

The Role of Risk-Based Internal Audit in Improving Fraud Detection Capability: Moderation of Information Technology Systems In The Central Maluku Regency Government

Jefry Gasperz¹, Pranatalindo Simanjuntak^{2*}, Sari Tamayani Tjio³, Christy Clayde Latuperissa⁴

^{1,2,3,4}Department of Accounting, Pattimura University, Ambon, Indonesia
Email: franssimanjuntak71@gmail.com^{2*}

Abstract

This study examines the impact of Risk-Based Internal Auditing (RBIA) on fraud detection (FD) capabilities and investigates the moderating role of Information Technology Systems (ITS) in this relationship. Fraud remains a significant challenge in public sector financial management particularly within local governments, where geographical dispersion and resource constraints can hinder effective oversight. A quantitative survey approach was employed, involving 32 Government Internal Supervisory Apparatus (APIP) auditors from the Central Maluku Regency Inspectorate. Data were analyzed using Partial Least Squares Structural Equation Modeling (PLS-SEM). The results indicate that RBIA influences FD ($\beta = 0.448$, $p < 0.001$), and ITS also impacts FD ($\beta = 0.352$, $p < 0.001$). Furthermore, the interaction between RBIA and ITS significantly affects FD ($\beta = 0.170$, $p < 0.001$), suggesting that ITS strengthens the relationship between RBIA and fraud detection capabilities. These findings imply that integrating risk-based auditing with robust information technology can enhance the ability of local government auditors to identify potential fraud. The study offers practical insights for local governments in archipelagic regions, where geographical fragmentation and operational constraints necessitate audit approaches supported by effective information technology systems. The findings highlight the importance of strengthening both risk-based audit practices and technological capacity to improve fraud oversight and accountability within local government.

Keywords: *fraud detection capability; information technology system; local government; risk based internal audit*

INTRODUCTION

Fraud remains a major problem in public sector governance because it can undermine accountability, transparency, and public trust. The increasing complexity of government financial management, coupled with decentralization and the development of digital technology, also increases the risk of various forms of fraud. In many countries, fraud in the public sector often occurs due to weak internal control systems, ineffective oversight, and limited organizational capacity to detect new risks. Therefore, strengthening

the internal audit function is a crucial step for public agencies to improve governance and enhance their ability to detect fraud (Nadirsyah et al., 2024).

In recent years, the internal audit function has undergone significant changes, from simply ensuring compliance to a strategic role supporting governance, risk management, and value creation for the organization. This shift has driven the adoption of Risk-Based Internal Auditing (RBIA), an approach that focuses audit resources on areas with the highest risk

levels. Unlike traditional auditing, RBIA enables auditors to be more proactive in detecting control weaknesses and potential fraud before they cause significant losses. Modern internal audit literature indicates that RBIA contributes to improving the effectiveness of risk management and strengthening the overall quality of organizational oversight (Handoyo, 2024).

The theoretical basis for explaining the relationship between internal audit and fraud detection capability can be explained through Agency Theory. This theory states that fraud can occur when an agent has more information than the principal and acts in their own personal interests that are not aligned with the principal's goals. In the public sector, government officials act as agents who manage public resources on behalf of the public. Information gaps and weak oversight can open up opportunities for opportunistic actions that increase the risk of fraud. Therefore, effective internal audit is a crucial mechanism for mitigating agency problems and strengthening organizational accountability (Nadirsyah et al., 2024).

Previous empirical studies have shown that the implementation of risk-based auditing has a positive impact on fraud prevention and detection (Al-Hajaya, 2019; Le et al., 2020). Harahap and Erlina (2024) found that risk-based internal auditing can improve fraud detection capabilities in Indonesian local governments because auditors can focus more on high-risk areas and strengthen risk mitigation efforts (Zahra, 2025). These findings suggest that the systematic identification and assessment of risks under RBIA can enhance auditors' ability to recognize irregularities and

potential fraudulent activities. Accordingly, the following hypothesis is proposed:

H1: Risk-Based Internal Audit has a positive effect on fraud detection capability.

