



JURNAL

Riset Akuntansi dan Keuangan Indonesia

URL : <http://journals.ums.ac.id/index.php/reaksi/index>



ISO 27001 Information Security Management System: Effect of Firm Audits in Emerging Blockchain Technology

Yunita Tanadi , Raden Roro Widya
Ningtyas Soeprajitno, Gery Lusiano
Firmansah, Tsanya El Karima
Accounting Department, Faculty
of Economics and Business,
Universitas Airlangga

[raden.roro.widya-2016@feb.unair.
ac.id](mailto:raden.roro.widya-2016@feb.unair.ac.id)

Keywords:

Information Security Management System, ISO 27001, Audit Firm

ABSTRACT

The emergence of Blockchain Technology is closely related to improving the ISO 27001 Information Security Management System for confidence in data and information security, preventing manipulation and various information risks that occur. This study examines the effect of the Audit Firm on companies that carry out ISO 27001 certification. This study uses 578 samples listed on the Indonesia Stock Exchange from 2013 – 2017. This study uses a quantitative method with OLS regression testing STATA 14. This study obtained the results that the Audit Firms have a significant influence at the 5% level on the company's decision to improve the Information Security Management System as proxied by ISO 27001. This research has an empirical contribution to developing theory, participating in developing research related to ISO 27001 certification, and assessing the existence of an Audit Firm on the improvement of the Security Management System. Corporate information in the era of blockchain technology.

INTRODUCTION

The emergence of blockchain technology brings a concept where recorded transactions can reliably verify each other's information regarding the entire joint transaction [1]. Blockchain developments that fall into the realm of auditing ensure that audit tracks can verify reported transactions. Guidelines for Auditing Management Systems (2011) describe the capabilities of blockchain in several situations, including the need for proof of guarantor, identity of ownership, and in a specific space of time. As a result, blockchain has claimed to have the potential to make accounting information more reliable and timely with a better alternative to accounting and auditing systems [2], [3], provides authentication transparency [4], [5].

Blockchain provides transparent and immutable data security and allows companies to record transactions in immutable accounting records [6]. Practically, manipulation, forgery, and destruction are impossible because of their sealed and cryptographically distributed state [7]. Blockchain tends to increase shareholder trust of the opportunity to disclose off-book transactions and hidden accounts, enhance firms' competitive stance and regulatory compliance [8].

This influences auditors to be involved in business and risk suppression by encouraging the guarantee of ISO 27001 certification as one of the company's information security management systems. This standard uses a control-based management approach based on risk analysis. Therefore, this security standard is a good response for companies that can be used as a guideline or framework for developing and maintaining an adequate information security management system. The ISO/IEC 27000, 27001, and 27002 standards are international standards receiving increasing recognition and adoption. They were referred to as "the common language of organizations worldwide" for information security.

In research conducted by [9], companies need to be responsible to any party (stakeholders) and maintain relationships with their stakeholders, one of which is the security of their data and information. The effort to improve the information security system to minimize the risk of misuse of the access to information [10], [11]. Several theories that support the use of ISO 27001 are

carried out by [12], which states that ISO 27001 has 133 information security controls. In practice, the company can choose which controls are most relevant to conditions in the field. According to [13], [14], the application of ISO/IEC 27001 is an essential requirement in achieving information security. It can protect aspects of information security, namely confidentiality, integrity, and availability.

Apart from that, [15] believes that the increasing significance of information technology will also increase the urgent need for adequate information security measures. As the four largest KAPs globally, the Big Four has Big Four can assist internal auditors in evaluating and improving the effectiveness of risk management, especially related to information security. Research by [16], [17] found an influence between the existence of the Big Four and the level of adoption of the risk-based approach, where there is more significant pressure on companies audited by the Big Four to implement and disclose information security [18].

This study uses OLS Regression testing processed using STATA 14. This study uses a sample of 578 companies listed on the Indonesia Stock Exchange (IDX) from 2013 - 2017. This study aims to determine the effect of Audit Firms on companies carrying out ISO 27001 certification. This study found that companies that use audit firm KAP Big 4 have a positive effect on their company's ISO certification. That is because audit firms included in BIG4 will reduce the risk of data leakage and increase company information security. In addition, this is because the audit firm fully supports the company's activities in maintaining their audit results and supports a better reputation.

