

Understanding the Potential Impact of Accounting Information System to Computer Accounting Fraud

Arnestesa Trinandha

*Ph.D Student Department of Accounting, Faculty Economics and Business,
Universitas Diponegoro, Indonesia. Jl. Erlangga Tengah No. 17 Semarang
(Corresponding author)*

Imam Ghozali

*Department of Accounting, Faculty Economics and Business,
Universitas Diponegoro, Indonesia.*

Fuad

*Department of Accounting, Faculty Economics and Business,
Universitas Diponegoro, Indonesia.*

Abstract

In addition to providing a positive impact on speed and accuracy of financial statement presentation, the use of Accounting Information System (AIS) also has the have risks that can provide opportunity for the users to misuse the system. Cheating through the information technology allows criminals to fastly gain more benefits (Romney, 1976; Lynch & Gomaa, 2008). The researches on the risks and threats of AIS have been widely conducted and the result shows that both risks and threats can happen (Loch et.al, 1992; Davis et.al., 1996; Henry, 1997; Dhillon,1999; Musa, 2006; Hanini, 2012; Muhrtala & Ogundeji, 2013; ALEKSANDROVA, 2016). Likewise, the research on computer related-fraud (Thompson,1998; Haugen & Selin,1999; Dhillon,1999; Seetharaman,2003; Lee & Lee, 2002) in which the result indicates the presence of unauthorized misuse or interference on computer usage results in computer-related fraud. Nevertheless, this study has not examined how to link the risk factors mediating the use of AIS and the AIS users' attention to perform computer-accounting fraud. Given the large impact on computer-based accounting fraud, it is important to examine the factors of AIS's usage on the attention of AIS's misuse (computer accounting fraud).The samples of this research were cooperatives in Indonesia which were selected because their growth affects on the increasing number of fraud cases. The research result shows that AIS has a positive effect on the risks of AIS which also has a positive

effect on the intention to commit computer-accounting fraud. However, good and deep understanding of the risks of AIS has not been done by AIS users from cooperatives. Thus, the risks of AIS are not a factor that mediates the use of AIS and the intention to commit computer-accounting fraud.

Keywords: Accounting Information Systems; The risks of Accounting Information Systems; Computer Accounting Fraud; Cooperatives.

JEL Classification: M41, M48, M15.

1. INTRODUCTION

The speed and accuracy of financial reporting can be implemented with the support of Accounting Information System (AIS). The inevitable technological advancement and the increasing number of cheaper accounting software in the market affects the consequence of accounting record method, from manual to computer-based. However, the risks of AIS may occur in all forms of enterprise among the benefits of AIS (Musa, 2006).

The research on the risks and threats of AIS has been frequently conducted (Loch et.al, 1992; Davis et.al., 1996; Henry, 1997; Dhillon,1999; Muhrtala & Ogundeji, 2013; Hanini, 2012; Musa, 2006) which shows the presence of the risks and threats. Corbitt (1998) and Musa (2006) propose that the greatest threat of computer system comes from inside, fraud by the staff. The problem in many security abuses is the users of technology who tend to sabotage the control of the system (Dhillon, 1999; Thanh, L. T, 2017).

The change of accounting system presentation from manual to computer-based brings risks and consequences on the occurrence of fraud forms shifting (from traditional embezzlement to information processing technology embezzlement). Romney (1976) also states that computer will make people easy to fraud because the computer fraud is difficult to be detected. The use of AIS in performing the accounting function gives a positive effect on the speed and accuracy of financial statement presentation and opportunities for the users to misuse the system because it allows criminals to gain more benefits (Romney, 1976; Lynch & Gomaa, 2008).

