > 0.05$, indicating normally distributed data.
- **Multicollinearity Test:** All independent variables had VIF values < 10 and tolerance > 0.1 , suggesting no multicollinearity issues.
- **Heteroskedasticity Test:** Glejser test significance values were > 0.05 for all variables, demonstrating the absence of heteroskedasticity. These results confirm that the data met the required assumptions for regression analysis.

C. Regression Analysis

1. Simultaneous Test (F-Test)

The F-test result ($\text{sig.} = 0.002 < 0.05$) indicates that digital security, compliance management systems, and fraud brainstorming simultaneously exert a significant influence on credit card fraud prevention.

2. Partial Test (t-Test)

- **Digital Security → Fraud Prevention:** Regression coefficient = 1.045, significance < 0.05 , indicating that enhanced authentication, encryption, and disaster recovery planning significantly reduce fraud risk.
- **Compliance Management System → Fraud Prevention:** Regression coefficient = 0.916, significance < 0.05 , showing that effective oversight, policies, training, and monitoring support stronger fraud prevention.
- **Fraud Brainstorming → Fraud Prevention:** Regression coefficient = 0.934, significance < 0.05 , demonstrating that collaborative brainstorming improves risk identification and preventive actions.

D. Moderated Regression Analysis (MRA)

The competence of the three lines of defense—defined as knowledge, problem-solving skills, intrinsic motivation, and collaboration—was tested as a moderating variable. Results showed that competence did **not** significantly moderate the relationships between digital security, compliance management systems, fraud brainstorming, and fraud prevention. This suggests that while competence is

operationally important, it does not strengthen the predictive power of these variables in the tested model. Fraud prevention effectiveness in banking institutions appears to rely more heavily on systemic integration, regulatory enforcement, and structured collaboration rather than on individual skill levels alone.

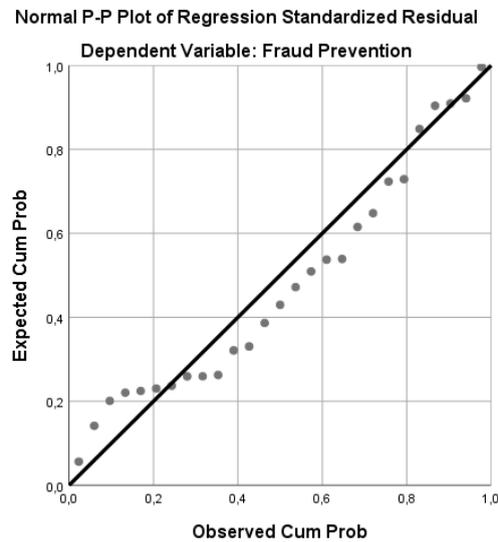


Figure 1. Normal P-P Plot of Regression Standardized Residual
Source: Data processed in 2025

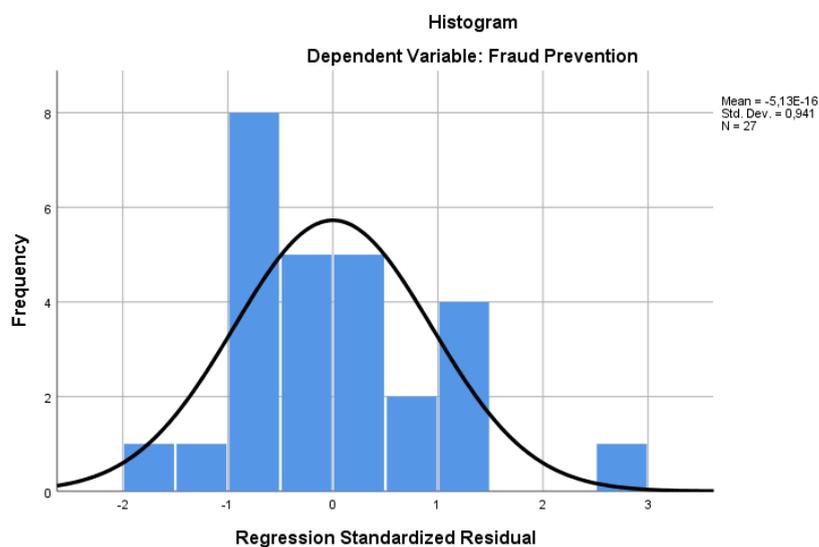


Figure 2. Histogram
Source: Data processed in 2025

DISCUSSION

A. Digital Security

The significant role of digital security aligns with game theory, emphasizing the need for banks to adapt continuously to evolving fraudster tactics. Security mechanisms such as encryption, authentication, and disaster recovery support the CIA triad confidentiality, integrity, and availability. This finding is consistent with previous research highlighting digital security as a determinant in reducing card-not-present fraud.

