



# “Evaluating the impact of risk management and risk-based internal audit on fraud detection in local governments”

## AUTHORS

Angginun Juwita Sari Harahap   
Erlina 

## ARTICLE INFO

Angginun Juwita Sari Harahap and Erlina (2024). Evaluating the impact of risk management and risk-based internal audit on fraud detection in local governments. *Problems and Perspectives in Management*, 22(3), 653-664. doi:10.21511/ppm.22(3).2024.50

## DOI

[http://dx.doi.org/10.21511/ppm.22\(3\).2024.50](http://dx.doi.org/10.21511/ppm.22(3).2024.50)

## RELEASED ON

Monday, 30 September 2024

## RECEIVED ON

Friday, 29 March 2024

## ACCEPTED ON

Friday, 30 August 2024

## LICENSE



This work is licensed under a [Creative Commons Attribution 4.0 International License](https://creativecommons.org/licenses/by/4.0/)

## JOURNAL

"Problems and Perspectives in Management"

## ISSN PRINT

1727-7051

## ISSN ONLINE

1810-5467

## PUBLISHER

LLC “Consulting Publishing Company “Business Perspectives”

## FOUNDER

LLC “Consulting Publishing Company “Business Perspectives”



NUMBER OF REFERENCES

38



NUMBER OF FIGURES

1



NUMBER OF TABLES

8

© The author(s) 2024. This publication is an open access article.



## BUSINESS PERSPECTIVES



LLC "CPC "Business Perspectives"  
Hryhorii Skovoroda lane, 10,  
Sumy, 40022, Ukraine  
[www.businessperspectives.org](http://www.businessperspectives.org)

**Received on:** 29<sup>th</sup> of March, 2024

**Accepted on:** 30<sup>th</sup> of August, 2024

**Published on:** 30<sup>th</sup> of September, 2024

© Angginun Juwita Sari Harahap,  
Erlina, 2024

Angginun Juwita Sari Harahap,  
Magister, Department of Accounting,  
Faculty of Economics and Business,  
Universitas Sumatera Utara [University  
of North Sumatra], Indonesia.

Erlina, Dr., Head of Study Program  
Accounting, Department of  
Accounting, Faculty of Economics  
and Business, Universitas Sumatera  
Utara [University of North Sumatra],  
Indonesia. (Corresponding author)



This is an Open Access article,  
distributed under the terms of the  
[Creative Commons Attribution 4.0  
International license](https://creativecommons.org/licenses/by/4.0/), which permits  
unrestricted re-use, distribution, and  
reproduction in any medium, provided  
the original work is properly cited.

**Conflict of interest statement:**

Author(s) reported no conflict of interest

Angginun Juwita Sari Harahap (Indonesia), Erlina (Indonesia)

# EVALUATING THE IMPACT OF RISK MANAGEMENT AND RISK-BASED INTERNAL AUDIT ON FRAUD DETECTION IN LOCAL GOVERNMENTS

**Abstract**

One of the leading indicators for improving fraud detection capability is the evaluation of the implementation of risk management and risk-based internal audit and information technology systems. This study aims to evaluate how risk management and risk-based internal audits influence fraud detection capabilities in local government when integrated with information technology systems. SPSS 26 was utilized for data analysis. The paper uses a quantitative approach, collecting primary data with questionnaires distributed among 200 auditors and 70 supervisors across four districts in West Java. A purposive sampling approach based on self-selection was used. The findings show that the ability to detect fraud is significantly and positively influenced by the implementation of a risk-based internal audit (sig 0.000 < 0.05) and risk management process (sig 0.000 < 0.05). On the other hand, the risk management framework (sig 0.107 > 0.05) has a negative and insignificant effect on improving fraud detection capability. In addition, the relationships between the risk management process (sig 0.006 < 0.05) and fraud detection capability were found to be moderated by information technology systems. However, information technology systems are unable to moderate the relationship between risk-based internal audit (sig 0.563 > 0.05) and risk management framework (sig 0.115 > 0.05) on fraud detection capability. Therefore, risk management and risk-based internal audits are able to detect fraud, and information technology systems can strengthen the risk management process with the ability to detect fraud.

**Keywords**

risk management, risk-based internal audit, fraud,  
information technology, auditor

**JEL Classification**

G32, H83, L86, D81

**INTRODUCTION**

Fraud or deception seriously threatens the integrity, finances, and reputation of the public sector worldwide. Fraud cases can occur not only because of weaknesses in law enforcement but also because of a lack of supervision over financial management. Auditors' ability to conduct risk-based internal audits still needs to run optimally, and more training needs to be provided. One example of a fraud case that occurred in Bogor Regency was related to giving bribes to a team of auditors from the West Java Supreme Audit Agency so that the Bogor Regency regional government's financial report for the 2021 fiscal year received an Unqualified Opinion (UO). Apart from that, the fraud case was also conducted by the regional head of Bandung City along with eight other people in connection with the bribery case for procuring CCTV and internet service providers in the Bandung Smart City program. Indonesia Corruption Watch (ICW) assesses that cases of fraudulent buying and selling of UO predicates involving the internal Supreme Audit Agency have occurred repeatedly, and there have also been many cases of bribery within the Regional Government.