Lynch and Gomaa (2003) try to develop theory of acceptance system called *the theory of planned behavior/TPB* to investigate the potential relationship among information technology users' behavior in business organizations with entity's vulnerability and employee's cheating behavior (Sundström, M., & Radon, A, 2015).. However, the researchers did not examine aspects of risk of technology that could affect the possibility of fraud. The risks of AIS are used to understand the risks perceived by system users, which are able to encourage or prevent the users from fraud. Thus, this study would examine the roles of mediation of AIS's risks on the use of AIS toward intention of AIS misuse (computer accounting fraud). The cooperatives in Indonesia were selected because of their rapid growth (194,295 cooperatives in 2012 and 203,701 cooperatives in 2013) which increased by 9,406 or 4.84%. Ironically, however, the high number of fraud occurs in cooperatives. Through the website of the Minister of

Cooperatives and Small and Medium Enterprises of the Republic of Indonesia (www.depkop.go.id), Syarief Hasan (2012) states that the fraud cases by cooperatives constitute 25% of the total existing cooperatives experiencing fraud. In 2012, the number of cooperatives is 194,295, thus the number of cooperatives experiencing fraud is approximately 48,573. In this case, the members face deficits by losing money entrusted to the cooperative management. Therefore, it is very important to examine the roles of mediation AIS risks on the use of AIS toward the intention of AIS misuse (computer-accounting fraud) in cooperative business sector in Indonesia.

2. LITERATURE REVIEW AND HYPOTHESIS

Accounting System Information is a resources coordination framework (data, materials, equipments, suppliers, personal and funds) to convert input of economic data into output of financial information used to carry out the activities of an entity and provide accounting information interested parties (Wilkinson, 1991; Andriyansah et al, 2017). The environment of accounting information system faces the threat of risks, both internal and external organizations (Loch et.al.,1992; Davis, 1996; Henry, 1997; Dhillon, 1999; Musa, 2006; Susanto & Handayani, 2008; Hanini, 2012, Muhrtala & Ogundeji, 2013). Hence, the following hypothesis is formulated:

H1. Accounting information systems has positive effect on risk of AIS.

Computer-accounting fraud is the misuse of computer in performing accounting function which focuses on hardware, software, data and the users' behavior. Dhillon (1999) explains that the large number of security breach is caused by the technology and its users who sabotage control of the system. Thus, in order to understand the occurrence of misuse of information technology through computer-accounting fraud, it is necessary to analyse the users' behavior and the computer device. Behavioral intention relates to the power of one's will to perform certain behaviors (Lee, 2009; KARMANOVA, 2016; Parwati et al, 2017).

Lee and Lee (2002); Lynch and Gomma (2003); Seetharaman (2004) examine computer misuse on the intention to do computer-related fraud. The use of information technology can reduce the portion of cost ratio by allowing the offenders to quickly target the victims at minimal cost or by reducing the possibility of being caught via online and audit trail (Lynch and Gomma, 2008). The use of AIS can create an environment susceptible to AIS risks. Based on the given review, the following hypothesis is proposed:

H2. The risk of accounting information systems (AIS) mediates the effect of accounting information system on intention to commit computer accounting fraud.

The risk of AIS perceived risk as a potential loss in getting expected benefits by using AIS (Featherman and Pavlou, 2003). Musa (2006) explains that deliberate risks over

the use of AIS such as entry of bad data, destruction of data, introduction to computer viruses are likely associated with computer fraud. Dhillon (1999) argues that the understanding of insecurity or computer misuse phenomenon can be connected to the occurrence of computer-related fraud. The use of information technology triggers a risk that allows criminals to fastly steal more. It also enables the impact on frequent criminal acts, the real incentive to use electronics or computers rather than use the manual way (Lynch & Goma, 2003). The following hypothesis is then formulated:

- H3. The risk of accounting information systems (AIS) has positive effect of intention to commit computer accounting fraud.