This research contributes to developing theories and literature related to decisions to improve Information Security Management Systems in companies. Practically, the results of this research will be a consideration for companies to carry out ISO 27001 certification, considering that the security of company information is crucial for the sustainability of the company itself. As for investors, investors will benefit if their companies pay more attention to certification and better risk safeguards.

Henceforth, this research is structured as follows; Section 2 covers the theoretical foundations relevant to information security management;

Section 3 research methodology used; Section 4 contains the research results, and Section 5 contains conclusions.

Literature Review and Hypothesis Development Stakeholder Theory

Stakeholder theory states that an entity tries to align its activities with stakeholder expectations [19]. Stakeholder theory states that the company is not an entity that only operates for its interests but must provide benefits to its stakeholders, shareholders, creditors, consumers, government suppliers, communities, analysts, and other parties.

Stakeholder theory describes which parties (stakeholders) the company is responsible for [9]. Therefore, companies must maintain relationships with their stakeholders by accommodating the wishes and needs of their stakeholders, one of which is the security of their data and information. This kind of decision is the best option because the use of IT in their operations is closely related to the increasingly widespread use of internet technology, real-time accounting systems, electronic commerce (e-commerce), and websites and social media for information disclosure. Consequently, ensure the improvement of their information security system to minimize the risk of misuse of the access to information [10], [11].

ISO 27001 Information Security Management System

Good management of information system security is needed to anticipate possible threats. Companies can implement and manage information system security behind the compilation of the ISO/IEC 27000 series, which is a standard on Information Security Management System (ISMS) or Information Security Management System (ISMS).

According to ISO/IEC 27000:2014, ISMS is a systematic approach to establishing, implementing, operating, monitoring, reviewing, maintaining, improving information security, and an overall approach to people, processes, and technology effective functioning of information security. According to [13], [14], the application of ISO/IEC 27001 is an essential requirement in achieving information security. It can protect aspects of information security, namely confidentiality, integrity, and availability. Furthermore, this

standard is independent of information technology products. It requires a risk-based management approach designed to ensure that the selected security controls can protect information assets from various risks and provide confidence in the level of security for interested parties.

Information Security Required within the company Charles Hughes, partner and head of IT practice at management consul AT Kearney, recently accredited, explains that ISO standards are becoming increasingly significant in assessments for public sector tenders. Implementing ISO/IEC 27001 becomes a reference for assessing information system security, increasing public trust in the information produced and processed by a company, and improving the quality assurance of information, integrating with other information system security models.

Audit Firms

Research conducted by [20] results that the Big Four variables significantly influence the disclosure of the risk-based approach. Hoyt (2008) conducted a study and obtained the results that the size of the audit firm has a significant effect on controlling information security risk. As the four largest KAPs globally, the Big Four has a good reputation and expertise to identify company risks that may occur. The Big Four can assist internal auditors in evaluating and improving the effectiveness of risk management, especially related to information security, improvement of the quality of a company's risk assessment and monitoring. Research by [16], [17] found an influence between the existence of the Big Four and the level of adoption of the risk-based approach, where there is tremendous pressure on companies audited by the Big Four to implement and disclose information security [18].

Large auditors usually have more experience and resources through the scale of their business, both audit and advisory services. Therefore, they can leverage their experience and resources to understand client vulnerabilities better and better assess information security risks. Therefore, it is highly relevant for auditors to encourage their behavior to improve their information security by adopting ISO 27001. From here, the hypothesis of this research has formulated:

H1: Audit Firm has affected the ISO 27001 Information Security Management System

RESEARCH METHODS

This study uses Logit Regression Analysis and is processed using STATA 14. This study uses a sample of companies listed on the Indonesia Stock Exchange (IDX) in 2013 – 2017 by excluding financial sector companies. The total initial population was 896 companies and excluded from the missing data, so 578 observation sample. For convenience, the following is the sample selection process shown in Table 1 in this study.

