“Factors influencing the effectiveness of credit card fraud prevention in Indonesian issuing banks”

AUTHORS	Yuli Dewi Harry Suharman Poppy Sofia Koeswayo Nanny Dewi Tanzil
ARTICLE INFO	Yuli Dewi, Harry Suharman, Poppy Sofia Koeswayo and Nanny Dewi Tanzil (2023). Factors influencing the effectiveness of credit card fraud prevention in Indonesian issuing banks. *Banks and Bank Systems*, *18*(4), 44-60. doi:10.21511/bbs.18(4).2023.05
DOI	http://dx.doi.org/10.21511/bbs.18(4).2023.05
RELEASED ON	Friday, 13 October 2023
RECEIVED ON	Friday, 04 August 2023
ACCEPTED ON	Friday, 22 September 2023
LICENSE	This work is licensed under a Creative Commons Attribution 4.0 International License
JOURNAL	"Banks and Bank Systems"
ISSN PRINT	1816-7403
ISSN ONLINE	1991-7074
PUBLISHER	LLC “Consulting Publishing Company “Business Perspectives”
FOUNDER	LLC “Consulting Publishing Company “Business Perspectives”

NUMBER OF REFERENCES	NUMBER OF FIGURES	NUMBER OF TABLES
52	0	8

BUSINESS PERSPECTIVES

LLC "CPC "Business Perspectives"
Hryhorii Skovoroda lane, 10,
Sumy, 40022, Ukraine
www.businessperspectives.org

Yuli Dewi (Indonesia), **Harry Suharman** (Indonesia), **Poppy Sofia Koeswayo** (Indonesia), **Nanny Dewi Tanzil** (Indonesia)

FACTORS INFLUENCING THE EFFECTIVENESS OF CREDIT CARD FRAUD PREVENTION IN INDONESIAN ISSUING BANKS

Received on: 4th of August, 2023
Accepted on: 22nd of September, 2023
Published on: 13th of October, 2023

Yuli Dewi, Doctoral Candidate, Faculty of Economics and Business (Accounting), Accounting Science Doctoral Study Program Department, Padjadjaran University, Indonesia. (Corresponding author)

Harry Suharman, Doctor, Head of Accounting Science Doctoral Study Programme; Lecturer, Faculty of Economics and Business, Padjadjaran University, Indonesia.

Poppy Sofia Koeswayo, Doctor, Lecturer, Faculty of Economics and Business, Padjadjaran University, Indonesia.

Nanny Dewi Tanzil, Doctor, Lecturer, Faculty of Economics and Business, Padjadjaran University, Indonesia.

Abstract

The increase in online credit card transactions in the digital era has caused an increase in credit card cyber incidents. This is happening globally, including in Indonesia. Thus, it will affect a bank's reputation as well as its financial losses. Therefore, optimal fraud risk management is needed in a banking effort to prevent credit card fraud. In response, this article intended to study credit card fraud prevention by examining the relationship between digital security required for customer data security; fraud brainstorming to identify process weaknesses; and compliance management to manage regulatory compliance. The next step was to test whether the anti-fraud specialist is competent to moderate this relationship. This study used a quantitative approach. This study included 27 Indonesian card issuers. Primary sources were used to collect data for this study. The primary data were analyzed using a structural equation model (SEM). The results of the study show that digital security, fraud brainstorming, and compliance management were positively and significantly related to the prevention of credit card fraud, at a significance level of 5%, the t-statistic has a numerical value of 6.161, 5.079, and 5.98 each. Furthermore, testing the moderating effect obtained t-statistic values of 7.330, 4.161, and 7.694. Competency results obtained with positive and significant influence moderate the relationship between these factors and credit card fraud prevention. These findings have policy implications for banking and government objectives in fighting credit card fraud through implementing prevention strategies.

Keywords banking sector, credit card, fraud management, cybercrime, security

JEL Classification G20, G21

Conflict of interest statement:
Author(s) reported no conflict of interest

INTRODUCTION

According to FST Media (2016) in the Economics of Fraud Survey, Indonesia has a high rate of credit card fraud due to its high online banking activity. As a country in Asia Pacific, Indonesia ranks 4.6 out of 5, where 5 is the worst. Indonesia is at high risk of credit card fraud by 86%, China by 70%, and Malaysia by 65%. Based on the AKKI (Indonesian Credit Card Association) report, banks in Indonesia suffered losses due to credit card fraud in 2007, reaching around IDR 70 billion. Similarly, 14 members of the EDC data breaching syndicate were arrested in 2011 for stealing up to 81 billion IDR from customer credit card balances.

In dealing with cybercrimes including credit card fraud, a strong information security management system is needed, which is built on three pillars: people, process, and technology. The condition that is happening in Indonesia is that currently Indonesia still needs 10 thousand cybersecurity experts through optimizing existing resources, including in the banking world, to anticipate carding attacks that continue to increase in Indonesia. Internal auditors, compliance func-

http://dx.doi.org/10.21511/bbs.18(4).2023.05

tions, and risk management as competent specialists are expected to have CFE or CISA qualifications and understand digital and cybersecurity, to combat technology-based fraud including carding. The aim is to oversight, assess the effectiveness of the anti-fraud program, and report the effectiveness of risk management to the Board of Directors, considering that cyberattacks in carding are very high and involve a lot of losses related to data security (ITG.ID, 2019).

From the Indonesian Cyber and Crypto Security Technology department, it was stated that in dealing with the rise of carding as a form of cybercrime, the concept of cyber development is needed, where the forming element is the development of specialist competencies, in addition to process and technology. In fulfilling specialist competencies to handle card security; cybersecurity literacy, workshops and knowledge sharing or brainstorming, fraud examiner certification, digital security for cyber incidents and awareness related to personal data protection, are required. In Indonesian banking practice, categorizing and identifying the risks of credit card fraud is not an easy thing to do, considering the complexity and dynamics of credit card fraud schemes. Lack of reliability and accuracy of data, as well as an understanding of providing categories and calculating losses, can lead to different interpretations in assessing the risk of credit card fraud in the banking industry. Likewise, digital security in banking in Indonesia is still considered weak, such as in dealing with identity theft from credit card customers or carding, where the mode is increasingly sophisticated. In addition, various bank fraud cases including carding were also acknowledged by Bank Indonesia to occur due to weak internal controls and compliance management, so banks need to rearrange internal controls by optimizing fraud risk management. Therefore, how to improve digital security, strengthen compliance management, fraud brainstorming and anti-fraud specialist competencies are important issues for issuer banks in Indonesia that must be anticipated to prevent credit card fraud from continuing to increase.

1. LITERATURE REVIEW AND THE HYPOTHESES

The emergence of various forms of cybercrime, especially carding, which involves credit card transactions, in the digital era is a negative side of the development of society and the fact is that crime is always developing, along with the development of society (Sidoti & Devasagayam, 2010). Because of that, along with the emergence of cybercrime, efforts to prevent and deal with it are important issues (Lee, 2019).

The development of a digital society (digital society), which has high expectations for a perfect customer experience, the availability of good infrastructure, demands effective service and protection of sensitive data, namely customer data. Digital security is needed to protect customer assets as valuable assets in cyberspace. This asset refers to company resources, which will face cyber threats and then need protection from these cyber threats (Badadare et al., 2018). For this reason, a digital security system that is managed properly is needed well, including in tackling credit card fraud.

Digital security itself, specifically in the banking business, is considered very important, because banks provide services through digital technology, such as e-banking, sms banking or m-banking. This is what can make bank data or customer data open to attacks by hackers who will steal these data. Because of this it is very important to carry out security strategies in the banking world such as data encryption, cooperate with a team of experts in the field of cybersecurity or create cybersecurity training for employees, including for internal auditors, so that they can carry out their function as continuous assurance in cybersecurity to determine the cybersecurity method that will be implemented. (No & Vasarhelyi, 2017; Al-Alawi & Al-Bassam, 2019).