The main components of risk management consist of a framework, risk management principles, and risk management processes (International Organization for Standardization, 2018). Risk management and risk-based internal audit techniques significantly influence the detection of fraudulent activities (Atmanegara et al., 2021). Previous research examining the correlation between risk management, risk-based internal audit, and fraud detection capabilities has produced inconsistent results. Information technology systems influence fraud detection capabilities (Abu Kwaik et al., 2021; Wahid, 2021). Sudarmanto (2018) and Atmanegara et al. (2021) state that risk management and risk-based internal audit influence fraud detection capabilities, while the risk management framework with the workload is considered to have no significant influence on fraud detection capabilities (Erlina et al., 2018; Atmanegara et al., 2021). Based on the differences in research results from previous theoretical studies, it is necessary to search for further evidence and determine the influence of risk-based internal audits and risk management on fraud detection capabilities and the existence of information technology systems in the local government sector.

## 1. LITERATURE REVIEW

Risk management is a methodical and systematic approach to detecting, measuring, assessing attitudes toward, finding solutions, and monitoring and reporting dangers that occur in an activity or process. Another definition of risk management is an activity conducted to identify, analyze, and control risks that may occur in an activity or activities to obtain higher effectiveness and efficiency (Arief et al., 2021). In line with the previous definition, risk management is the process of identifying, analyzing, assessing, and responding to risks that threaten organizational goals, aiming to optimize opportunities and minimize threats (Pritchard, 2012). This process involves identifying, measuring, and controlling risks and financial problems faced by financial institutions (Hull, 2018). Risk management involves coordinating methods, activities, and processes used to manage organizational risks (International Organization for Standardization, 2018). By applying these components, an organization or institution can implement a systematic and structured approach to reduce and anticipate uncertainty. Risk management is an important thing for every government agency to implement in managing future risks.

Risk-based internal audit complements risk management to increase effectiveness in anticipating risks within an institution. The process links internal audits to a comprehensive organizational risk management framework (IIA, 2012). Risk-based internal audit is an audit method that prioritizes business risks and adjusts audit activities to assure management that critical risks have

been identified, evaluated, and managed appropriately (Pickett, 2016). This type of audit refers to an approach that views risk as a key factor in planning, implementing, and reporting audit results. It emphasizes careful risk assessment to determine the focus and depth of the audit (Reding, 2018). The main objective of a risk-based internal audit is to mitigate risk, proactively identify areas where danger may occur, and protect the company (Rustam, 2017). Elements that influence the success of implementing risk-based internal audits include the internal audit function, top management commitment, training, policy framework, and communication (Erlina et al., 2018). The application of a risk-based internal audit increases compliance and accountability, whereas increasing the level of company compliance with applicable regulations and standards by identifying areas that are vulnerable to violations and evaluating the effectiveness of internal controls in ensuring compliance (Nguyen, 2024). Apart from that, risk management impacts the willingness of internal auditors to report defects in risk procedures to the audit committee. However, a strong relationship with the audit committee does not appear to affect the willingness to report. The study also found that the majority of organizations have recently adopted (De Zwaan et al., 2011). Implementing a risk-based internal audit in the government sector can be a solution to detecting fraud.

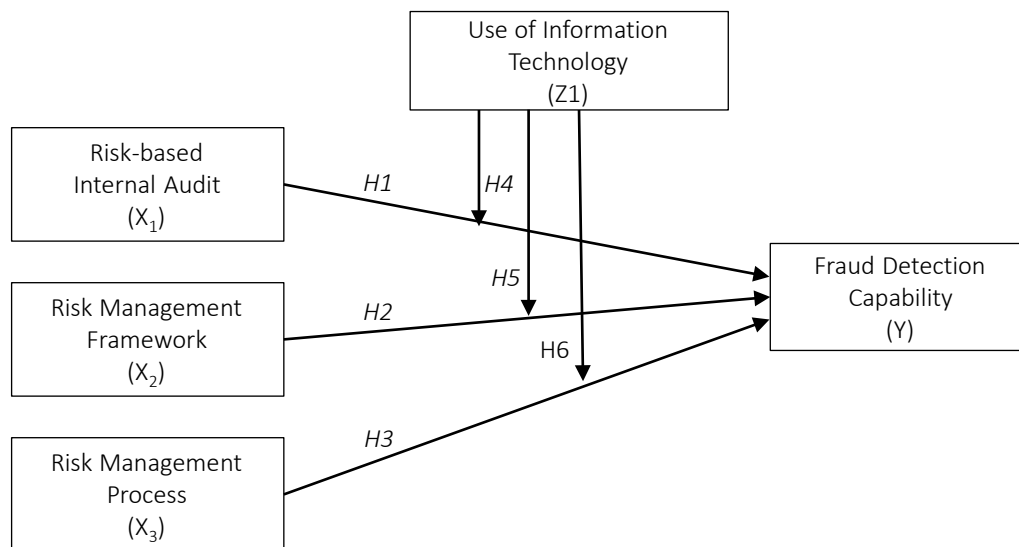
Evaluation in the application of risk management and risk-based internal audit can be related to the application of the concept of agency theory. An agency relationship is a contractual arrangement where one or more individuals (principals)

employ other individuals (agents) to perform a service on their behalf, which includes granting decision-making power to the agent (Jensen & Meckling, 1976). Agency theory is one of the basic theories in accounting, which analyzes the relationship between the principal, the owner of resources, and the agent, the manager of resources (Budiandru et al., 2022). Integration between risk management and risk-based internal audit can help strengthen the principles of agency theory by increasing supervision and control over manager behavior and increasing transparency and accountability in managing the risks faced by the organization (De Zwaan et al., 2011). By strengthening internal control systems and reducing uncertainty, risk management can help reduce agency conflicts between owners and managers in a company. By identifying, assessing, and managing potential risks, risk management can increase trust and accountability in agency relationships (Linda et al., 2021). The principal gives authority to the agent, hoping that the agent will act in the principal's interests. Conflicts often occur in this relationship as a result of differences in interests.