Similarly, various studies on public sector governance also show that an effective internal audit function plays a crucial role in preventing fraud, strengthening internal control, and improving governance quality. These research findings confirm that RBIA is increasingly becoming a crucial instrument in strengthening accountability in the public sector (Harahap & Erlina, 2024).

The effectiveness of RBIA in fraud detection is increasingly supported by information technology. Integrated systems, digital governance, big data, and audit analytics enable real-time data access, process automation, anomaly detection, and comprehensive risk assessment, thereby strengthening audit quality and oversight effectiveness (Sidauruk, 2024).

The relevance of technology use in auditing can be explained through the *Technology Acceptance Model* (TAM), which states that individuals are more likely to accept technology if it is perceived as useful and easy to use. In the audit context, the use of technology helps auditors process large amounts of data, detect unusual transaction patterns, and support evidence-based decision-making. (Lowe et al., 2018; Manita et al., 2020). Recent research also indicates that the use of data analytics can improve fraud prevention and detection capabilities among Government Internal Supervisory Apparatus (APIP), particularly in environments characterized by complex financial transactions and extensive operational activities. Based on this

theoretical and empirical argument, the following hypothesis is proposed:

H2: Information Technology Systems have a positive effect on fraud detection capability.

Recent research also shows that the use of data analytics can improve fraud prevention and detection capabilities in the Government Internal Supervisory Apparatus (APIP), especially in environments with complex financial transactions and extensive operational activities (Lowe et al., 2018).

Limitations in previous literature lie in the context of research, which has been largely conducted in the private sector, state-owned enterprises, or local governments with relatively uniform geographic conditions. Research addressing local governments in island regions is still very limited, even though such regions face specific challenges in the form of wide geographical distribution, limited transportation, and uneven technological infrastructure, which can impact audit and oversight effectiveness. Central Maluku Regency serves as an important example due to its dispersed archipelagic character, making supervision and monitoring more complex. In these circumstances, the effectiveness of fraud detection capability is determined not only by the quality of the RBIA but also by the availability and utilization of information technology systems that support data access, communication, and cross-regional coordination. Based on Agency Theory, RBIA, TAM, and Contingency Theory, information technology systems are seen as a critical factor in strengthening the effectiveness of RBIA. Because the success of control mechanisms is highly dependent

on environmental conditions and available technological support, RBIA will be more effective in detecting fraud if supported by adequate IT infrastructure and digital audit capabilities (Pratama et al., 2025). Therefore, Information Technology Systems can be expected to strengthen the relationship between RBIA and fraud detection capability. Based on this argument, the following hypothesis is proposed:

H3: Information Technology Systems positively moderate the relationship between Risk-Based Internal Audit and fraud detection capability.

Previous studies have largely focused on private, state-owned, or geographically uniform local government contexts. Research in island regions remains limited, despite challenges such as geographic dispersion, limited transportation, and uneven technological infrastructure. Central Maluku's archipelagic characteristics make supervision more complex, highlighting the role of RBIA and information technology in supporting fraud detection through data access, communication, and coordination.

This study examines the effects of Risk-Based Internal Audit and Information Technology Systems on fraud detection capability and the moderating role of Information Technology Systems in the relationship between RBIA and fraud detection capability among Government Internal Audit Apparatus in Central Maluku Regency. It contributes to public sector audit literature by extending RBIA research to island local governments and highlighting the contingent role of information technology.

METHODS

This study employed a quantitative approach with an explanatory survey design to examine the effect of Risk-Based Internal Audit (RBIA) on fraud detection capability (FD) and the moderating role of Information Technology Systems (ITS). The research population comprised all Government Internal Supervisory Apparatus (APIP) auditors assigned to the Inspectorate of Central Maluku Regency, Maluku Province. Thus, the study population was limited to auditors within the Central Maluku Regency Inspectorate and did not include auditors from other district, municipal, or provincial inspectorates. Using a census (saturated sampling) technique, all members of the population were included as respondents, resulting in 32 auditors.