Previous studies explained that the development of information technology brings benefits as well as risks of fraud related to information technology. The widespread use of technology has led to the rise of cybercrime in the banking sector (Quick & Sayar, 2021; Sekhar & Kumar, 2023). Banking is an industry that experiences the highest cybercrime. Therefore, it is necessary to apply digital or cybersecurity with various mechanisms to deal with fraud threats. Digital security frameworks can be used to analyze and identify cyber threats such as data theft or malware attacks. In addition, Goztepe (2012) explains that digital security provides information security with technological solutions that can automatically assist in fraud prevention and detection. Rule-based expert system employing fuzzy rules (FRBCES) is a digital security that utilizes artificial intelligence using algorithm code to execute fraud prevention mechanisms. Today's fraud prevention methods are no longer manual but automated to monitor the high volume of information and transaction data.

Past studies argue that increased customer interaction in digital transactions makes compliance management necessary to anticipate the development of fraud. It is proven that companies that use comprehensive compliance management can reduce compliance violations or fraud. Companies that use compliance management to ensure compliance with rules through certain system mechanisms must be supported by senior leaders to reduce fraud (Coglianese & Nash, 2021). Another study also suggests that a certain system, namely an automated knowledge-based compliance management system, is needed to overcome the limitations of special personnel in studying the rules that become standard compliance in companies, including anti-fraud compliance (S. Kim & Y. Kim, 2017).

Several previous researchers found that fraud brainstorming has an influence on fraud risk assessment as an effort to prevent fraud (Carpenter, 2007; Mohd-Nassir et al., 2016). Brainstorming will improve the accuracy of judgments in assessing fraud risk to prevent fraud. In addition, a study by Dewi et al. (2023) explains that the fraud risk management team using the brainstorming method can provide a more accurate credit card fraud risk assessment as an effort to prevent fraud, especially in terms of its causes. fraud and the impact of credit card fraud. Fraud brainstorming helps to discuss the emergence of fraud, detail fraud, and think like a fraudster so that you can find strategies to prevent and anticipate fraud. Talamantes (2020) further shows that knowledge sharing between anti-fraud specialists is very important. This is because cybercriminals will find data and software vulnerabilities that are used at any time, including in the banking industry. Therefore, experts must share information to face challenges and determine reactions to potential cybercrime threats such as carding related (Viswanathan et al., 2005).

The competence of specialists who control anti-fraud banks can strengthen the link between digital security, compliance management, and fraud brainstorming on fraud prevention efforts, including credit card fraud. Pearson and Singleton (2008) explain that digital or cybersecurity in dealing with cybercrime can be carried out if experts with competence and certification in the field of fraud examiners and digital forensics, both forensic accounting and forensic auditing, support it. According to previous studies, the use of compliance management with strong competency support in the form of knowledge of compliance, legislation, and skills to analyze past behavior, which can be a predictor of possible future fraud risk, is necessary to address the growing complexity of fraud (Remmerbach & Krumme, 2020). Further research has examined, fraud brainstorming which is strengthened by competence (interpersonal skills) will affect the success of fraud prevention (B. Schafer & J. Schafer, 2019)

Subjects related to credit card fraud prevention factors in particular and cybercrime in general, in previous studies also included several variables as determining factors, such as anti-fraud IT technology, law enforcement, attitude awareness, and ethics (Riley, 2007; Obuh & Babatope, 2011; Othman et al., 2015; Kathirvel, 2013). Within the scope of technology for credit card fraud prevention, Singh and Jain (2019) also suggest that CCFPD (Credit Card Fraud Prevention and Detection) can be used as a framework for preventing and detecting credit card fraud at the application level and credit card transaction level. Likewise, Laurens and Zou (2016) argue that Dynamic Soft Descriptor merchants can confirm whether the cardholder is an official who conducts online transactions.

Various theories explain the application of factors that can make cybercrime fraud prevention such as carding more effective. Fraud prevention efforts are important because according to Dell'Ariccia (2001), based on agency theory from Jensen and Meckling (1976), it is very important to make fraud prevention efforts, because fraud can reduce profits and company reputation. Another example of theory is Donaldson and Davis' theory (1991) which helps explain the relationship between principals (shareholders) and stewards. This theory explains that the agent as a steward believes that personal needs will also be fulfilled by themselves by fulfilling the principal's interests for the progress of the company. This can be achieved because the agent has good competence.

Another theory is that put forward by Neumann and Morgenstern. This theory consists of rules that create competitive situations to maximize one's winnings. Game theory is defined as a study model of conflict and cooperation among rational decision makers, where this technique is used to analyze situations in which two or more people make decisions that may affect their well-being (Myerson, 2002). Banks can use this game theory to explain that digital security uses analysis where fraud perpetrators will choose a certain level of fraud (Vatsa et al., 2007), and vice versa, banks will also create certain security systems that can compensate for fraudster strategies in committing fraud.

Another factor, namely compliance management, can also be explained by signaling theory. This theory is to explain the existence of a condition when two parties (individuals and companies) have access to different information. The sender or giver of the signal will choose what and how to communicate information, and the receiver will choose how to interpret the signal (Connelly et al., 2011). Signaling theory can be related to the importance of compliance management in the banking system.

The brainstorming fraud factor can be explained by Social Judgment theory. An individual's attitude towards a particular issue results from a process of consideration that occurs within them towards the issue at hand (Hovland & Sherif, 1980). In general, it can be explained that knowing someone's motivation to do carding in taking a fraud prevention strategy is very important. Several factors that cause the possibility of external and internal bank actors committing crimes are pressure, opportunity, rationalization, ability, arrogance, and collusion. Collusion between the two parties to commit fraud on third parties can cause changes in employee culture and behavior from honest to dishonest (Vousinas, 2019).

For this reason, this study tries to broaden the scope by integrating all variables related to people, process and technology, to handle carding related credit card transactions. Based on the various opinions above, this study tries to analyze whether factors such as digital security, fraud brainstorming, compliance management, competency of anti-fraud specialists can influence the effectiveness of credit card fraud prevention. Therefore, the hypotheses are as follows:

H1: *Digital security has a positive effect on credit card fraud prevention.*

H2: *Compliance management has a positive effect on credit card fraud prevention.*

H3: *Fraud brainstorming has a positive effect on credit card fraud prevention.*

H4: *Competence of an anti-fraud specialist has a positive effect as a moderator of the relationship between digital security and credit card fraud prevention.*

H5: *Competence of an anti-fraud specialist has a positive effect as a moderator of the relationship between compliance management and credit card fraud prevention.*

H6: *Competence of an anti-fraud specialist has a positive effect as a moderator of the relationship between fraud brainstorming and credit card fraud prevention.*

2. RESEARCH METHODOLOGY

This study used a quantitative design with descriptive research methods to describe phenomena according to the identified variables. It was designed to provide systematic information. The researchers decided to use a survey because it is the most widely used and effective strategic tool in economic and business research (Sekaran & Bougie, 2016). Surveys are also a tool for collecting quantitative data in an effective and systematic way so as to run statistical tests and obtain generalizable results (Bryman, 2016).

This research sample was taken based on the non-probability sampling method through total quota sampling, namely sampling, with the entire population from the unit of analysis determined by the researcher. The unit of analysis or members of this research population are 27 credit card issuing banks in Indonesia with the observation units being banking committee members that supervise anti-fraud controls. They supervise a Risk Management, Compliance, and Internal Audit Unit in the Credit Card Business. Because it involved the practice of implementing fraud prevention at each bank, the identities and responses given by respondents through this questionnaire were kept confidential. 63 questionnaire questions were analyzed to determine research findings. The respondents recorded the implementation of digital security practices, fraud brainstorming sessions, compliance management and competence of anti-fraud control units at their respective banks. Participants were also asked to provide details regarding position in the company, participation in anti-fraud training and ownership of Fraud Examiner Certificates.