The regional government system has now been digitized to implement risk management and risk-based internal audits using information technology systems. Information technology systems currently support the progress of financial preparation and reporting. A system is a collection of two or more interconnected elements that interact to achieve goals (Romney & Steinbart, 2020). Meanwhile, information results from processing the data in question and is useful for its users (Suprpto et al., 2023). Furthermore, Williams and Sawyer (2010) stated that information technology is a broad term that includes any technology used to create, process, store, communicate, and transmit information. In general, an information technology system combines hardware, software, network infrastructure, and technology to collect, process, store, and disseminate data useful in business and organizational environments (K. C. Laudon & J. P. Laudon, 2020). Another definition of an information technology system is a series of tools, procedures, and methods designed to produce useful information for management and organizations to achieve their goals (Rainer & Cegielski, 2018).

Regional governments in Indonesia use an information technology system called the Regional Development Information System (RDIS) to implement regional development, especially regarding the willingness to analyze development planning and mapping in looking at the influence of information technology in achieving organizational goals in line with the technology acceptance model (TAM). The technology acceptance model (TAM) is a framework used to assess user acceptance and satisfaction with information technology solutions (Emilia & Ravi, 2021). TAM is a strong guide in explaining the factors influencing user behavior and using various technologies (Putri et al., 2023). Implementing risk management and risk-based internal audits through information technology systems will increase the ability to detect fraud if implemented well.

Many frauds occur because of the pressure of existing opportunities and the (generally accepted) justification for the action. Fraud refers to intentional illegal actions carried out by individuals inside or outside an organization; these actions aim to manipulate or provide false reports to others to gain personal or group benefits while causing losses to other parties either directly or indirectly (ACFE, 2016). Fraud is classified into three forms: misuse of assets, financial statement fraud, and corruption (ACFE, 2016). Fraud in the government sector includes actions that aim to obtain personal benefits or harm other parties illegally, violate public trust and ethics, and violate laws or organizational policies (ACFE, 2019). Meanwhile, the explanation of fraud in the government sector refers to all actions involving abuse of power or position within a government entity to obtain personal gain or harm the public interest (Vona, 2018). In line with this definition, fraud in the government sector involves dishonest, manipulative, or deceptive practices aimed at taking illegal advantage of public resources or harming the interests of society (Minahan, 2017). Fraud in the government environment is characterized by violations committed by individuals at various levels of authority, including leaders and other officials. Every government agency must have rules for running government and financial reporting. In the fraud triangle theory, it is explained that fraud is the result of the interaction between three main factors, namely pressure, opportunity, and rationalization. When these three factors are present in the



**Figure 1.** Conceptual framework

same situation, the risk of fraud increases significantly (Wells, 2004). This statement aligns with the definition presented by the Association of Certified Fraud Examiners (ACFE). The fraud triangle theory is a concept that states that three main factors, namely pressure, opportunity, and rationalization, are often present together to motivate someone to commit fraud (ACFE, 2019).

In the context of regional government financial management, the integration of risk management, including a risk management framework, risk management process, and internal risk management, is crucial. The advent of digitalization, facilitated by technology systems, represents a novel approach to fraud detection in the local government sphere. This study, therefore, seeks to delve into the factors that enhance fraud detection through risk management evaluations and risk-based internal audits, leveraging information technology systems in local governments.

Based on the conceptual framework (Figure 1), the study suggested the following hypotheses:

- H1: Risk-based internal audit has a significant influence on fraud detection capabilities.*
- H2: Risk management framework has a significant influence on fraud detection capabilities.*
- H3: Risk management process has a significant influence on fraud detection capabilities.*

*H4: Information technology systems moderate the relationship between risk-based internal audit and fraud detection capabilities.*

*H5: Information technology systems moderate the relationship between risk management frameworks and fraud detection capabilities.*

*H6: Information technology systems moderate the relationship between risk management processes and fraud detection capabilities.*

## 2. METHOD

This study uses a quantitative methodology to determine the influence of one variable on another. The ability to detect fraud is the dependent variable. Independent variables include risk-based internal audit, risk management framework, and risk management process. The moderating variable is the application of information technology systems. Multiple linear analysis methods were employed using SPSS v26. Regression analysis measures the strength of the relationship between two or more variables and reveals the relationship between dependent and independent variables (Ghozali, 2013).

This paper focused on the population of 27 districts/cities in West Java Province. This study uses non-probability sampling, namely the purposive sampling method. The criteria used for the sample are as follows:

1. Districts/cities that have fraud problems.
2. Districts/cities with the largest area.
3. Districts/cities with the largest population.

Therefore, this analysis was conducted in four districts/cities in West Java Province: Bogor Regency, Garut Regency, Bekasi City, and Bandung City. The data source comes from primary data by distributing questionnaires among 200 auditors and 70 supervisors of local government affairs organizers (PPUD) spread across four districts/cities in West Java Province. Respondents included main auditors, middle auditors, young auditors, first auditors, and advanced executing auditors. Respondents from supervisors of local government affairs consisted of intermediate PPUD, young PPUD, and first PPUD. In the working area of the regional inspectorate of Bogor Regency, there are 47 auditors and 22 PPUD; the regional inspectorate of Bekasi City has 55 auditors and 10 PPUD; the regional inspectorate of Bandung City has 50 auditors and 16 PPUD, and the regional inspectorate of Garut Regency has 43 auditors and 27 PPUD.