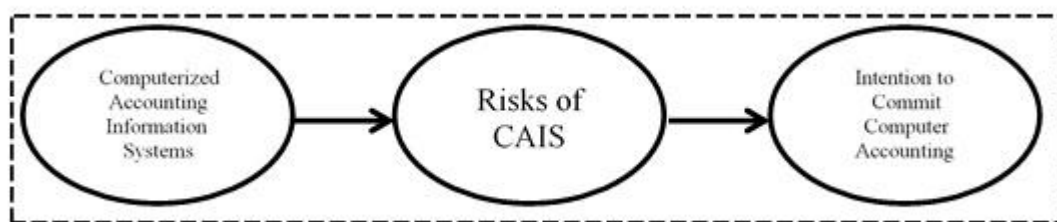


Fig 1. Model Research

3. RESEARCH METHOD

3.1 Population and Sample

Based on data the number of cooperatives published on the website of Ministry of Cooperatives and Small and Medium Enterprises (<http://www.depkop.go.id>), then the population in this study were all cooperatives in Central Java, Indonesia as many as 28.227 units. In this study the applied method in collecting the samples was convenience and purposive sampling, with criteria the cooperatives that have been using accounting software. The questionnaire was distributed conveniently based on addresses available in the database of Ministry of Cooperatives and SMEs. Since the database of the Ministry of Cooperatives and SMEs can not show which cooperative has been using accounting software and which ones not yet, then to acknowledge whether a cooperative has been using accounting software, researchers asked questions in the questionnaire.

3.2 Profile of Respondents

The number of respondents involved in this research was 232 respondents consisting of : 54.7% women; 45.3% men; 13.4% age of 20-25; 41.8% age of 26-30, 25.4% age of 31-35; 12.5% age of 36-40; 6.9% age of 41-45. Based on the experience of using AIS, there were: 63.4% using 1-5 years of system; 22.8 % using 6-10 years of system; 13.8%

using 11-15 years of system. Based on the education level, there were: 7.3% who had completed high school; 37.9% who possessed college diplomas; 51.3% who held bachelor's degree; and 3.4% possessed master's degree.

3.3 Research Instrument and Measurement

The instrument of this study is questionnaire adopted from the previous research and developed by the researcher. The questionnaire was designed by using five Likert scales consisting of *strongly disagree (1)* to *strongly agree (5)*. Face validity and construct validity were used to test the validity of the research model, while Construct Reliability (CR) was employed for testing reliability. Instruments are considered valid if they possess a factor loading value greater than 0.4, and considered reliable if the CR value is greater than 0.7 and the Variance Extract is greater than 0.5 (Hair et al., 2010). Validity and reliability testing were conducted and it has been found that all instruments in this research are valid and reliable. Refer to Table 1 for further clarification of these results.

Table 1. Instrument Validity and Reliability

Variable	Indicators	Factor Loading	Construct Reliability (CR) & Variance Extract (VE)
Accounting Information Sytem	- Activity of transaction processing system	0.71	CR: 0.76 VE: 0.51
	- Implementation of the cycle of financial transactions	0.75	
	- Consistency of data in the AIS database system	0.68	
Risk of CAIS	- Performance risk	0.66	CR: 0.79 VE: 0.50
	- Time risk	0.71	
	- Social risk	0.73	
	- Privacy risk	0.68	
Intention to commit Computer Accounting Fraud	- Damage of files	0.69	CR: 0.96 VE: 0.88
	- Unauthorized access	0.76	
	- Entry Viruses	0.73	
	- Deletion of the outputs	0.73	

Source: primary data analyzed

Findings

Goodness of fit Evaluation

SEM analysis with AMOS statistical software was used as the data processing. The result of goodness of fit test shows that RMSEA=0.037; GFI=0.957; AGFI=0.931; TLI=0.978 and CFI=0.983. In conclusion, this research model is fit.

Goodness of Fit:

Chi Square =53,705
 Probability =,088
 RMSEA =,037
 GFI =,957
 AGFI =,931
 CMIN DF =1,310
 TLI =,978
 CFI =,983
 DF =41