In filling out this research survey, all 215 respondents were asked to provide answers in the form of levels of approval and disapproval of questions on a Likert response scale consisting of 5 points, namely with a score range of 5 for strongly agree, to a score of 1 for strongly disagree.

Furthermore, as a method of analysis, the Structural Equation Model-Partial Least Square (SEM-PLS) method is used. SEM is used in this study to build the initial model with the variables tested. As for this study, the variables discussed will be divided into several dimension categories where each dimension is measured by indicators. The variables in this study are:

1) Competence of anti-fraud specialist;
2) Digital Security;
3) Compliance Management;
4) Fraud Brainstorming;
5) Credit Card Fraud Prevention.

In the analysis of data testing using SEM (Structural Equation Modeling) and SMARTPLS (Partial Least Square), there are two types of models which are a measurement model (outer model) and a structural model (inner model). The measurement model explains the proportion of variance of each manifest variable or indicator that can be explained in the latent variable. Each latent variable will then describe a structural model that examines the effect of each exogenous latent variable on the endogenous latent variable (Hair et al., 2019). Next, the steps for testing the data are written as follows:

2.0.1. Outer model analysis or measurement model

Validity test (convergent validity and discriminant validity). For convergent validity, according to Hair et al. (2019) and Ghozali (2014), most of the reference factor loadings of 0.50 or more (≥ 0.50) are considered to have strong enough validity to explain latent constructs. Discriminant Validity is comparing the AVE (square root of Average Variance Extracted) value of each construct, with the correlation between the construct and other constructs (Ghozali, 2008). *Reliability test* (composite reliability and Cronbach's alpha). It is reliable if the composite reliability value is ≥ 0.7 (Ghozali, 2014, p. 43). Otherwise, it is unreliable if it is < 0.7. For the Cronbach's Alpha test, the value suggested in is > 0.6, generally.

2.0.2. Inner model analysis or structural model

R-square test is used to define the variance in the endogenous variable explained by the exogenous variable(s). R-square is for endogenous constructs, path coefficient values or t-values for each path to test the significance between constructs in structural models (Abdillah & Jogiyanto, 2009, p. 62).

Goodness of Fit (GoF) values between 0.1 and 0.25 have a small category, values between 0.25 and 0.0.36 have a moderate category, and values more than 0.36 have a large category (Hair et al., 2019).

2.0.3. Hypothesis test

The criteria for testing the hypothesis in this study is a significance level (α) of 5% and is determined by the following criteria:

- the hypothesis is accepted if t-test > t-table (1.96);

http://dx.doi.org/10.21511/bbs.18(4).2023.05

- the hypothesis is rejected if t-test < t-table (1.96).

The P-value can also determine the hypothesis test, with these criteria:

- the hypothesis is accepted if P-value < 0.05;
- the hypothesis is rejected if P-value > 0.05.

2.0.4. Conversion to the equation system

The path diagram conversion can be explained in the equation as follows:

$$Y = \beta_1 X_1 + \beta_2 X_2 + \beta_3 X_3 + \beta_4 \cdot Z + \\ + \beta_5 X_1 \cdot Z + \beta_6 X_2 \cdot Z + \beta_7 X_3 \cdot Z + \zeta_1, \qquad (1)$$

where Y = Credit Card Fraud Prevention; X_1 = Digital Security; X_2 = Compliance Management; X_3 = Fraud Brainstorming; Z = Competence; β_1 = Digital Security path coefficient to Credit Card Fraud Prevention; β_2 = Path coefficient of compliance management to Credit Card Fraud Prevention; β_3 = Coefficient of the Fraud Brainstorming Path to Credit Card Fraud Prevention; β_4 = Competency path coefficient for Credit Card Fraud Prevention; β_5 = Digital Security path coefficient moderated by Competence; β_6 = Compliance Management path coefficient moderated by Competence; β_7 = Fraud Brainstorming path coefficient with moderation by Competence; and ζ_1 = other factors' influence.

3. RESEARCH RESULTS

In demographic survey, the results showed that there were 50 people (23%) in the Compliance Unit Supervision, 99 people (46%) in the Risk Management Unit Supervision, and 66 people (31%) in the Internal Audit Unit Supervision. There were 96 (45%) males and 119 (55%) females, of which 177 people (82%) were graduates, 23 people (11%) were postgraduates, and 15 people (7%) had diplomas degrees. Related to the age of the respondents, 45 people (21%) were under the age of 30, 104 people (48%) were between the ages of 31 and 40, 66 people (31%) were over the age of 40.

The next was validity test as a stage of the outer model analysis (see Table 1).

Table 1 showed the convergent validity test after reduction. It can be seen from the loading factor values and average variance extracted (AVE). And after reducing some of the lowest indicators (X3.2.2, Y.3.3, Y.4.3, Y.4.4, Y.4.6), all remaining indicators are tested and declared valid since they have a loading factor greater than 0.5. Some of these indicators were not used because they were considered less representative in explaining the factors that make credit card fraud prevention more effective.

Cronbach's Alpha and Composite Reliability (CR) are performed to test construct reliability. Thus, it will be seen that all indicators are reliable and

Table 1. Convergent validity test

Variable	Dimension	Indicator	Loading Factor	AVE
Digital Security (X1)	Confidentiality data security (X1.1)	Authentication mechanism (X1.1.1)	0.852	0.74
		Proper password (X1.1.2)	0.874	
		Cybersecurity training (X1.1.3)	0.856	
	Integrity data security (X1.2)	Data encryption (X1.2.1)	0.912	0.838
		Access control (X1.2.2)	0.919	
	Availability data security (X1.3)	System patching regularly (X1.3.1)	0.937	0.866
		Comprehensive disaster recovery plan (X1.3.2)	0.924	
Compliance Management System (X2)	Oversight of the board of directors and management (X2.1)	Oversight and commitment (X2.1.1)	0.721	0.644
		Change Management (X2.1.2)	0.840	
		Comprehension, identification, and risk management (X2.1.3)	0.823	
		Self-identification and corrective action (X2.1.4)	0.821	
	Compliance program (X2.2)	Policies and procedures (X2.2.1)	0.806	0.684
		Compliance training (X2.2.2)	0.818	
		Compliance monitoring and audit (X2.2.3)	0.861	
		Consumer complaint response (X2.2.4)	0.821	