Data were also obtained from secondary data in the form of documents related to risk management implemented by local governments. In testing the data, a classical assumption test was carried out as a statistical requirement that must be met in multiple linear regression analysis to provide certainty regarding the accuracy of the data, unbiased and consistent. The classic assumption test consists of the normality, multicollinearity, and heteroscedasticity tests. Hypothesis analysis was conducted using the *T*-test statistics to evaluate the impact of independent variables on related variables, either individually or partially. This test was conducted using a significance level of 5%, which shows that if the variable relationship is below 0.05, it is declared to have a significant effect and vice versa. Furthermore, the coefficient of determination test ( $R^2$ ) is an important measure in linear regression, which indicates how well the model can explain variations in the dependent variable (Wooldridge, 2019). The moderating variable test is conducted to determine how much power the moderating variable has for the relationship between the independent and dependent variables, with a significance level of 5%.

Variable measurement was conducted using a Likert scale ranging from strongly disagree (score 1) to strongly agree (score 5). The risk-based internal audit variable indicators are internal audit function, top management commitment, development training, policy framework, and communication process. The risk management framework indicators consist of leadership and commitment, integration, framework design, implementation, evaluation, and improvement. Risk management process indicators consist of communication and consultation, determining context, risk identification, risk analysis, risk evaluation, risk treatment, and monitoring and review. Indicators for information technology systems consist of the benefits, use of technology systems, ease of use, effectiveness of technology systems, and application security. Meanwhile, indicators of fraud detection capability consist of using technology systems to detect fraud, government performance, good corporate governance, pressure in detecting fraud, opportunities, capabilities, and the level of fraud occurrence.

### 3. RESULTS

This study targeted 200 auditors and 70 supervisors of regional government affairs in four regencies/cities in West Java, Indonesia: Bogor Regency, Garut Regency, Bekasi City, and Bandung City. Data processing was conducted via SPSS by first conducting descriptive statistics to determine the accuracy of the existing data.

Based on the results of descriptive statistical tests in Table 1, risk-based internal audit has an average value of 33.96%, risk management framework has an average value of 34.04%, and risk management has an average value of 33.43%. In comparison, a moderating variable (implementation of information technology systems) has an average value of 28.99%, while the ability to detect fraud has an average value of 33.76%.

Next, a classical assumption test was carried out to test the quality of the research data as a requirement for conducting multiple linear regression analysis in the normality test to see whether the residual value is normal. The normality test was carried out using the one-sample Kolmogorov-Smirnov test.

**Table 1.** Descriptive statistics

Model		Risk-based Internal Audit	Risk Management Framework	Risk Management Process	Implementation of Information Technology System	Fraud Detection Capability
N	Valid	270	270	270	270	270
	Missing	0	0	0	0	0
Mean		33.96	34.04	33.43	28.99	33.76
Std. Deviation		4.675	4.035	4.438	5.356	5.850
Variance		21.857	16.285	19.696	28.688	34.221

**Table 2.** Normality test

One-Sample Kolmogorov-Smirnov Test			Unstandardized Residuals
N			270
Normal Parameters <sup>b</sup>	Mean		.0000000
	Std. Deviation		3.21895619
Most Extreme Differences	Absolute		.197
	Positive		.189
	Negative		-.197
Statistical Tests			.197
Asymp. Sig. (2-tailed)			.200 <sup>c</sup>

Note: a. Test distribution is Normal. b. Calculated from data. c. Lilliefors Significance Correction.

According to the Kolmogorov-Smirnov test criteria, if the significance is  $> 0.05$ , then the data will be normally distributed, and vice versa. The normality test (Table 2) results show that the data are normally distributed, namely a significance value of  $0.200 > 0.05$ .

After the normality test in the classical assumption, there is a multicollinearity test to determine whether the independent variables are correlated in the regression model. If the tolerance value is  $> 0.10$  and  $VIF < 10$ , the study has no multicollinearity. If the tolerance value is  $< 0.10$  and  $VIF > 10$ , there is multicollinearity interference. Table 3 shows no multicollinearity in this study because all variables have tolerance values  $> 0.10$  and  $VIF < 10$ .

After the multicollinearity test, the study determined whether there was an inequality in the variance of the residuals in the regression model through the heteroscedasticity test. The heteroscedasticity test was conducted using Spearman's rho test by correlating the residual value (unstandardized residual) with each independent variable. If the correlation is significant  $> 0.05$ , there is no heteroscedasticity problem, and vice versa. Table 4 shows that heteroscedasticity does not occur because the significance value is  $0.179 > 0.05$ , then  $0.069 > 0.05$ , and  $0.059 > 0.05$ .

The next step is the *T*-test to evaluate the impact of independent variables, both individually and partially, on related variables. This test was carried

**Table 3.** Multicollinearity test

Model		Coefficients <sup>a</sup>					Collinearity Statistics	
		Unstandardized Coefficients		Standardized Coefficients	T	Sig.	Tolerance	VIF
		B	Std. Error	Beta				
1	(Constant)	-2.732	1.714		-1.594	.112		
	Risk-Based Internal Audit	.783	.081	.626	9.629	.000	.269	3.713
	Risk Management Framework	-.141	.087	-.097	-1.618	.107	.317	3.152
	Risk Management Process	.439	.077	.333	5.684	.000	.332	3.013

Note: a. Dependent Variable: Fraud Detection Ability.