Primary data were collected through a structured questionnaire. The questionnaire used a five-point Likert scale, ranging from 1 = strongly disagree to 5 = strongly agree. Measurement items were adapted from indicators used in previous studies and adjusted to the context of public sector internal auditing. RBIA was measured through risk-based audit planning, audit prioritization based on risk, risk-based evaluation of internal controls, and integration of audit activities with risk management (Al-Hajaya, 2019; Handoyo, 2024). FD was measured through the auditor's ability to identify red flags, speed in detecting irregularities, accuracy in analyzing indications of fraud, and effectiveness in reporting fraud-related findings. ITS was measured through the availability of integrated financial information systems, utilization of data analytics, accessibility of

real-time information, and auditors' ability to utilize information technology (Lowe et al., 2018; Manita et al., 2020; Sidauruk, 2024).

Before hypothesis testing, the measurement model was evaluated using PLS-SEM procedures. Instrument validity was assessed through convergent and discriminant validity, while reliability was evaluated using Cronbach's alpha and composite reliability. Convergent validity was assessed based on outer loadings and Average Variance Extracted (AVE), whereas discriminant validity was assessed using the appropriate PLS-SEM discriminant validity criteria. These procedures were conducted to ensure that the measurement instruments adequately represented the constructs under investigation.

The structural model was subsequently assessed using the coefficient of determination (R^2), path coefficients, and hypothesis testing. The moderating effect of ITS was tested within the PLS-SEM framework by constructing an interaction term between RBIA and ITS. Therefore, Moderated Regression Analysis (MRA) was not treated as a separate analytical method; rather, the moderation analysis was performed as part of the PLS-SEM structural model. The empirical model is specified as follows:

$$Fraud\ Detection = \beta_0 + \beta_1 RBIA + \beta_2 ITS + \beta_3 (RBIA \times ITS) + \varepsilon$$

Where FD represents fraud detection capability, RBIA represents Risk-Based Internal Audit, ITS represents Information Technology Systems, $RBIA \times ITS$ represents the interaction between RBIA and ITS, β_0 represents the constant, β_1 – β_3 represent the

estimated path coefficients, and ε represents the error term.

Hypothesis testing was performed using SmartPLS bootstrapping with 5,000 subsamples at a 5% significance level ($\alpha = 0.05$). Hypotheses were supported when the path coefficient was significant at $p < 0.05$. For the moderation hypothesis, significance was assessed based on the RBIA $\times$ ITS interaction coefficient and its bootstrap confidence interval.

The analytical procedure therefore consisted of four main stages: (1) descriptive analysis of respondent characteristics; (2) evaluation of the measurement model through validity and reliability testing; (3) evaluation of the structural model and direct effects; and (4) testing of the moderating effect of ITS through the interaction term in the PLS-SEM model. All analyses were performed using SmartPLS. The conceptual model of the study is presented in Figure 1.

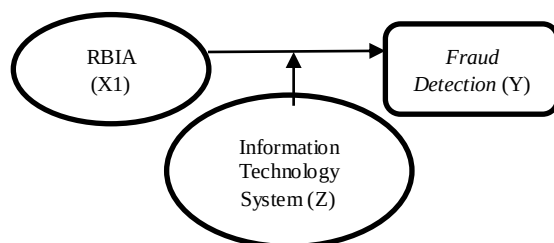


Figure 1. Research Model

RESULT AND DISCUSSION

Respondent Profile

This study involved 32 Government Internal Supervisory Apparatus (APIP) auditors and supervisory officials from the Inspectorate of Central Maluku Regency, Maluku Province. The respondents were selected using a census (saturated sampling) approach, in which all members of the defined population were included in the

study. Therefore, the respondent profile reflects the characteristics of the APIP personnel within the specific research setting rather than the broader population of auditors across Maluku Province.

Table 1. Respondent Characteristics

No	Characteristics	Category	Freq (People)	Percent (%)
1	Gender	Man	20	62.5
		Woman	12	37.5
2	Age	< 25 Years	1	3.1
		25–35 Years	8	25.0
		36–45 Years	11	34.4
		46–55 Years	9	28.1
		> 55 Years	3	9.4
3	Last education	Diploma	2	6.3
		Bachelor degree)	20	62.5
		Masters (S2)	9	28.1
		Doctorate (S3)	1	3.1
4	Current Position	First Expert Auditor	6	18.8
		Junior Expert Auditor	11	34.4
		Associate Expert Auditor	8	25.0
		Principal Expert Auditor	1	3.1
		P2UPD	4	12.5
		Structural Position	2	6.3
5	Length of Service at the Inspectorate	< 1 Year	2	6.3
		1–5 Years	7	21.9
		6–10 Years	9	28.1
		11–15 Years	8	25.0
		> 15 Years	6	18.8
6	Audit Experience	< 1 Year	1	3.1