Table 1 (cont.). Convergent validity test

Variable	Dimension	Indicator	Loading Factor	AVE
Fraud Brainstorming (X3)	Assembling the right people (X3.1)	Engagement of all participating team members (X3.1.1)	0.850	0.676
		Team contribution (X3.1.2)	0.794	
	Assessing the process (X3.2)	Process Issues (X3.2.1)	0.856	0.742
		Manual vs automated system (X3.2.3)	0.859	
		New system vs legacy system (X3.2.4)	0.869	
	Assessing the players (X3.3)	Employee background (X3.3.1)	0.859	0.796
		Employee authority (X3.3.2)	0.923	
		Working period (X3.3.3)	0.894	
	Assessing the data (X3.4)	Manual data (X3.4.1)	0.872	0.776
		Automated Data (X3.4.2)	0.889	
	Assessing the environment (X3.5)	Assessment of the workplace (X3.5.1)	0.936	0.877
		Assessment of the environment pressure (X3.5.2)	0.937	
	Developing fraud schemes (X3.6)	Development of detailed business processes (X3.6.1)	0.751	0.655
		Possibility of collusion (X3.6.2)	0.864	
	Developing procedures of control based on identified fraud schemes (X3.7)	Procedures for preventive control (X3.7.1)	0.839	0.694
		Procedure for detective control (X3.7.2)	0.827	
	Developing fraud triggers (X3.8)	Unusual Transaction (X3.8.1)	0.914	0.753
		Inconsistency of customer data information (X3.8.2)	0.819	
Fraud Prevention (Y)	Tone at the top (Y.1)	Leading by example (Y.1.1)	0.892	0.833
		Creating a culture of integrity (Y.1.2)	0.933	
	Streamlining employee on-boarding process (Y.2)	Verification of prospective new employees (Y.2.1)	0.922	0.833
		Verification of promoted employees (Y.2.2)	0.904	
	Continuous anti-fraud training and awareness campaigns (Y.3)	Awareness of the importance of fraud prevention (Y.3.1)	0.916	0.847
		Employee training related to red flags (Y.3.2)	0.934	
	Entrenchment of Sound Internal Control Systems (Y.4)	Surprise audit; (Y.4.1)	0.805	0.660
		Physical security of assets (Y.4.2)	0.852	
		Multi-level authorization (Y.4.5)	0.778	
	Creating and Sustaining an Anti-Fraud Reporting Mechanism (Y.5)	Reporting through the media whistleblowing system by management (Y.5.1)	0.954	0.906
		Protection and reward to the whistleblower (Y.5.2)	0.961	
		Parties Managing Complaints (Y.5.3)	0.943	
	Use of artificial intelligence techniques (Y.6)	Anomaly detection of transaction (Y.6.1)	0.981	0.962
		Monitoring customer behavior in transactions (Y.6.2)	0.981	
Competence (Z)	Knowledge (Z.1)	General knowledge (Z.1.1)	0.905	0.816
		Task-specific knowledge (Z.1.2)	0.901	
	Skill (Z.2)	Communication skill (Z.2.1)	0.894	0.785
		Problem solving skill (Z.2.2)	0.866	
		Task uncertainty skill (Z.2.3)	0.898	
	Intrinsic motivation (Z.3)	Mastery (Z.3.1)	0.866	0.763
		Autonomy (Z.3.2)	0.886	
		Purpose (Z.3.3)	0.869	
	Collaborative mindset (Z.4)	"We" focus behavior (Z.4.1)	0.846	0.799
		Sharing information (Z.4.2)	0.947	
		Communication (Z.4.3)	0.885	

consistently measure their respective variables. This test is useful for the various factors influencing credit card fraud prevention at Indonesian issuing banks.

Table 2 above shows that all research variables have CR values greater than 0.7 and Cornbach's Alpha values greater than 0.6.

http://dx.doi.org/10.21511/bbs.18(4).2023.05

Table 2. Reliability test

Variable	Cronbach's Alpha	Composite Reliability (CR)
X1	0.919	0.935
X1.1	0.825	0.895
X1.2	0.807	0.912
X1.3	0.846	0.928
X2	0.911	0.928
X2.1	0.815	0.878
X2.2	0.846	0.896
X3	0.934	0.943
X3.1	0.673	0.807
X3.2	0.826	0.896
X3.3	0.872	0.921
X3.4	0.712	0.874
X3.5	0.860	0.935
X3.6	0.631	0.791
X3.7	0.659	0.819
X3.8	0.680	0.859
Y	0.815	0.774
Y.1	0.802	0.908
Y.2	0.800	0.909
Y.3	0.820	0.917
Y.4	0.744	0.853
Y.5	0.948	0.967
Y.6	0.960	0.981
Z	0.944	0.952
Z.1	0.774	0.899
Z.2	0.863	0.917
Z.3	0.845	0.906
Z.4	0.873	0.922

The structural model test in this study was carried out with the R-square value. According to Ozili (2023), the R-Square Category is 0-0.09 = weak, 0.10-0.50 = moderate, and 0.51-0.99 = strong.

Table 3. R-square

Construct	R-Square	R-Square Adjusted	Information
X_1-Y	0.859	0.857	Strong
X_2-Y	0.818	0.817	Strong
X_3-Y	0.763	0.762	Strong
Z-Y	0.272	0.271	Moderate

Descriptive statistics indicate that the factors that influence the prevention of credit card fraud at the credit card issuing banks in Indonesia can be explained in various ways, starting with the factors with the highest results, namely digital security, compliance management, fraud brainstorming and the competence of anti-fraud specialists.

Moreover, the Goodness of Fit (GoF) was calculated for the model as follows:

$$GoF = \sqrt{\overline{AVE} \cdot \overline{R^2}} = \sqrt{0.723 \cdot 0.780} = 0.751. \quad (2)$$

Based on Hair's criteria, it was concluded that the research model formed was good (> 0.36), namely 0.751.

4. HYPOTHESIS TESTING

Hypothesis testing used 5,000 bootstrapped samples with a 95 percent confidence interval. The results of data processing and bootstrap in the SEM-PLS analysis show that the relationship hypothesized in the formal research model is statistically significant, because the p-value is less than 0.05, reaching the required level at 95% reliable. In other words, the hypothesis in the research model is accepted.

The results of the sample bootstrapping are presented below.

H1: Digital Security.

Based on Table 4, the t-statistics are greater than the t-table, namely 6.161 > 1.96 at a significance level = 5%. In addition, the p-value (0.017) < 0.05 means H_0 is rejected. Digital security significantly affects fraud prevention.

Table 4. Estimates based on the structural model

Hypothesis	Relationship	β value	Standard Deviation	T-statistics	P-values	T-table	Outcome
H_1	$X_1 \rightarrow Y$	0.727	0.118	6.161	0.017	1.96	Accepted
H_2	$X_2 \rightarrow Y$	0.701	0.138	5.079	0.027	1.96	Accepted
H_3	$X_3 \rightarrow Y$	0.600	0.100	5.980	0.00	1.96	Accepted
Bootstrap result for moderating effect							
Hypothesis	Relationship	β value	Standard Deviation	t-statistics	p-values	t-table	Outcome
H_4	$X_1 \cdot Z \rightarrow Y$	0.755	0.103	7.330	0.005	1.96	Accepted
H_5	$X_2 \cdot Z \rightarrow Y$	0.774	0.186	4.161	0.031	1.96	Accepted
H_6	$X_3 \cdot Z \rightarrow Y$	0.731	0.095	7.694	0.004	1.96	Accepted

Note: X_1 = digital security, X_2 = compliance management, X_3 = fraud brainstorming, Z = competence, Y = fraud prevention.

H2: Compliance Management.

Based on Table 4, the t-statistics value is greater than the t-table, namely 5.079 > 1.96 at a significance level = 5%. In addition, the p-value (0.027) < 0.05 then H_0 is rejected. The compliance management has a significant effect on fraud prevention.

H3: Fraud Brainstorming.

Based on Table 4, the value of the t-statistics is greater than the t-table, namely 5.98 > 1.96 at a significance level = 5%. In addition, the p-value (0.00) < 0.05 means that H_0 is rejected. Fraud brainstorming has a significant effect on fraud prevention.

H4: Digital Security was moderated by Competence of an anti-fraud specialist.

Based on Table 4, the t-statistics value is greater than the t-table, namely 7.330 > 1.96 at a significance level = 5%. In addition, the p-value (0.005) < 0.05 means that H_0 is rejected. Competence has a significant effect as a moderator of the relationship between digital security and fraud prevention.

H5: Compliance Management System was moderated by Competence of an anti-fraud specialist.

Based Table 4, the t-statistics value is greater than the t-table, namely 4.161 > 1.96 at a significance level = 5%. In addition, the p-value (0.031) <0.05 means that H_0 is rejected. Competence has a significant effect as a moderator of the relationship between compliance management on fraud prevention, or competence can strengthen the relationship between compliance management and credit card fraud prevention.