**Table 4.** Heteroscedasticity test

		Correlations				
Model			Risk-Based Internal Audit	Risk Management Framework	Risk Management Process	Unstandardized Residuals
Spearman's rho	Risk-Based Internal Audit	Correlation Coefficient	1.000	.779**	.729**	.082
		Sig. (2-tailed)	.	.000	.000	.179
		N	270	270	270	270
	Risk Management Framework	Correlation Coefficient	.779**	1.000	.670**	.111
		Sig. (2-tailed)	.000	.	.000	.069
		N	270	270	270	270
	Risk Management Process	Correlation Coefficient	.729**	.670**	1.000	-.126*
		Sig. (2-tailed)	.000	.000	.	.059
		N	270	270	270	270
	Unstandardized Residuals	Correlation Coefficient	.082	.111	-.126*	1.000
		Sig. (2-tailed)	.179	.069	.039	.
		N	270	270	270	270

Note: \*\*. Correlation is significant at the 0.01 level (2-tailed). \*. Correlation is significant at the 0.05 level (2-tailed).

out using a significance level of 5%. If the variable *T*-test value is <0.05, it is declared to have a significant effect and vice versa.

Table 5 shows that a risk-based internal audit has a coefficient value of 0.783, which is positive. It shows that increasing the implementation of risk-based internal audits will increase the ability to detect fraud. Apart from that, a significance value of 0.000 < 0.05 indicates a positive and statistically significant influence. Therefore, hypothesis 1 is accepted.

Furthermore, the risk management framework has a negative coefficient value of -0.141. This shows that implementing a risk management framework does not positively impact increasing fraud detection capabilities. The *p*-value of

0.107 > 0.05 indicates that there is no statistically significant effect. Therefore, hypothesis 2 is rejected.

Risk management process has a coefficient value of 0.439, which is positive. It shows that improving the risk management process will increase the ability to identify fraud. A *p*-value of 0.000 < 0.05 indicates a statistically significant and positive effect. Therefore, hypothesis 3 is accepted.

The next statistical test is the coefficient of determination test. The coefficient of determination in regression analysis measures the proportion of variance in the dependent variable that the independent variable can explain. In this case, it can show how much the variable can explain its impact.

**Table 5.** Hypotheses results

Model	Unstandardized Coefficients		Standardized Coefficients	t	Sig.
	B	Std. Error	Beta		
(Constant)	-2.732	1.714		-1.594	.112
1 Risk-based Internal Audit	.783	.081	.626	9.629	.000
Risk Management Framework	-.141	.087	-.097	-1.618	.107
Risk Management Process	.439	.077	.333	5.684	.000

Note: Dependent Variable: Fraud Detection Ability.

**Table 6.** Coefficient of determination

Model	R	R Square	Adjusted R-Square	Std. Error of the Estimate
1	.835a	.697	.694	3.237

Note: Predictors: (Constant), Risk Management Process, Risk Management Framework, Risk-Based Internal Audit, b Dependent Variable: Fraud Detection Ability.



**Table 7.** Moderation test results

Model	Unstandardized Coefficients		Standardized Coefficients	t	Sig.
	B	Std. Error	Beta		
(Constant)	-7.755	8.096		-.958	.339
Risk-based Internal Audit	.532	.344	.425	1.547	.123
Risk Management Framework	-.699	.390	-.482	-1.794	.074
Risk Management Process	1.312	.332	.996	3.950	.000
1 Implementation of Information Technology System	.251	.326	.229	.769	.443
RBIA – Application of STI	.008	.013	.322	.579	.563
STI Framework – Application	.024	.015	.903	1.581	.115
Risk Management Process – Application of STI	-.036	.013	-1.437	-2.748	.006

Note: Dependent Variable: Fraud Detection Ability.

Table 6 shows that the R-square value is 0.697, thus indicating that the combined influence of risk-based internal audit, risk management framework, and risk management process on fraud detection capability is equal to 69.7%. The remaining 30.3% is caused by other independent variables not regarded in this study.

The next test is to check the moderation between the variables. Moderating variables are measured to see the variable’s ability to strengthen or weaken the relationship between the independent and dependent variables. A hypothesis is considered to strengthen the relationship between the variables if the statistical value is <0.05 and vice versa.

Table 7 shows that the application of information technology systems only moderates the risk management process on the ability to detect fraud with a significant value of 0.006 < 0.05, which means that the application of information technology systems strengthens the relationship between the risk management process and the ability to detect fraud. Therefore, hypothesis 6 is accepted.

Meanwhile, implementing information technology systems does not moderate risk-based internal audits on fraud detection capabilities because the significant value is 0.563 > 0.05. So, hypothesis 4 is rejected. Furthermore, implementing information technology systems does not moderate the

risk management framework on fraud detection capabilities with a significant value of 0.115 > 0.05, rejecting hypothesis 5.

Table 8 shows the coefficient of the determination test, which combines the independent variable, dependent variable, and moderating variable. The R-square value is 0.715, indicating that the combined influence of the variables is 71.5%. The remaining 28.5% is caused by other independent variables. The ability to explain a variable increases from 69.7% to 71.5%.

Therefore, from the results of the hypothesis testing carried out, the results show that Hypothesis 1 (H1), hypothesis 3 (H3) and hypothesis 6 (H6) can be accepted because they have a positive and significant effect, while for hypothesis 2 (H2), hypothesis 4 (H4) and hypothesis 5 (H5) are rejected because they have a negative and insignificant effect.