Table 1. Sample selection and firm distribution by industry and period

Selection criteria	Observations
Initial observations	896
Excluded: firms with missing data	(318)

Final observations	578
--------------------	-----

This table reports the sample selection for the period and industry breakdown of the sample firms. In addition, panel A reports the selection of firm-year observations for the regression analyses in this study.

This study uses ISO 27001 as a dependent variable to represent the company's condition to certifications and representing to achieve information security and protect aspects of information security. AFIRM is an independent variable that represents what the audit firm qualification can affect the policy to the company get the special attention about certification. This study also involves a control variable representing the company to reduce bias analysis. To know the detail of variable, Table 2 show all of the variable definitions.

Table 2. Variables Definitions

Initial Name	Definitions	Sources
Dependent Variable		
ISO 27001	Dummy variable, 1 for companies that have ISO 27001 certification, and 0 for otherwise.	Annual Report
Independent Variable		
AFIRM	Dummy variable, 1 for companies audited by KAP Big Four, and 0 for otherwise.	Annual Report
Control Variables		
ARL	The number of days between the end of the financial year and the date of the audit report signature	Annual Report
OPN	Dummy variable, 2 for companies that receive an unqualified audit opinion, 1 for companies with a modified audit opinion, and a value of 0 for companies with a disclaimer audit opinion and without an opinion.	ORBIS
AFEE	Total audit fees in the company.	Annual Report
FSIZE	Natural logarithm of total assets at the end of the fiscal year	ORBIS
LEV	Total debt divided by total assets	ORBIS
ROE	Earnings before interest and tax divided by the total book value of equity	ORBIS
ROA	Earnings before interest and tax divided by the total book value of assets	ORBIS

Table 3 displays the distribution of the research sample by Industry Sector and Year observations. Again, we used unbalanced data and show that the construction industries have dominated in this

sample. However, that does not affect the main testing because the measurement in this study obtained be clear.

Table 3. Firm Distributions by Industry and Year Observations

Industry	Year Observations					Total
	2013	2014	2015	2016	2017	
(SIC 1) Mining	28	29	28	29	25	139
(SIC 2) Construction Industries	20	39	45	42	28	174
(SIC 3) Manufacturing	11	17	20	25	20	93
(SIC 4) Transportation, Communications and Utilities	13	17	21	21	17	89
(SIC 5) Wholesale & Retail Trade	6	8	7	8	20	39

Industry	Year Observations					Total
	2013	2014	2015	2016	2017	
(SIC 6) Finance and Banking	7	0	0	0	10	17
(SIC 7) Service Industries	3	3	8	7	6	27
Total	88	113	129	132	116	578

Table 3 reports the industry breakdown of the firms and firm-year observations. Again, the industry classification has based on one-digit SIC codes.

RESULTS AND DISCUSSION

Empirical Result

Table 4 shows descriptive statistics on 578 companies used in this research sample. It can show the mean of companies that have ISO 27001 is 0.031. That's mean the companies in Indonesia only have a few ISO 27001 Information Security Management

System certifications. The mean of BIG 4 is 0.517, ARL is 74,535, with OPN having a mean of 1.991. For non-dummy variables, the magnitude of the variation is more complex. For example, ROE has a minimum value of -139,230 and a maximum value of 182.220, while ROA has a minimum value of -44,930 and a maximum value of 70,920.

Table 4. Statistic Descriptive

	Mean	Median	Minimum	Maximum
ISO27001	0.031	0.000	0.000	1.000
AFIRM	0.517	1.000	0.000	1.000
ARL	74.535	78.000	17.000	274.000
OPN	1.991	2.000	0.000	2.000
AFEE	5.062e+09	8.618e+08	20900000.000	1.704e+12
FSIZE	21.437	21.451	16.535	25.664
LEV	1.408	0.958	0.008	14.812
ROE	10.148	10.440	-139.230	182.220
ROA	6.024	4.930	-44.930	70.920

Note: This table shows the Descriptive Statistics used in this study. The total sample used is 578 observations from companies listed on the Indonesia Stock Exchange 2013 – 2017.