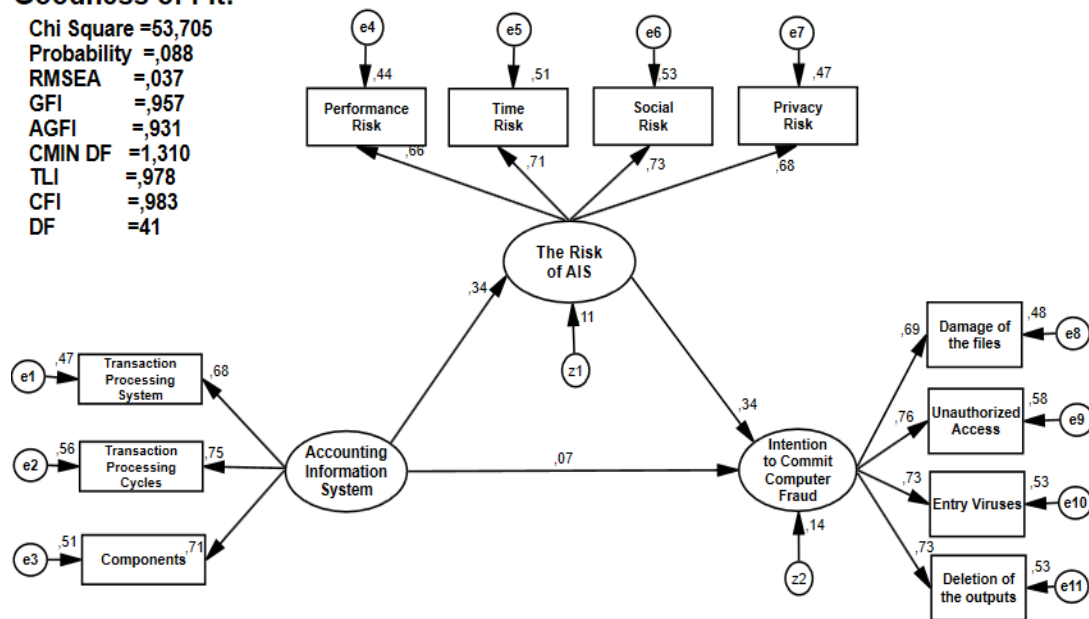


Fig 2. Analysis Model with AMOS

Results of Hypothesis Testing

Results of hypothesis are shown in table 2 below :

Table 2. Results of Hypothesis Testing

Hypothesis	Estimate	S.E.	Critical Ratio	P value (≤ 0.05)	Explanation
H1: Accounting information systems has positive effect on risk of AIS.	.333	.091	3.658	***	Accepted
H2: The risk of accounting information systems mediates the effect of accounting information system on intention to commit computer accounting fraud.	.068	.084	.807	.420	Rejected
H3: The risk of AIS has positive effect of intention to commit computer accounting fraud.	.329	.090	3.652	***	Accepted

Source: primary data analyzed

4. DISCUSSION AND CONCLUSION

4.1 Discussion

The result of the first hypothesis shows that Accounting Information System (AIS) has a positive effect on the risks of AIS. This result supports the previous research which states that AIS face the perceived threat of risk, both from internal and external organizations (Loch et.al.,1992; Davis, 1996; Henry, 1997; Dhillon, 1999; Musa, 2006; Susanto & Handayani, 2008; Hanini, 2012, Muhrtaala & Ogundeji, 2013).

The result of the second hypothesis shows that AIS is not the mediator of its effect on the intention to commit computer-accounting fraud. It is because of the lack of cooperative management understanding of the importance of AIS risks. Thus, AIS risks are not a mediating effect of accounting information system users on the intention to commit computer-accounting fraud.

The result of the third hypothesis shows that the risk of AIS has a positive effect of intention to commit computer-accounting fraud. These results are consistent with the research by Musa (2006), Dhillon (1999), Lee and Lee (2002), Lynch and Gomaa (2003), Seetharaman (2004), who explain that the risks of AIS usage can be connected to the occurrence of computer-related fraud. The use of information technology triggers a risk that allows criminals to fastly steal more. It also enables the impact of frequent criminal acts, the real incentive to use electronics or computers rather than use manual way (Lynch & Gomaa, 2008).

4.2 Conclusion

This research shows the users' awareness of the use of AIS that triggers the risks. The risks of using AIS allow users to misuse AIS. Information technology fraud gives a chance to get more result. However, good and deep understanding of the risks of AIS has not been done by the AIS users from cooperatives, thereby the risks of AIS are not a factor that mediates the use of AIS toward the intention to commit computer-accounting fraud.