## 4. DISCUSSION

The results are helpful for detecting fraud in the government sector. The study evaluated risk-based internal audit, risk management framework, risk management process, and information technology systems. After conducting descriptive statistical tests, which is then continued with the classic

**Table 8.** Coefficient of determination test results

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.845a	.715	.707	3.167

Note: Predictors: (Constant), Risk Management Process – STI Implementation, Risk Management Framework, Risk Management Process, Risk-Based Internal Audit, Information Technology System Implementation, RBIA – STI Implementation, Framework – STI Implementation b. Dependent Variable: Fraud Detection Ability.

assumption test to determine the quality of the data, the data are normally distributed and the study can start the regression analysis stage.

Based on the results of hypotheses testing, risk-based internal audits have a fairly large and positive influence on the ability to identify fraud. It is in line with Atmanegara et al. (2021), Erlina et al. (2018), and Erlina et al. (2021). Research findings show that implementing risk management and risk-based internal audit has a noteworthy impact on identifying fraudulent activities. Focusing on risk-prone areas increases effectiveness in detecting risks. It is directly related to agency theory because internal audits act as a control that can reduce agency problems. Apart from that, increasing the competency and skill of auditors as the implementation of risk-based audits is considered important for developing auditor skills and competence. It is in line with the results of direct interviews, and it was stated that the implementation of risk-based internal audits could have been more successful due to a lack of auditor training. This training can develop the competence of auditors in the future, so implementing risk-based internal audits can increase supervision effectiveness, reduce losses due to fraud, strengthen corporate governance, and increase public and stakeholder trust.

Next, the risk management framework is an important element in fraud detection. However, the findings from the hypothesis testing show that the risk management framework does not influence the competency to identify fraud. The results align with Nugroho and Wiwik (2021) and Kwaik et al. (2023). Respondents considered that a framework is indeed needed in an institutional unit. However, it must also be adapted to human resource conditions, and the principles must be accompanied by strong commitment. The effectiveness of implementing a risk management framework will be limited if it is not implemented and appropriately focused. The risk management framework must continue to be improved to assess the extent to which human resources are prepared to face future pressures in detecting fraud. It will help overcome agency problems and increase public and stakeholder trust in the government. The implications require the government to expand the focus on risk management and, more specifically, strengthen the process of implementing an effective

framework, comprehensive monitoring, and a strong organizational culture.

The risk management process has a vital role in improving the ability to detect fraud because its indicators are very complex. Based on the results of hypothesis testing, the risk management process positively and significantly influences the ability to identify fraud. The results are in line with Haddad (2023), Sudarmono (2020), and Agus and Budi (2021). Respondents consider that good communication in the risk management process will also influence other elements in the risk management process. An effective risk management process allows companies to identify, assess, and manage fraud risks better. A strong monitoring mechanism can help overcome agency problems, thereby ensuring that auditors act according to common interests and goals. The risk management process runs well and impacts fraud detection capabilities due to comprehensive risk identification, structured risk assessment and prioritization, strong internal control, and continuous monitoring. A strong risk management process will improve government financial governance, reduce financial and reputational losses, strengthen public trust, and increase the operational efficiency of the audit process.

Information technology systems are currently important to implement in regional financial management in line with the development of digitalization. The regional development information system, run by all relevant inspectorates, is important in monitoring financial reporting. Based on the results of hypotheses testing, information technology systems can only strengthen the relationship between risk management processes and the ability to detect fraud. It is in line with the components of the risk management process because monitoring and review can be conducted through the system. Respondents acknowledged that having an information technology system would help risk management. The results are in line with Monteiro et al. (2022), Candra et al. (2019), and Wahid (2021). By utilizing information technology, organizations can increase effectiveness and efficiency in identifying and managing risks and detecting and preventing fraud. It reduces agency problems, strengthens corporate governance, and increases stakeholder confidence. Information technology systems can detect anomalies and behavioral patterns through data analytics.

Meanwhile, implementing information technology systems cannot moderate the relationship between risk-based internal audit and management frameworks on fraud detection capabilities. Although information technology can potentially improve risk-based internal audit processes and risk management, this is only sometimes the case in practice. Sub-optimal implementation, lack of training, resistance to change, and an unbalanced

focus between technical and process aspects can hinder the effectiveness of information technology in moderating this relationship. The results show the importance of reevaluating technology implementation, increasing supporting technology training, overcoming resistance to change, and focusing on auditor processes and culture to improve information technology systems in moderating the relationships to improve fraud detection.

---

## CONCLUSION

The purpose of this study was to evaluate risk management and risk-based internal audits with information technology systems in detecting fraud in local governments. This study shows that the evaluation results of the application of risk management and risk-based internal audit can detect fraud and then, with the application of information technology systems, can strengthen the risk management process with the ability to detect fraud. Implementing a risk-based internal audit methodology and using risk management techniques is expected to improve the efficiency and effectiveness of financial management and the detection of fraudulent activities. The application of risk-based internal audit has a positive impact on improving the ability to detect fraud. This shows that a risk-focused approach allows auditors to be more effective in identifying areas that have high fraud potential. By prioritizing audits in areas most susceptible to risk, auditors can more quickly and accurately detect signs of fraud. Risk management in terms of the risk management framework has a negative effect on the ability to detect fraud, which shows that the more stringent or complex the risk management framework can actually reduce its effectiveness in detecting fraud. This happens because risk management processes that are too bureaucratic or rigid can blur the focus on identifying potential fraud or make organizations more confident that risks are well managed, thereby reducing vigilance against fraud.