In Table 5. Explains the relationship between variables, which can show the correlation between variables. There are three kinds of asterisks *, **, and ***, which show a better effect as the number of asterisks increases. While the negative sign indicates a reverse relationship and the positive sign

indicates a unidirectional relationship. This study shows that BIG4, ARL, FSIZE have correlations on ISO27001. BIG 4 itself has correlated by ARL at 10% level, OPN at 5% level, and FSIZE, LEV, ROA, ROE at 1% level.

Tabel 5. Pearson Correlation

	ISO27001	AFIRM	ARL	OPN	AFEE	FSIZE	LEV	ROE
ISO27001	1.000							
AFIRM	0.173*** (0.000)	1.000						
ARL	-0.112*** (0.007)	-0.078* (0.061)	1.000					
OPN	0.017 (0.688)	0.097** (0.020)	-0.363*** (0.000)	1.000				
AFEE	0.022 (0.595)	0.057 (0.170)	-0.049 (0.243)	0.004 (0.932)	1.000			
FSIZE	0.218***	0.454***	-0.151***	-0.045	0.014	1.000		

	ISO27001	AFIRM	ARL	OPN	AFEE	FSIZE	LEV	ROE
	(0.000)	(0.000)	(0.000)	(0.281)	(0.729)			
LEV	-0.001	-0.124***	0.055	-0.012	-0.005	-0.245***	1.000	
	(0.982)	(0.003)	(0.184)	(0.769)	(0.907)	(0.000)		
ROE	-0.009	0.158***	-0.212***	0.083**	0.261***	0.191***	-0.255***	1.000
	(0.831)	(0.000)	(0.000)	(0.047)	(0.000)	(0.000)	(0.000)	
ROA	-0.015	0.227***	-0.197***	0.082**	0.262***	0.219***	-0.273***	0.893***
	(0.711)	(0.000)	(0.000)	(0.048)	(0.000)	(0.000)	(0.000)	(0.000)

p-values in parentheses

* *p* < 0.1, ** *p* < 0.05, *** *p* < 0.01

Main Result

In this study, the proposed hypothesis testing uses a logit regression model to test an audit firm's

effect on companies with ISO 27001 certification.

The following is the regression equation model in this study.

$$ISO27001 = \beta_1 + \beta_2 AFIRM_{it} + \beta_3 OPN_{it} + \beta_4 AFEE_{it} + \beta_5 FSIZE_{it} + \beta_6 LEV_{it} + \beta_7 ROE_{it} + \beta_8 ROA_{it} + \varepsilon$$

In Table 6. it is known the results of testing with OLS regression to test the effect of the independent variable on the dependent variable, each of which follows the regression model used in this study. The results of testing this hypothesis indicate the effect of BIG 4 (AFIRM) on companies to carry out ISO 27001 certification to reduce the risk of data leakage and improve company information security. Auditors affiliated with BIG 4 have a significant effect at the 5% level and are positive with a coefficient of 0.036 against ISO 27001.

Table 6. Logit Regression Result

	ISO27001
AFIRM	0.038** (2.36)
ARL	-0.001** (-2.21)
OPN	-0.025 (-0.31)
AFEE	0.000 (0.79)
FSIZE	0.020*** (3.85)
LEV	0.004 (0.86)
ROE	0.000 (0.36)
ROA	-0.002 (-1.37)
_cons	-0.312 (-1.39)

	ISO27001
r2	0.072
N	578

t statistics in parentheses * *p* < 0.1, ** *p* < 0.05, *** *p* < 0.01

The result of this study explained that the Big Four as 4 KAPs has an excellent reputation and expertise to identify company risks, understand client vulnerabilities, and assess information security risks better. The level of adoption of the risk-based, where there is more significant pressure on companies audited by the Big Four to implement and disclose information security.

CONCLUSION

Blockchain technology has emerged in the world of auditors and was also responded to improve the ISO 27001 Information Security Management System in the company. This study found a significant and positive effect of the Audit Firm on the ISO 27001 Information Security Management System. BIG4 KAP in Indonesia has a good reputation and expertise to identify corporate risks, understand client vulnerabilities, and better assess information security risks. However, this study has limitations in measurement, and indicators may be needed in other measurements in the variables you want to represent for a better information security management system.