B. Compliance Management System (CMS)

The positive influence of CMS supports signaling theory, where strong compliance practices communicate integrity and accountability to stakeholders. Effective oversight and systematic monitoring contribute to preventing fraudulent activities, in line with past studies such as Quick & Sayar (2020) and Coglianesse & Nash (2018).

C. Fraud Brainstorming

Fraud brainstorming significantly enhances the accuracy of fraud risk assessments. Consistent with social judgment theory, collaborative discussions across the three lines of defense integrate diverse perspectives, enabling better anticipation of fraud schemes. Previous studies (Carpenter et al., 2006; Nassir et al., 2015) similarly support the value of brainstorming in improving fraud detection.

This finding is consistent with Carpenter (2007) and Carpenter et al. (2011), who demonstrate that structured fraud brainstorming enhances fraud risk identification and improves the quality of fraud-related judgments through collective professional reasoning.

D. Competence of the Three Lines of Defense

Despite theoretical expectations, competence did not strengthen the relationships among the independent variables and fraud prevention. While literature indicates that knowledge and skills improve fraud control, standardized procedures within banking may limit the impact of individual differences. Therefore, competence remains essential for operational quality but is not a moderating factor in the structural model.

E. SDG Contribution

- Improvements in fraud prevention directly support **SDG 16** by promoting stronger governance, transparency, and institutional resilience.
- The use of secure and innovative digital systems aligns with **SDG 9**, reinforcing the importance of technological innovation and robust financial infrastructure.

CONCLUSION

- Fraud prevention in Indonesia's banking credit card sector is significantly influenced by digital security, compliance management systems, and fraud brainstorming activities. These three factors play a crucial role in reducing fraud risk by strengthening technological defenses, regulatory adherence, and collaborative risk identification. However, the competence of the three lines of defense does not moderate these relationships, indicating that system integration,

institutional procedures, and structured controls have a stronger impact on fraud prevention than individual skill levels alone.

- The findings contribute to broader sustainability goals by supporting **SDG 16**, through strengthened transparency, accountability, and institutional integrity, and **SDG 9**, through enhanced digital innovation and secure financial infrastructure. Together, these results emphasize the importance of integrating technology, compliance culture, and collaborative practices to achieve sustainable and resilient fraud prevention in the banking industry.

Managerial Implications

1. **Strengthen Digital Security (SDG 9)**Banks should continuously upgrade digital security systems—including authentication, encryption, and recovery controls—to enhance cyber resilience and support sustainable technological innovation.
2. **Institutionalize Compliance Culture (SDG 16)**Strong leadership, systematic monitoring, and consistent policy enforcement are essential to embed a robust compliance culture that promotes transparency and institutional trust.
3. **Embed Fraud Brainstorming Practices**Fraud brainstorming should be conducted regularly across the three lines of defense to improve fraud risk identification, encourage cross-unit collaboration, and build future-oriented, sustainable fraud prevention frameworks.

REFERENCES

- Ajzen, Icek. (1991). The theory of planned behavior. *Organizational Behavior and Human Decision Processes*, 50(2), 179-211. doi: 10.1016/0749-5978(91)90020-t
- Arens, A. (2016). *Auditing and assurance services*. 15th Edition. New York: Pearson Publishing.
- Armitage, C.J., & Conner, M. (2001). Efficacy of the theory of planned behavior: A meta-analytic review. *British Journal of Social Psychology*, 40(4), 471-499. doi: [10.1348/014466601164939](https://doi.org/10.1348/014466601164939).
- Arthur, J.B., & Huntley, C.L. (2005). Ramping up the organizational learning curve: Assessing the impact of deliberate learning on organizational performance under gainsharing. *Academy of Management Journal*, 48(6), 1159-1170. doi: 10.5465/amj.2005.19573115
- Ashton, A. H. (1985). Does consensus imply accuracy in accounting studies of decision making? *The Accounting Review*, 60(185), 173-185. doi:10.1016/0169-2070(86)90095-6
- Association of Certified Fraud Examiners. (2012). *Report to the nations on occupational fraud and abuse*, Japan: Asia Pacific Edition, <http://www.acfe.com/rtnn>.
- Association of Certified Fraud Examiners. (2017). *Survei fraud Indonesia 2016*. Jakarta: ACFE Indonesia Chapter.
- Association of Certified Fraud Examiners. (2018). *Report to the nations: 2018 global study on occupational fraud and abuse*. Japan: Asia Pacific Edition.
- Association of Certified Fraud Examiners. (2019). *Survei fraud Indonesia 2019*. Jakarta: ACFE Indonesia Chapter
- Bank Indonesia. (2015). *SE implementasi standar nasional teknologi chip dan penggunaan pin untuk kartu yang diterbitkan di Indonesia*. Indonesia: Bank Indonesia.