Furthermore, information technology systems are able to improve the ability to detect fraud with this risk management relationship indicating that the integration of information technology with risk management processes allows organizations to monitor and analyze data more effectively and in real-time. Information technology enables the automation of risk monitoring and anomaly detection processes, which accelerates the identification of potential fraud. Meanwhile, information technology systems cannot moderate the relationship between risk-based internal audits and the ability to detect fraud. This shows that although information technology can improve the efficiency and effectiveness of the audit process, it does not automatically strengthen or affect the relationship between risk-based internal audit and the ability to detect fraud. This may be because other factors, such as the quality of risk-based audit implementation, auditor competence, or management policies, have a more dominant role in detecting fraud.

The findings of this study are useful for local government policymakers who want to understand the significance of implementing and refining risk management frameworks and risk-based internal audits. By understanding the positive and negative impacts of these approaches, they can design more effective policies to detect and prevent fraud. In addition, the findings can improve the internal control system by enhancing the internal control system implemented, especially in the integration of information technology with risk management. The findings are also useful in developing risk management strategies that not only focus on compliance but also on effectiveness in detecting potential fraud. Based on these findings, a more adaptive and less bureaucratic strategy can be developed.

Future research should look for other variables that could be used, such as workload, training, and other factors. In addition, the samples used can be increased to get maximum results.

## AUTHOR CONTRIBUTIONS

Conceptualization: Angginun Juwita Sari Harahap, Erlina.  
 Data curation: Angginun Juwita Sari Harahap, Erlina.  
 Formal analysis: Angginun Juwita Sari Harahap, Erlina.  
 Funding acquisition: Angginun Juwita Sari Harahap, Erlina.  
 Investigation: Angginun Juwita Sari Harahap, Erlina.  
 Methodology: Erlina.  
 Project administration: Angginun Juwita Sari Harahap.  
 Resources: Angginun Juwita Sari Harahap, Erlina.  
 Software: Angginun Juwita Sari Harahap, Erlina.  
 Supervision: Angginun Juwita Sari Harahap, Erlina.  
 Validation: Angginun Juwita Sari Harahap, Erlina.  
 Writing – original draft: Angginun Juwita Sari Harahap, Erlina.  
 Writing – review & editing: Angginun Juwita Sari Harahap, Erlina.

## ACKNOWLEDGMENT

The authors would like to thank the University of North Sumatra, especially the Research Institute, for its support and the Ministry of Education and Research through the Directorate of Research, Technology, and Community Service program for providing intellectual assistance and funding for this project in the PMDSU grant (number: 91/UN5.4.10.S/PPM/KP-DRTPM/2024).

## REFERENCES

1. Abu Kwaik, N., Sweis, R., Allan, B., & Sweis, G. (2023). Factors affecting risk management in industrial companies in Jordan. *Administrative Sciences*, 13(5), Article 132. <https://doi.org/10.3390/admsci13050132>
2. Agus, S., & Budi, Y. (2021). The influence of internal control, risk management and whistleblowing systems on fraud prevention. *Journal of Internal Control, Risk Management and Information Systems*, 7(2), 112-125. Retrieved from <https://jurnal.stie-aas.ac.id/>
3. Arief, B., Putra, R. G., Meidawati, N., & Puspaningsih, A. (2021). The influence of internal audit, motivation, and work environment on employee performance. *Journal of Contemporary Accounting*, 3(3), 150-161. <https://doi.org/10.20885/jca.vol3.iss3.art4>
4. Association of Certified Fraud Examiners (ACFE). (2016). *Fraud examiner's guide (International edition)*. Austin, TX: Association of Certified Fraud Examiners. Retrieved from [https://www.fraud-](https://www.fraud-magazine.com/products.aspx?id=4294992609&terms=Sample%20fraud%20report)
5. Association of Certified Fraud Examiners (ACFE). (2019). *Fraud examiner's manual*. Austin, TX: Association of Certified Fraud Examiners. Retrieved from <https://www.acfe.com/training-events-and-products/books-and-manuals>
6. Atmanegara, A. W., Erlina, Muda, I., & Adnans, A. A. (2021). Can the risk management implementation intensify the internal auditor expertise finding risk in local government? *Webology*, 18(Special Issue), 646-653. <http://dx.doi.org/10.14704/WEB/V18SI05/WEB18252>
7. Budiandru, Z., Nur, B., Abbas, Y. E., & Febrina, I. (2022). Detecting fraud financial statements in manufacturing companies Indonesia. *JEMASI: Jurnal Ekonomi Manajemen dan Akuntansi*, 18(2). Retrieved from <http://ejournal.iba.ac.id/index.php/jemasi>
8. Candra, R. M., Sari, Y. N., Iskandar, I., & Yanto, F. (2019). Information technology asset security risk management system using ISO 31000:2018. *Jurnal CoreIT*, 5(1).
9. De Zwaan, L., Stewart, J. D., & Subramaniam, N. (2011). Internal audit involvement in enterprise risk management. *Managerial Auditing Journal*, 26(7), 586-604. <https://doi.org/10.1108/02686901111151323>
10. Emilia, F. M., & Ravi, S. (2021). Analysis of the influence of perceived usefulness, perceived ease of use and attitude toward using technology on actual to use halodoc application using the technology acceptance model (TAM) method approach. *International Research Journal of Advanced Engineering and Science*, 6(1), 135-140. Retrieved from <https://irjaes.com/wp-content/uploads/2021/01/IRJAES-V6N-1P101Y21.pdf>
11. Erlina, E., Nasution, A. A., Yahy, I., & Atmanegara, A. W. (2021). The role of risk-based internal audit in improving audit quality. *Manage-*