	1–5 Years	6	18.8
	6–10 Years	9	28.1
	11–15 Years	8	25.0
	> 15 Years	8	25.0
7*	Certification/ Training	29	90.6
	Auditor Training		
	QIA/CIA	8	25.0
	CGCAE/CGAP	3	9.4
	CA	4	12.5
	CPA	1	3.1
	Risk Management	13	40.6
	SPIP/RBIA	24	75.0
8	Audit Frequency		
	1–3 Times	4	12.5
	4–6 Times	13	40.6
	7–10 Times	10	31.3
	> 10 Times	5	15.6

*Note: Certification/training categories are not mutually exclusive; respondents may have participated in multiple training programs or hold more than one professional certification. Percentages are therefore calculated based on the total number of respondents (n = 32) and do not necessarily sum to 100%.

The respondent characteristics provide contextual information regarding the professional background of the 32 APIP personnel included in this study. Male respondents accounted for 62.5% of the sample, while female respondents accounted for 37.5%. In terms of age, the largest group was 36–45 years (34.4%), followed by 46–55 years (28.1%). Respondents aged 25–35 years accounted for 25.0%, while those below 25 years and above 55 years accounted for 3.1% and 9.4%, respectively.

Regarding educational attainment, most respondents held a bachelor's degree (62.5%), followed by a master's degree (28.1%). Diploma and doctoral graduates accounted for 6.3% and 3.1%, respectively. In terms of current position, Junior Expert Auditors represented the largest group (34.4%),

followed by Associate Expert Auditors (25.0%) and First Expert Auditors (18.8%). P2UPD and structural-position holders accounted for 12.5% and 6.3%, respectively, while Principal Expert Auditors accounted for 3.1%.

The respondents also had substantial experience in the inspectorate. A total of 71.9% had worked at the Inspectorate for more than six years, consisting of 28.1% with 6–10 years, 25.0% with 11–15 years, and 18.8% with more than 15 years of service. Similarly, 78.1% of respondents had more than six years of audit experience. These figures indicate that most respondents had considerable exposure to internal audit and supervisory activities.

Professional development was also relatively extensive. Most respondents had participated in Auditor Training (90.6%), while 75.0% had received SPIP/RBIA-related training and 40.6% had received risk management training. Some respondents also reported professional certifications, including QIA/CIA, CGCAE/CGAP, CA, and CPA. Because certification and training categories were not mutually exclusive, these percentages reflect the proportion of respondents with each qualification or training experience rather than a distribution across mutually exclusive categories.

With respect to audit frequency, 87.5% of respondents reported conducting audits at least four times per year, comprising 40.6% conducting 4–6 audits, 31.3% conducting 7–10 audits, and 15.6% conducting more than 10 audits annually. Only 12.5% reported conducting 1–3 audits per year. Overall, the respondent profile indicates that the sample includes APIP personnel with varied

demographic and professional characteristics and substantial experience in internal audit activities. However, given the relatively small sample size ($n = 32$) and the single research setting at the Central Maluku Regency Inspectorate, these characteristics should be interpreted as contextual information about the respondents rather than evidence that the sample is statistically representative of APIP auditors in Maluku Province or other local governments.