- Beasley, M.S., & Jenkins, J.G. (2003). *A primer for brainstorming fraud risks*. Journal of Accountancy. Accessed from: <https://www.aicpa.org/PUBS/jofa/dec2003/beasley.htm>
- Becker, G.S. (1974). *Crime and punishment: an economic approach*. Chicago: National Bureau of Economic. doi: 10.1016/S0002-9610(56)80126-8
- Bonner, S.E., & Lewis, B.L. (1990). Determinants of auditor expertise. *Journal of Accounting Research*, 28, 1-20.
- Boritz, E.J. (2015). Are fraud specialist relatively more effective than auditors at modifying audit programs in the presence of fraud risk?. *The Accounting Review of American Accounting Association*, 90(3), 881-915. doi: 10.2308/accr-50911
- Borthick, A. F., Curtis, M. B., & Sriram, R. S. (2006). Accelerating the acquisition of knowledge structure to improve performance in internal control reviews. *Accounting, Organizations and Society*, 31(4), 323-342. doi: 10.1016/j.aos.2005.12.001
- Bragg, S.M. (2014). *Accounting control, best practices*. 4th Edition. Colorado: Wiley Press.
- Brazel, J.F., Carpenter, T.D., & Jenkins, J.G. (2010). Auditors' use of brainstorming in the consideration of fraud: reports from the field. *The Accounting Review*, 85(4), 1273-1301. doi: 10.2308/accr.2010.85.4.1273
- Carpenter, T. D. (2007). Audit team brainstorming, fraud risk identification, and fraud risk assessment: Implications of SAS No. 99. *The Accounting Review*, 82(5), 1119–1140. <https://doi.org/10.2308/accr.2007.82.5.1119>
- Carpenter, T. D., Durtschi, C., & Gaynor, L. M. (2011). The incremental benefits of audit brainstorming in fraud risk assessment. *Journal of Accounting Research*, 49(3), 647–673. <https://doi.org/10.1111/j.1475-679X.2011.00401.x>
- Carpenter, T. D., Reimers, J. L., & Fretwell, P. (2011). Internal auditors' fraud risk assessment: The role of professional skepticism and audit experience. *Auditing: A Journal of Practice & Theory*, 30(3), 45–69. <https://doi.org/10.2308/ajpt-10137>
- Coglianesi, C., & Nash, J. (2018). *Achieving compliance: Tools and strategies*. Brookings Institution Press.
- Donaldson, L., & Davis, J. H. (1991). Stewardship theory or agency theory: CEO governance and shareholder returns. *Australian Journal of Management*, 16(1), 49–64.
- Jensen, M. C., & Meckling, W. H. (1976). Theory of the firm: Managerial behavior, agency costs and ownership structure. *Journal of Financial Economics*, 3(4), 305–360.
- Neumann, J. von, & Morgenstern, O. (1944). *Theory of games and economic behavior*. Princeton University Press.
- Popoola, O. M. J., Che-Ahmad, A., & Samsudin, R. S. (2016). An empirical investigation of fraud risk assessment and knowledge requirement on fraud related problem representation in Nigeria. *Accounting Research Journal*, 29(1), 1–20.
- Quick, R., & Sayar, A. (2020). Compliance management systems: A conceptual framework and empirical insights. *Journal of Business Compliance*, 3(2), 45–60.
- Sherif, C. W., Sherif, M., & Hovland, C. I. (1980). *Social judgment: Assimilation and contrast effects in communication and attitude change*. Yale University Press.
- United Nations. (2015). *Transforming our world: The 2030 agenda for sustainable development*. United Nations.