- ment *Journal International*, 11(12), 299-310. Retrieved from [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=3785747](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3785747)
12. Erlina, Putri, D. R., Sopanah, & Muda, I. (2018). Model of successful implementation of risk-based internal audit in regencies/cities in North Sumatra. *International Journal of Civil Engineering and Technology*, 9.
  13. Ghozali, I. (2013). *Multivariate analysis application with the IBM SPSS 21 program*. Semarang: Diponegoro University Publishing Agency.
  14. Haddad, H. (2023). Implementing risk management in local government: An exploratory case study of Moroccan cities. *International Journal of Organizational Analysis*, 31(1), 23-37. <https://doi.org/10.18488/74.v10i1.3320>
  15. Hull, J. C. (2018). *Risk management and financial institutions*. Wiley.
  16. Indonesia Corruption Watch. (2022). *Performance evaluation report of the Corruption Eradication Commission for the 2019–2024 period*. Retrieved from <https://icw.or.id/ZJcr>
  17. International Organization for Standardization. (2018). *ISO 31000:2018 Risk Management – Guidelines*. Geneva. Retrieved from <https://www.iso.org/obp/ui/#iso:std:iso:31000:ed-2:v1:en>
  18. 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](https://doi.org/10.1016/0304-405X(76)90026-X)
  19. Laudon, K. C., & Laudon, J. P. (2020). *Management information systems: Managing the digital firm*. Pearson.
  20. Linda, A., Kwat, W. J., Niswah, B., Widiarto, A., & Manurung, P. N. (2021). Can the risk management committee improve riskmanagement disclosure practices in Indonesian companies?. *Investment Management and Financial Innovation*. [https://doi.org/10.21511/imfi.18\(3\).2021.19](https://doi.org/10.21511/imfi.18(3).2021.19)
  21. Minahan, T. P. (2017). *Fraud and corruption in public services*. CRC Press.
  22. Monteiro, P. A., Vale, J., Leite, E., Lis, M., & Kurowska-Pysz, J. (2022). The impact of information systems and non-financial information on company success. *International Journal of Accounting Information Systems*, 45. <https://doi.org/10.1016/j.acinf.2022.100557>
  23. Nguyen, N. K. D. (2024). Factors affecting risk-based audit and quality audit. *Emerging Science Journal*, 8(3), Article 957. <https://doi.org/10.28991/ESJ-2024-08-03-010>
  24. Nugroho, L., & Wiwik, U. (2021). Internal control and risk management issues on the sustainability of micro and small enterprises in Indonesia. *BİLTÜRK Journal of Economics and Related Studies*. <http://dx.doi.org/10.47103/bil-turk.993568>
  25. Pickett, K. H. S. (2016). *The internal auditing handbook*. Wiley.
  26. Pritchard, C. L. (2012). *Risk management: Concepts and guidance*. CRC Press.
  27. Putri, L.T., Aini, A. P. N., Solekah, N. A., & Istiqomah, D. F. (2023). Exploring e-commerce adoption in small and medium enterprises (SMEs) using the technology acceptance model. *International Journal of Business Economics (IJBE)*, 5(1), 1-14. <https://doi.org/10.30596/ijbe.v5i1.16262>
  28. Rainer, Jr., R. K., & Cegielski, C. G. (2018). *Management information systems: Managing digital organizations*. Wiley.
  29. Reding, K. F. (2018). *Internal auditing: Assurance & consulting services*. South-Western Cengage Learning.
  30. Romney, M. B., & Steinbart, P. J. (2020). *Accounting information systems* (15<sup>th</sup> ed.). Upper Saddle River, NJ: Pearson.
  31. Rustam, B. R. (2017). *Risk management*. Jakarta: Salemba Empat.
  32. Sudarmanto, E. (2020). Risk management: Early detection of fraud prevention efforts. *Journal of Business Management*, 15(2), 78-89. <https://doi.org/10.32502/jimn.v9i2.2506>
  33. Suprpto, K., Nadirsyah, & Darwanis. (2023). Determinations of fraud in local governments in the Province of Aceh. *International Journal of Current Science Research and Review*, 6(11), 7329-7337. <https://doi.org/10.47191/ijcsrr/V6-i11-38>
  34. The Institute of Internal Auditors (IIA). (2012). *Practice guide: Internal audit and risk management*. IIA. Retrieved from [https://iia-indonesia.org/files/magazine/Majalah\\_IA\\_Aug2016.pdf](https://iia-indonesia.org/files/magazine/Majalah_IA_Aug2016.pdf)
  35. Vona, L. W. (2018). *Fraud risk assessment: Building a fraud audit program*. Wiley.
  36. Wahid, W. A. (2021). Review analysis of the uses of information systems at PT Pertamina. *Journal of Information Technology and Computer Engineering*, 2(2). <https://doi.org/10.37148/bios.v2i2.20>
  37. Williams, A., & Sawyer, S. (2010). *Using information technology: A practical introduction to computers & communications* (8<sup>th</sup> ed.). New York, NY: McGraw-Hill.
  38. Wooldridge, J. M. (2019). *Introductory econometrics: A modern approach* (7<sup>th</sup> ed.). Boston, MA: Cengage Learning.