H6: Fraud Brainstorming was moderated by Competence of an anti-fraud specialist.

Based on Table 4, the t-statistical value is greater than the t-table, namely 7.694 > 1.96 at a significance level = 5%. In addition, the p-value (0.004) < 0.05 means that H_0 is rejected. It means that competence has a significant effect as a moderator of the relationship between fraud brainstorming and fraud prevention.

5. DISCUSSION

The next is the discussion to find out the estimation results of the statistical data processing with applicable theory and practice.

Hypothesis testing showed that digital security has a significant positive effect on credit card fraud prevention; the higher the digital security, the higher the credit card fraud prevention. So, this study is in accordance with research from Auchey (2020), maintaining digital security requires data analytics to prevent potential threats to technological systems. This is where agency theory becomes the basis for understanding the strategy of company management in maximizing the use of data analytics, both for the audit process and for fraud prevention, so as to reduce operational costs due to the impact of fraud losses that arise.

Shiva et al. (2010) explained that game theory is a potentially good solution for managing dynamic analytical mechanisms in digital or cybersecurity because, although there are advances in information technology in securing digital aspects (confidentiality, integrity, and availability of data security), they still cannot keep up with cybercrimes such as dynamic credit card data theft.

In practice, issuing banks in Indonesia need to improve data authentication mechanisms, as well as more continuous audits of system access. The entire digital security process must comply with the banking code of ethics, local guidelines, Information Security Management System (SMKI), and international (PCI DSS, NIST Framework). The SMKI uses SNI (Indonesia National Standard) and ISO/IEC 27001:2013 rules which are information security guidelines that explain the requirements for creating, implementing, analyzing, maintaining, and documenting information to keep it safe.

Currently, digital security governance in Indonesia is still partial, so the handling of cybersecurity issues is not yet integrated. This makes cyber threats even more real, such as data security in credit card businesses. For this reason, up-to-date IT Governance and a comprehensive GRC are needed to create awareness regarding best practices in cybersecurity to reduce the risk of cyber fraud.

http://dx.doi.org/10.21511/bbs.18(4).2023.05

Therefore, cybercrimes such as carding as a form of credit card fraud in cyberspace require preventative action. This preventive action is urgently needed because issuing banks in Indonesia are still lacking in protecting cardholders' personal data through their digital and cybersecurity, under the umbrella of the Personal Data Protection Law.

Based on the test results, it is known that the compliance management had a significant positive effect on fraud prevention and provided positive results. These results support the research hypothesis through empirical evidence that the better the compliance management, the better the fraud prevention. According to Holt et al. (2016), signaling theory is used as a basis for seeing whether there are detectable signals from actions that lead to fraud, by using compliance management. This is mainly performed by forensic accountants or auditors to catch indications of fraud, so that fraud can be prevented.

Survey results on issuing banks in Indonesia show that there is a need to improve a number of things, such as a culture of communication and compliance. Company ethics and legal requirements must be implemented, not just as an empty item on the checklist, but as a compliance culture in action. As explained in PBI 13/2/PBI/2011, compliance management functions to formulate strategies to encourage the creation of a culture of compliance, ensure systems, and company procedures comply with the law.

The survey results showed that fraud brainstorming had a significant positive effect on fraud prevention. According to Brazel et al. (2010), two or more auditors who interact with each other, either between auditors or with groups outside them, can influence the success of making fraud prevention policy formulations. Based on social judgment theory, it can support the success of fraud brainstorming in developing fraud prevention strategies.

From the survey results, fraud brainstorming has been carried out in issuing banks in Indonesia but is not continuous, especially in discussing the audit plan design. In practice, the brainstorming that has been carried out at this time is mostly carried out after the occurrence of fraud, which is based on cardholder reports. This causes an increase in the burden of reserves for losses as a bank risk expected loss due to fraud.

According to the empirical results obtained based on the survey, there are several dimensions that need improvement, namely fraud brainstorming related to assessing the environment, assessing data, assessing employees, and assessing the process. In line with previous research, there are weaknesses in the detailed discussion regarding the several dimensions above that can make banks less focused on strategic planning sessions to obtain ideas related to cyber risk mitigation (Hubs, 2012). Brainstorming is important, as explained in ISA 240, SAS No. 99, and SAS No. 82, which encourages auditors to conduct brainstorming with the involvement of various team members to analyze the potential for fraud.

According to Brazel et al. (2010), decision-making based on brainstorming in accordance with social judgment theory will provide better quality decisions compared to individual decisions. Carrying out the task of fraud risk assessment in the credit card business will make the resulting decisions even better because there is a process of sharing knowledge and experience related to credit card fraud prevention (Dewi et al., 2023).

The research results proved that the influence of digital security, compliance management, and fraud brainstorming on fraud prevention in the credit card business sector is strengthened by the competence of anti-fraud specialists, namely the 2nd and 3rd lines of banking such as risk management, compliance, and internal auditor teams. This means that digital security will have a stronger relationship with fraud prevention if it is supported by the competence of anti-fraud specialists. Competence here is competence in forensic accounting skills. This skill enables a specialist to gather evidence of fraud and present it clearly. Problem-solving skills in dealing with complex types of fraud. According to Hasham et al. (2019), a lack of competence in preventing cybercrime such as credit card fraud will have a negative impact on companies and increase money laundering crimes, which will threaten national security in general.

Using agency theory to ensure good IT governance between digital and cybersecurity, and fraud prevention, which is strengthened by competence, can help companies become more strategic (Posthumus & Solms, 2021). Other research has proven that in the security competency model developed by NICE (National Initiative for Cybersecurity Education) USA, the human factor is very crucial to strengthening cybersecurity to prevent fraud. A lack of competency can result in vulnerabilities in digital system security (E. Szczepaniuk & H. Szczepaniuk, 2022).

Digital security in Indonesia must be based on ISO 27001-2013, which is a ten-year-old framework, according to the Ministry of Communication and Information's directives. This makes hacking easier because security maturity should improve over time. Actually, there is already a digital security method as of 2022 but it hasn't started to be effectively implemented. In other words, the digital security strategy must be strengthened by the competence of the specialists.

Research results proved, the influence of compliance management on credit card fraud prevention is strengthened by competence. Quick and Sayar (2021) argue that a bank's compliance management can achieve its goal of systematically preventing and sanctioning violations of company regulations if the competence of its supporting specialists is strengthened. Based on agency theory, agents can take different actions from the goals set by the principals. This will have a bad impact on the company if the principal has poor skills to anticipate it. Specialist skills are needed to oversee optimal compliance management implementation.

Research results also proved that the effect of fraud brainstorming on fraud prevention is strengthened by the competence of anti-fraud specialists. Brainstorming can help anti-fraud specialists to identify the types of fraud based on the evidence gathered.

CONCLUSION

The findings of this study show that in preventing credit card fraud in Indonesian banks, factors such as digital security, compliance management, and fraud brainstorming are needed, which are strengthened by the competence of anti-fraud specialists. From the results of this study, it can be explained that the first factor is increasing digital security through data analytics security, which is useful for preventing potential threats to technology systems. The second is a compliance management to get to know customers, manage risks using a compliance dashboard, and organize multiple layers of defense to prevent carding. The third is fraud brainstorming which must be carried out regularly and with quality to help specialists improve the quality of fraud consideration. The success of making fraud prevention policy formulations can be affected by this interaction.

Improving digital security, compliance management, optimizing brainstorming, which is strengthened by the competence of anti-fraud specialists, are important things to maximize fraud prevention efforts in the credit card business in Indonesia. These competencies can be improved through professional training. The achievement of these conditions can have a significant impact on the proper management of fraud risk, including eradicating money laundering crimes in various modes, including through credit card fraud.