REFERENCE

- [1] A. Bahga and V. K. Madiseti, "Blockchain platform for industrial internet of things," *J. Softw. Eng. Appl.*, vol. 9, no. 10, pp. 533–546, 2016.
- [2] J. G. Coyne and P. L. McMickle, "Can blockchains serve an accounting purpose?," *J. Emerg. Technol. Account.*, vol. 14, no. 2, pp. 101–111, 2017.
- [3] J. Kokina, R. Mancha, and D. Pachamanova, "Blockchain: Emergent industry adoption and implications for accounting," *J. Emerg. Technol. Account.*, vol. 14, no. 2, pp. 91–100, 2017.
- [4] J. Dai and M. A. Vasarhelyi, "Toward blockchain-based accounting and assurance," *J. Inf. Syst.*, vol. 31, no. 3, pp. 5–21, 2017.
- [5] D. Yermack, "Corporate governance and blockchains," *Rev. Financ.*, vol. 21, no. 1, pp. 7–31, 2017.
- [6] F. S. Piazza, "Bitcoin and the blockchain as possible corporate governance tools: Strengths and weaknesses," *Bocconi Leg. Pap.*, vol. 9, p. 125, 2017.
- [7] M. Rauchs and G. Hileman, "Global blockchain benchmarking study," *Cambridge Cent. Altern. Financ. Reports*, 2010.
- [8] D. Tapscott and A. Tapscott, "How blockchain will change organizations," *MIT Sloan Manag. Rev.*, vol. 58, no. 2, p. 10, 2017.
- [9] R. E. Freeman and J. McVea, "A stakeholder approach to strategic management. The Blackwell handbook of strategic management, 189-207," *Anal. D'UNE Rev. Litt.*, 2001.
- [10] A. Kotb and C. Roberts, "The impact of e-business on the audit process: An investigation of the factors leading to change," *Int. J. Audit.*, vol. 15, no. 2, pp. 150–175, 2011.
- [11] A. H. Amoush, "Using Information Technology among Auditors in Jordan," *Int. Res. J. Appl. Financ.*, vol. 10, no. 3, pp. 109–114, 2019.
- [12] M. Bakri and N. Irmayana, "Analisis Dan Penerapan Sistem Manajemen Keamanan Informasi SIMHP BPKP Menggunakan Standar ISO 27001," *J. Tekno Kompak*, vol. 11, no. 2, pp. 41–44, 2017.
- [13] C. Chazar, "Standar manajemen keamanan sistem informasi berbasis ISO/IEC 27001: 2005," *J. Inform. dan Sist. Inf.*, vol. 7, no. 2, pp. 48–57, 2015.
- [14] S. D. Utomo, I. D. Pamungkas, and Z. Machmuddah, "The moderating effects of managerial ownership on accounting conservatism and quality of earnings," *Acad. Account. Financ. Stud. J.*, vol. 22, no. 6, p. 2635, 2018.
- [15] G. Disterer, "ISO/IEC 27000, 27001 and 27002 for information security management," 2013.
- [16] M. S. Beasley, R. Clune, and D. R. Hermanson, "Enterprise risk management: An empirical analysis of factors associated with the extent of implementation," *J. Account. public policy*, vol. 24, no. 6, pp. 521–531, 2005.
- [17] K. Desender, "On the determinants of enterprise risk management implementation," in *Enterprise IT governance, business value and performance measurement*, IGI Global, 2011, pp. 87–100.
- [18] C. J. P. Chen, X. Su, and X. Wu, "Auditor changes following a Big 4 merger with a local Chinese firm: A case study," *Audit. A J. Pract. theory*, vol. 29, no. 1, pp. 41–72, 2010.
- [19] D. G. Barako and A. M. Brown, "Corporate social reporting and board representation: evidence from the Kenyan banking sector," *J. Manag. Gov.*, vol. 12, no. 4, pp. 309–324, 2008.
- [20] J. Meizaroh & Lucyanda, "Pengaruh Corporate Governance dan Konsentrasi Kepemilikan pada Pengungkapan Enterprise Risk Management," *Simp. Nas. Akunt. XIV. Hal*, pp. 1–30, 2011.