LIMITATION AND SUGGESTIONS FOR FUTURE RESEARCH

This study has several limitations. The researcher only examines the intention to commit computer-accounting fraud, but not examining the behavior of doing computer fraud. It is because of the difficulty of measuring AIS users' behavior in committing computer-accounting fraud. For further researchers, the researcher suggests to examine the influence of the use of AIS toward the system misuse behavior. It is possible to add moderation affects based on gender, age and experience of using the system, so that various explanation of system users' behavior toward system misuse can be obtained.

REFERENCES

- [1] Aleksandrova, A.V., Protsenko, E. V., Sekering, V.D., & Gorohova, A. E (2016) Risk Management Tools in Russian Aviation Engineering Companies. *Editorial Board*, 11(1), 39. <https://www.ceeol.com/search/article-detail?id=535512>
- [2] Bierstaker L. James et.al., 2006. "Accountants perceptions regarding fraud detection and prevention methods." *Managerial Auditing Journal*, 21(5), 520-535. <https://doi.org/10.1108/02686900610667283>
- [3] Davis, Charles E. 1996. "Perceived Security Threats to today's Accounting Information Systems: a Survey of CISAs". *IS Audit & Control Journal*, 3, 38-41.
- [4] Dhillon Gupreet, 1999. "Managing and controlling computer misuse". *Information Management and Computer Security*, 7(4), 171-175. <https://doi.org/10.1108/09685229910292664>
- [5] Dorminey Jack et.al., 2012. "The Evolution of Fraud Theory". *Issues in Accounting Education* 27(2),555-579. <https://doi.org/10.2308/iace-50131>
- [6] Hanini A.E., 2012. "The Risk of Using Computerized Accounting Information Systems in the Jordanian banks: their reasons and ways of prevention". *European Journal of Business and Management*, 4(20), 53-63. [http://pakacademicsearch.com/pdf-files/ech/517/53-63%20Vol%204,%20No%2020%20\(2012\).pdf](http://pakacademicsearch.com/pdf-files/ech/517/53-63%20Vol%204,%20No%2020%20(2012).pdf)
- [7] Haugen S. and Selin R.J., 1999. "Identifying and controlling computer crime and employee fraud". *Industrial Management and Data Systems* 99(8), 340-344. <https://doi.org/10.1108/02635579910262544>
- [8] Henry Laurie, 1997. "A Study of the nature and security of accounting information systems: The case of Hampton Roads, Virginia". *The Mid-Atlanta Journal of Business*, 33(3), 171-189. <https://search.proquest.com/openview/6763f0a13f1ec31d7c6b5d070b6e4197/1?pq-origsite=gscholar&cbl=24292>
- [9] KARMANOVA, T. E., PODSEVALOVA, E. N., MITYURNIKOVA, L. A., SILAEVA, A. A., & ATAMANOVA, M. A. (2016). Peculiarities of improving internal financial control in the Russian corporations. *Editorial Board*, 11(1), 39 <https://www.ceeol.com/search/article-detail?id=535525>
- [10] Loch, Karen D., Houston H. Carr and Merrill E. Warkentin 1992. "Threats to Information Systems: Today's Reality, Yesterday's Understanding". *MIS Quarterly*, Juni, 173-186. http://www.jstor.org/stable/249574?seq=1#page_scan_tab_contents
- [11] Makumbi L., Miriti K.E. and Kahinge M.A., 2012. "An Anlysis of Information Technology (IT) Security Practices: A Case Study of Kenyan Small and Medium Enterprises (SMEs) in the Financial Sector". *International Journal of Computer Applications*, 57(18), 33-36 <http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.252.8124&rep=rep1&type=pdf>