All the factors mentioned must be supported by strong competency factors from anti-fraud specialists. Competence can ensure good quality banking IT governance, strengthen the relationship between digital security and fraud prevention, overcome weaknesses in understanding local and international regulations related to payment card security standards, understand the use of big data, strengthen the effectiveness of knowledge sharing with specialists to realize optimal fraud prevention.

AUTHOR CONTRIBUTIONS

Conceptualization: Yuli Dewi, Harry Suharman, Poppy Sofia Koeswayo, Nanny Dewi Tanzil.
Data curation: Yuli Dewi, Harry Suharman, Poppy Sofia Koeswayo, Nanny Dewi Tanzil.
Formal analysis: Yuli Dewi, Harry Suharman, Poppy Sofia Koeswayo, Nanny Dewi Tanzil.
Investigation: Yuli Dewi, Harry Suharman, Poppy Sofia Koeswayo, Nanny Dewi Tanzil.
Methodology: Yuli Dewi, Harry Suharman, Poppy Sofia Koeswayo, Nanny Dewi Tanzil.
Project administration: Yuli Dewi, Harry Suharman, Poppy Sofia Koeswayo, Nanny Dewi Tanzil.
Resources: Yuli Dewi, Harry Suharman, Poppy Sofia Koeswayo, Nanny Dewi Tanzil.
Software: Yuli Dewi, Harry Suharman, Poppy Sofia Koeswayo, Nanny Dewi Tanzil.
Supervision: Yuli Dewi, Harry Suharman, Poppy Sofia Koeswayo, Nanny Dewi Tanzil.
Validation: Yuli Dewi, Harry Suharman, Poppy Sofia Koeswayo, Nanny Dewi Tanzil.
Visualization: Yuli Dewi, Harry Suharman, Poppy Sofia Koeswayo, Nanny Dewi Tanzil.
Writing – original draft: Yuli Dewi, Harry Suharman, Poppy Sofia Koeswayo, Nanny Dewi Tanzil.
Writing – reviewing & editing: Yuli Dewi, Harry Suharman, Poppy Sofia Koeswayo, Nanny Dewi Tanzil.

ACKNOWLEDGMENTS

This research was conducted as part of the process of study completion at the Padjadjaran University, Bandung, Indonesia. We would like to express our sincere gratitude to the respondents who participated in this research.

REFERENCES

1. Abdillah, W., & Jogiyanto. (2009). *Partial Least Square (PLS) Alternatif SEM.*
2. Al-Alawi, A. I., & Al-Bassam, S. A. (2019). Assessing the Factors of Cybersecurity Awareness in the Banking Sector. *Arab Gulf Journal of Scientific Research, 37*(4), 17-32. https://doi.org/10.51758/AGJSR-04-2019-0014
3. Auchey, D. (2020). Effective Data Analytics and Security Strategies in Internal Audit Organizations. *Walden Dissertation and Doctoral Studies,* 8838. Retrieved from https://scholarworks.waldenu.edu/dissertations/8838/
4. Badadare, V. L., Patil, R. Y., & Waghmare, V. (2018). Cybersecurity need of digital era: a review. *International Journal of Computer Applications, 182*(22), 9-12. Retrieved from https://www.ijcaonline.org/archives/volume182/number22/badadare-2018-ijca-918002.pdf
5. Bailey, K. (2017). *A Combined Wavelet and ARIMA Approach to Predicting Financial Time Series Ken Bailey* (Master's Thesis). Dublin City University. Retrieved from https://core.ac.uk/download/pdf/130141601.pdf
6. 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. https://doi.org/10.2308/accr.2010.85.4.1273
7. Bryman, A. (2016). *Social Research Methods* (5th ed.). The United States of America by Oxford University Press.
8. 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
9. Chandra Sekhar, & Kumar, M. (2023). An Overview of Cyber Security in Digital Banking Sector. *East Asian Journal of Multidisciplinary Research, 2*(1), 43-52. https://doi.org/10.55927/eajmr.v2i1.1671
10. Chaudhary, K., & Mallick, B. (2012). Exploration of Data mining techniques in Fraud Detection: Credit Card. *International Journal of Electronics and Computer Science Engineering, 1*(3), 1765-1771. Retrieved from https://docplayer.net/10658329-Exploration-of-data-mining-techniques-in-fraud-detection-credit-card-khyati-chaudhary.html
11. Coglianese, C., & Nash, J. (2021). Compliance Management Systems: Do They Make a Difference? In B. Van Rooij & D. Sokol (Eds), *The Cambridge Handbook of Compliance* (pp. 571-593). Cambridge: Cambridge University Press. https://doi.org/10.1017/9781108759458.039
12. Connelly, B. L., Certo, S. T., Ireland, R. D., & Reutzel, C. R. (2011). Signaling Theory: A Review and Assessment. *Journal of Management, 37*(1), 39-67. https://doi.org/10.1177/0149206310388419
13. Dell'Ariccia, G. (2001). Asymmetric information and the structure of the banking industry. *European Economic*

Review, 45(10), 1957-1980. https://doi.org/10.1016/S0014-2921(00)00085-4

14. Dewi, Y., Suharman, H., Sofia Koeswayo, P., & Dewi Tanzil, N. (2023). What is the key determinant of the credit card fraud risk assessment in Indonesia? An idea for brainstorming. *Banks and Bank Systems, 18*(1), 26-37. https://doi.org/10.21511/bbs.18(1).2023.03

15. Donaldson, L., & Davis, J. H. (1991). Stewardship Theory or Agency Theory: CEO Governance and Shareholder Returns. *Australian Journal of Management, 16*(1), 49-64. https://doi.org/10.1177/031289629101600103

16. FST Media. (2016). *The Economics of Fraud – Mitigating Risk Amidst Fast Growth and Innovation*. Retrieved from https://fst.net.au/wp-content/uploads/file/white-paper/the-economics-of-fraud-report.pdf

17. Ghauri, F. (2021). Digital Security Versus Private Information. *International Journal of Computer Science and Information Security (IJCSIS), 19*(7), 10-20. https://doi.org/10.5281/zenodo.5164002

18. Goztepe, K. (2012). Designing fuzzy rule based expert systems for cybersecurity. International Journal of Information Security Science. *International Journal of Information Security Science, 1*(1), 13-19. Retrieved from https://dergipark.org.tr/en/pub/ijiss/issue/16057/167848

19. 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

20. Hasham, S., Joshi, S., & Mikkelsen, D. (2019). *Financial Crime and Fraud in The Age of Cybersecurity.* McKinsey & Company. Retrieved from https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/financial-crime-and-fraud-in-the-age-of-cybersecurity

21. Holt, T. J., Smirnova, O., & Hutchings, A. (2016). Examining signals of trust in criminal markets online. *Journal of Cybersecurity, 2*(2), 137-145. https://doi.org/10.1093/cybsec/tyw007

22. Hovland, C. I., & Sherif, M. (1980). *Social judgments: Assimilation and contrast effects in communication and attitude change*. Greenwood Press. Retrieved from https://psycnet.apa.org/record/1963-06591-000

23. HSN Consultants Inc. (2021). *Nilson Report 1209*. Retrieved from https://nilsonreport.com/newsletters/1209/

24. Hubs, R. (2012). *Fraud brainstorming. Planning to find fraud.* Fraud Magazines, July/August, 2012. Association of Certified Fraud Examiners, Inc. Retrieved from https://www.fraud-magazine.com/article.aspx?id=4294973852

25. IT Governance Indonesia (ITG.ID). (2019). *Apa saja peran audit internal dalam cyber security?* ITG.id. Retrieved from https://itgid.org/apa-saja-peran-audit-internal-dalam-cyber-security/

26. 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. https://doi.org/10.1016/0304-405X(76)90026-X

27. Kathirvel, K. (2013). Credit Card Frauds and Measures to Detect and Prevent Them. *International Journal of Marketing, Financial Services & Management Research, 2*(3), 172-179. Retrieved from https://silo.tips/download/credit-card-frauds-and-measures-to-detect-and-prevent-them#

28. Kim, S.S., & Kim, Y. J. (2017). The effect of compliance knowledge and compliance support systems on information security compliance behavior. *Journal of Knowledge Management, 21*(4), 986-1010. https://doi.org/10.1108/JKM-08-2016-0353

29. Laurens, R., & Zou, C. C. (2016). Using Credit/Debit Card Dynamic Soft Descriptor as Fraud Prevention System for Merchant. *2016 IEEE Global Communications Conference (GLOBECOM)* (pp. 1-7). https://doi.org/10.1109/GLOCOM.2016.7842369

30. Lee, L. (2019). Cybercrime has evolved: it's time cybersecurity did too. *Computer Fraud & Security, 2019*(6), 8-11. https://doi.org/10.1016/S1361-3723(19)30063-6

31. Mohd-Nassir, M. D., Mohd-Sanusi, Z., & Ghani, E. K. (2016). Effect of brainstorming and expertise on fraud risk assessment. *International Journal of Economics and Financial Issues, 6*(4), 62-67. Retrieved from https://www.econjournals.com/index.php/ijefi/article/view/2690

32. Myerson, R. (2002). *Game theory, analysis of conflict*. Harvard University Press. https://doi.org/10.2307/j.ctvjsf522

33. No, W. G., & Vasarhelyi, M. A. (2017). Cybersecurity and continuous assurance. *Journal of Emerging Technologies in Accounting, 14*(1), 1-12. https://doi.org/10.2308/jeta-10539

34. Obuh, A. O., & Babatope, I. S. (2011). Cybercrime Regulation: The Nigerian Situation. In E. Adomi (Ed.), *Frameworks for ICT Policy: Government, Social and Legal Issues* (pp. 98-112). IGI Global. https://doi.org/10.4018/978-1-61692-012-8.ch007

35. Othman, R., Aris, N. A., Mardziyah, A., Zainan, N., & Amin, N. M. (2015). Fraud Detection and Prevention Methods in the Malaysian Public Sector: Accountants' and Internal Auditors' Perceptions. *Procedia Economics and Finance, 28,* 59-67. https://doi.org/10.1016/S2212-5671(15)01082-5

36. Pearson, T. A., & Singleton, T. W. (2008). Fraud and Forensic Accounting in the Digital Environment. *Issues in Accounting Education, 23*(4), 545-559. https://doi.org/10.2308/iace.2008.23.4.545

37. Petrov, C. (2021). *20 Credit Card Fraud Statistics to Keep You Aware in 2022.* Spendmenot. Retrieved from https://spendmenot.com/blog/credit-card-fraud-statistics/

38. Popoola, O. M. J., Che Ahmad, A., & Samsudin, R. (2013). *Forensic Accounting Knowledge and Skills on Task Performance Fraud Risk Assessment: Nigerian Public Sector Experience* (MPRA Paper No. 66676). Retrieved from https://mpra.ub.uni-muenchen.de/66676/1/MPRA_paper_66676.pdf

39. Posthumus, S., & Solms, R. V. (2004). A Framework for the governance of information security. *Computers & Security,* 23(8), 638-646. https://doi.org/10.1016/j.cose.2004.10.006

40. Quick, R., & Sayar, S. (2021). The impact of assurance on compliance management systems on bank directors' decisions. *International Journal of Auditing, 25*(1), 3-23. https://doi.org/10.1111/ijau.12210

41. Remmerbach, K., & Krumme, R. (2020). *The effectiveness of compliance management systems.* FH Münster University of Applied Sciences. Retrieved from https://www.kulturkaufhaus.de/en/detail/ISBN-9783947263219/Remmerbach-Klaus-Ulrich/The-effectiveness-of-compliance-management-systems

42. Riley, B. (2007). Anti-fraud technologies: a business essential in the card industry. *Card Technology Today, 19*(10), 10-11. https://doi.org/10.1016/S0965-2590(08)70133-6

43. Schafer, B. A., & Schafer, J. K. (2019). *Interpersonal Affect, Accountability and Experience in Auditor Fraud Risk Judgments and the Processing of Fraud Cues* (pp. 43-65). https://doi.org/10.1108/S1475-148820190000022004

44. Sekaran, U., & Bougie, R. (2016). *Research Methods for Business: A Skill Building Approach* (7th ed.). Wiley.

45. Shiva, S., Roy, S., & Dasgupta, D. (2010). Game theory for cybersecurity. *Proceedings of the Sixth Annual Workshop on Cybersecurity and Information Intelligence Research* (pp. 1-4). https://doi.org/10.1145/1852666.1852704

46. Sidoti, P. M., & Devasagayam, R. (2010). Credit cards and college students: effect of materialism and risk attitude on misuse. *The Marketing Management Journal, 20*(2), 64-79. Retrieved from https://www.mmaglobal.org/_files/ugd/3968ca_dbde4f639d944242b-91d677bf3fd5461.pdf#page=71

47. Szczepaniuk, E. K., & Szczepaniuk, H. (2022). Analysis of cybersecurity competencies: Recommendations for telecommunications policy. *Telecommunication Policy, 46*(3), 102282. https://doi.org/10.1016/j.telpol.2021.102282

48. Talamantes, J. (2020). *Why is intelligence sharing important in cybersecurity?* RedTeam Security. Retrieved from https://www.redteamsecure.com/blog/why-is-intelligence-sharing-important-in-cyber-security

49. Vatsa, V., Sural, S., & Majumdar, A. K. (2007). A Rule-Based and Game-Theoretic Approach to Online Credit Card Fraud Detection. *International Journal of Information Security and Privacy, 1*(3), 26-46. https://doi.org/10.4018/jisp.2007070103

50. Viswanathan, M., Yang, Y. K., Whangbo, T. K., Kim, N. B., & Garner, B. (2005). Knowledge-based compliance management systems – methodology and implementation. *Fourth Annual ACIS International Conference on Computer and Information Science (ICIS'05)* (pp. 25-29). https://doi.org/10.1109/ICIS.2005.79

51. Vousinas, G. L. (2019). Advancing theory of fraud: the S.C.O.R.E. model. *Journal of Financial Crime, 26*(1), 372-381. https://doi.org/10.1108/JFC-12-2017-0128

52. Yogi Prabowo, H. (2012). A better credit card fraud prevention strategy for Indonesia. *Journal of Money Laundering Control, 15*(3), 267-293. https://doi.org/10.1108/13685201211238034

APPENDIX A

Table A1. Variable description of Digital Security

Indicator	Categories					Sum	Average Score	Score Category
	Very Good	Good	Fair	Poor	Bad			
X1.1.1	135	66	14	0	0	215	4.56	Very Good
	63%	31%	7%	0%	0%	100%		
X1.1.2	140	57	14	4	0	215	4.55	Very Good
	65%	27%	7%	2%	0%	100%		
X1.1.3	110	61	27	12	5	215	4.21	Very Good
	51%	28%	13%	6%	2%	100%		
X1.2.1	120	64	21	4	6	215	4.34	Very Good
	56%	30%	10%	2%	3%	100%		
X1.2.2	134	57	17	3	4	215	4.46	Very Good
	62%	27%	8%	1%	2%	100%		
X1.3.1	131	64	15	2	3	215	4.48	Very Good
	61%	30%	7%	1%	1%	100%		
X1.3.2	132	64	16	0	3	215	4.50	Very Good
	61%	30%	7%	0%	1%	100%		
Digital Security							4.44	Very Good