- [12] Muhrtala O.T. and Ogundeji M., 2013. “*Computerized Accounting Information Systems and Perceived Security Threats in Developing Economies: the Nigerian Case*”. *Universal Journal of Accounting and Finance* 1(1), 9-18. http://www.hrpub.org/journals/article_info.php?aid=168
- [13] Musa, A.,2006. “*Exploring perceived threats of CAIS in developing countries: the case of Saudi Arabia.*” *Managerial Auditing Journal*, 21(4), 387-407. <https://doi.org/10.1108/02686900610661405>
- [14] Musa, A.,2007. “*Evaluating the security controls of CAIS in developing countries: an empirical investigation.*” *Information Management and Computer Security*, 15(2),128-148. <https://doi.org/10.1108/09685220710748038>
- [15] Purnamasari I.D., 2014. “The Threat Level Tolerance in the Company of Accounting Information System”. *International Journal of Computer and Communications Security*, 2(5), 173-178. https://s3.amazonaws.com/academia.edu.documents/30930735/2012_Proceeding_The_2nd_ICBB.pdf?AWSAccessKeyId=AKIAIWOWYYGZ2Y53UL3A&Expires=1523379211&Signature=drS711sut3br%2Fpmsgx%2BUPChGou9A%3D&response-content-disposition=inline%3B%20filename%3D%20THE_THREAT_LEVEL_TOLERANCE_IN_THE_COMPAN.pdf
- [16] Seetharaman, S. dan Periyamayagam, 2004. “*Anatomy of Computer Accounting Frauds*”, *Managerial Auditing Journal*, 19(8), 1055-1072 <https://doi.org/10.1108/02686900410557953>
- [17] Andriyansah, Zahra, F., Santorry, Parwati, N. M. S., Kurniawan, S., Simanjuntak, R. H., . . . Mulatsih, R. (2017). Does Accounting Control System Boost Marketing Capabilities? *International Journal of Civil Engineering & Technology*, 8(8), 209–216.
- [18] Sundström, M., & Radon, A. (2015). Utilizing the concept of convenience as a business opportunity in emerging markets. *Organizations and Markets in Emerging Economies*, 6(2), 7-21. <https://www.ceeol.com/search/article-detail?id=460355>
- [19] Thanh, L. T. (2017). Corruption, Provincial Institutions And Capital Structure: New Evidence From A Transitional Economy. *Organizations & Markets in Emerging Economies*, 8(1). <http://web.a.ebscohost.com/abstract?direct=true&profile=ehost&scope=site&authtype=crawler&jrnl=20294581&AN=123789001&h=uYPIIcJM5hcpRH4oKGPdGyl35vZK%2bKsCcnOTYx7MYakNj3GVA0CPGtJhLjONdhJSxoR86WXFkiMTxDcfGDHJA%3d%3d&crl=c&resultNs=AdminWebAuth&resultLocal=ErrCrlNotAuth&crlhashurl=logina.spx%3fdirect%3dtrue%26profile%3dehost%26scope%3dsite%26authtype%3dcrawler%26jrnl%3d20294581%26AN%3d123789001>
- [20] Zahra, F. et al, 2017.” Does e-procurement solve Indonesia Local Government budgetary Slack Through It Adaptive Culture?” *International Journal Of Civil Engineering and Technology* 8(8), 1001-1010 <http://www.iaeme.com/ijciat/issues.asp?JType=IJCIET&VType=8&IType=8>

- [21] Trim R.J Peter, 2006. “*Managing computer security issues: preventing and limiting future threts and disasters*”. Disaster Prevention and Management 14(4),493-505. <https://doi.org/10.1108/09653560510618339>
- [22] Whitman E.M., 2004. “*In defense of the realm: understanding the threats to information security*”. International Journal of Information Management , 24, 43-57. <https://doi.org/10.1016/j.ijinfomgt.2003.12.003>
- [23] Wilhelm K. Wesley, 2004. “*The Fraud Management Lifecycle Theory: A Holistic Approach to Fraud Management.*” Journal of Economic Crime Management 2(2),1-38. <https://utica.edu/academic/institutes/ecii/publications/articles/BA309CD2-01B6-DA6B-5F1DD7850BF6EE22.pdf>
- [24] Parwati NMS, et. al, 2017. “*The Effect Of Self Assessmen System and Fraud Detection Possibility Toward Tax Evasion Behavior.*” Journal of Economic Crime Management 2(2),1-38. <http://www.iaeme.com/IJMET/issues.asp?JType=IJMET&VType=8&IType=8>