Table A2. Variable description of Compliance Management

Indicator	Categories					Sum	Average Score	Score Category
	Very Good	Good	Fair	Poor	Bad			
X2.1.1	138	62	0	12	3	215	4.49	Very Good
	64%	29%	0%	6%	1%	100%		
X2.1.2	140	60	0	15	0	215	4.51	Very Good
	65%	28%	0%	7%	0%	100%		
X2.1.3	141	52	0	22	0	215	4.45	Very Good
	66%	24%	0%	10%	0%	100%		
X2.1.4	140	59	0	16	0	215	4.50	Very Good
	65%	27%	0%	7%	0%	100%		
X2.2.1	149	58	0	8	0	215	4.62	Very Good
	69%	27%	0%	4%	0%	100%		
X2.2.2	146	54	0	15	0	215	4.54	Very Good
	68%	25%	0%	7%	0%	100%		
X2.2.3	139	60	0	16	0	215	4.50	Very Good
	65%	28%	0%	7%	0%	100%		
X2.2.4	140	56	0	19	0	215	4.47	Very Good
	65%	26%	0%	9%	0%	100%		
Compliance Management System							4.51	Very Good

Table A3. Variable description of Fraud Brainstorming

Indicator	Categories					Sum	Average Score	Score Category
	Very Good	Good	Fair	Poor	Bad			
X3.1.1	62	80	0	60	13	215	3.55	Good
	29%	37%	0%	28%	6%	100%		
X3.1.2	132	55	0	16	12	215	4,30	Very Good
	61%	26%	0%	7%	6%	100%		
X3.2.1	56	82	0	66	11	215	3.49	Good
	26%	38%	0%	31%	5%	100%		
X3.2.2	149	31	0	22	13	215	4,31	Very Good
	69%	14%	0%	10%	6%	100%		

Table A3 (cont.). Variable description of Fraud Brainstorming

Indicator	Categories					Sum	Average Score	Score Category
	Very Good	Good	Fair	Poor	Bad			
X3.2.3	37	79	0	75	24	215	3.14	Fair
	17%	37%	0%	35%	11%	100%		
X3.2.4	46	92	0	54	23	215	3.39	Fair
	21%	43%	0%	25%	11%	100%		
X3.3.1	39	95	0	57	24	215	3.32	Fair
	18%	44%	0%	27%	11%	100%		
X3.3.2	34	98	0	71	12	215	3.33	Fair
	16%	46%	0%	33%	6%	100%		
X3.3.3	43	98	0	64	10	215	3.47	Fair
	20%	46%	0%	30%	5%	100%		
X3.4.1	43	108	0	58	6	215	3.58	Fair
	20%	50%	0%	27%	3%	100%		
X3.4.2	38	97	0	65	15	215	3.36	Fair
	18%	45%	0%	30%	7%	100%		
X3.5.1	38	93	0	71	13	215	3.33	Fair
	18%	43%	0%	33%	6%	100%		
X3.5.2	36	91	0	80	8	215	3.31	Fair
	17%	42%	0%	37%	4%	100%		
X3.6.1	169	14	0	26	6	215	4.46	Very Good
	79%	7%	0%	12%	3%	100%		
X3.6.2	35	127	0	52	1	215	3.67	Good
	16%	59%	0%	24%	0%	100%		
X3.7.1	139	34	0	39	3	215	4.24	Very Good
	65%	16%	0%	18%	1%	100%		
X3.7.2	161	19	0	28	7	215	4.39	Very Good
	75%	9%	0%	13%	3%	100%		
X3.8.1	42	117	0	55	1	215	3.67	Good
	20%	54%	0%	26%	0%	100%		
X3.8.2	53	108	0	53	1	215	3.74	Good
	25%	50%	0%	25%	0%	100%		
Fraud Brainstorming							3.69	Good

Table A4. Variable description of Competence

Indicator	Categories					Sum	Average Score	Score Category
	Very Good	Good	Fair	Poor	Bad			
Z.1.1	46	116	48	5	0	215	3.94	Good
	21%	54%	22%	2%	0%	100%		
Z.1.2	0	99	0	0	116	215	2.38	Poor
	0%	46%	0%	0%	54%	100%		
Z.2.1	0	114	0	0	101	215	2.59	Poor
	0%	53%	0%	0%	47%	100%		
Z.2.2	0	115	0	0	100	215	2.61	Fair
	0%	53%	0%	0%	47%	100%		
Z.2.3	0	113	0	0	102	215	2.58	Fair
	0%	53%	0%	0%	47%	100%		
Z.3.1	36	117	59	3	0	215	3.87	Good
	17%	54%	29%	1%	0%	100%		
Z.3.2	40	109	63	3	0	215	3.87	Good
	19%	51%	29%	1%	0%	100%		
Z.3.3	34	118	56	7	0	215	3.83	Good
	16%	55%	26%	3%	0%	100%		

Table A4 (cont.). Variable description of Competence

Indicator	Categories					Sum	Average Score	Score Category
	Very Good	Good	Fair	Poor	Bad			
Z.4.1	0	117	0	0	98	215	2.63	Fair
	0%	54%	0%	0%	46%	100%		
Z.4.2	29	145	37	0	4	215	3.91	Good
	13%	67%	17%	0%	2%	100%		
Z.4.3	0	119	0	0	96	215	2.66	Fair
	0%	55%	0%	0%	45%	100%		
Competence							3.17	Fair

Table A5. Variable description of Credit Card Fraud Prevention

Indicator	Categories					Sum	Average Score	Score Category
	Very Good	Good	Fair	Poor	Bad			
Y.1.1	104	52	28	27	4	215	4.05	Good
	48%	24%	13%	13%	2%	100%		
Y.1.2	118	58	13	23	3	215	4.23	Very Good
	55%	27%	6%	11%	1%	100%		
Y.2.1	107	50	25	25	8	215	4.04	Good
	50%	23%	12%	12%	4%	100%		
Y.2.2	104	61	20	26	4	215	4.09	Good
	48%	28%	9%	12%	2%	100%		
Y.3.1	83	83	17	26	6	215	3.98	Good
	39%	39%	8%	12%	3%	100%		
Y.3.2	79	86	19	24	7	215	3.96	Good
	37%	40%	9%	11%	3%	100%		
Y.3.3	96	72	19	24	4	215	4.08	Good
	45%	33%	9%	11%	2%	100%		
Y.4.1	61	91	24	29	10	215	3.76	Good
	28%	42%	11%	13%	5%	100%		
Y.4.2	73	83	12	37	10	215	3.80	Good
	34%	39%	6%	17%	5%	100%		
Y.4.3	30	54	24	55	52	215	2.79	Fair
	14%	25%	11%	26%	24%	100%		
Y.4.4	76	69	31	37	2	215	3.84	Fair
	35%	32%	14%	17%	1%	100%		
Y.4.5	63	47	23	63	19	215	3.34	Fair
	29%	22%	11%	29%	9%	100%		
Y.4.6	24	33	13	18	127	215	3.89	Good
	11%	15%	6%	8%	59%	100%		
Y.5.1	24	29	20	20	122	215	3.87	Good
	11%	13%	9%	9%	57%	100%		
Y.5.2	34	27	18	26	110	215	3.70	Good
	16%	13%	8%	12%	51%	100%		
Y.5.3	26	23	18	21	127	215	3.93	Good
	12%	11%	8%	10%	59%	100%		
Y.6.1	25	33	16	38	103	215	3.75	Good
	12%	15%	7%	18%	48%	100%		
Y.6.2	20	40	17	42	96	215	3.72	Good
	9%	19%	8%	20%	45%	100%		
Credit Card Fraud Prevention							3.82	Good