Evaluation of the Measurement Model (Outer Model)

Convergent Validity Test

Table 2. Convergent Validity

Variables	Indicator	Loading Factor	AVE	Information
<i>Risk-Based Internal Audit (RBIA)</i>	RBIA1	0.847	0.636	Retained
	RBIA2	0.831		Retained
	RBIA3	0.825		Retained
	RBIA4	0.815		Retained
	RBIA5	0.813		Retained
	RBIA6	0.728		Retained
	RBIA7	0.829		Retained
	RBIA8	0.836		Retained
	RBIA9	0.775		Retained
	RBIA10	0.808		Retained
	RBIA11	0.716		Retained
	RBIA12	0.730		Retained
<i>Information Technology Systems (ITS)</i>	ITS1	0.861	0.634	Retained
	ITS2	0.804		Retained
	ITS3	0.831		Retained
	ITS4	0.671		Retained
	ITS9	0.801		Retained
<i>Fraud detection capability (FD)</i>	FD1	0.886	0.584	Retained
	FD12	0.716		Retained
	FD2	0.727		Retained
	FD4	0.681		Retained
	FD5	0.793		Retained

The measurement model was assessed to evaluate construct reliability and validity before testing the structural model. Convergent validity was examined using outer loadings and Average Variance Extracted (AVE). Following Hair et al. (2022), loadings of 0.70 or higher are generally considered adequate, while

indicators with loadings between 0.60 and 0.70 may be retained when theoretically relevant and supported by adequate AVE and reliability. As shown in Table 2, the RBIA, ITS, and FD constructs achieved AVE values of 0.636, 0.634, and 0.584, respectively, with outer loadings ranging from 0.716–0.847, 0.671–0.861, and 0.681–0.886. Thus, all constructs exceeded the recommended AVE threshold of 0.50, indicating adequate convergent validity. Two indicators, ITS4 (0.671) and FD4 (0.681), had loadings slightly below 0.70 but above 0.60. They were retained because their respective constructs achieved AVE values above 0.50, the indicators remained theoretically relevant, and their removal was not necessary to maintain adequate overall measurement quality. Therefore, these indicators were retained for subsequent reliability and discriminant validity assessment rather than removed solely because of a marginal deviation from the 0.70 threshold.

The non-sequential codes in Table.2, particularly ITS9 and FD12, follow the original questionnaire numbering and reflect the indicator-screening process. They were not renumbered to preserve traceability between the final PLS-SEM model and the original instrument. Accordingly, the absence of ITS5–ITS8 and FD3 reflects items excluded during screening rather than coding errors. ITS9 and FD12 were retained based on their measurement performance and theoretical relevance and should therefore be understood as retained indicators from the original instrument, not statistical outliers.

Discriminant Validity Test

Table 3. Discriminant Validity
Fornell-Larcker Criterion

Variables	RBIA	ITS	FD
RBIA	0.745		
ITS	0.447	0.793	
FD	0.670	0.582	0.775
HTMT (Heterotrait-Monotrait Ratio)			
Variables	RBIA	ITS	FD
RBIA	-		
ITS	0.489	-	
FD	0.735	0.642	-

Discriminant validity was evaluated using the Fornell–Larcker Criterion and the Heterotrait -Monotrait Ratio (HTMT). The test results showed that the square root of the AVE value of each construct was higher than the correlation between constructs, thus meeting the Fornell–Larcker criteria. In addition, the HTMT values between RBIA–ITS (0.489), RBIA–FD (0.735), and ITS–FD (0.642) were below the limits of 0.85 and 0.90 recommended in the literature. Thus, all constructs have met the requirements of discriminant validity, indicating that each construct has distinct characteristics conceptually and empirically. These results confirm that the measurement model is suitable for further structural model testing.

Reliability Test

Table 4. Reliability

Construct	Cronbach's Alpha	Composite Reliability
<i>Risk-Based Internal Audit (RBIA)</i>	0.895	0.916
<i>Information Technology Systems (ITS)</i>	0.852	0.893
<i>Fraud detection capability (FD)</i>	0.888	0.913

Construct reliability was evaluated using Cronbach's Alpha and Composite Reliability (CR). According to Hair et al. (2022), a construct is considered reliable if it

has a Cronbach's Alpha and Composite Reliability value above 0.70. The test results (Table 4) show that all constructs meet the reliability criteria. The Risk-Based Internal Audit (RBIA) variable has a Cronbach's Alpha value of 0.895 and a Composite Reliability of 0.916. The Information Technology System (ITS) variable obtained a Cronbach's Alpha value of 0.852 and a Composite Reliability of 0.893, while the Fraud detection capability (FD) variable has a Cronbach's Alpha value of 0.888 and a Composite Reliability of 0.913. All of these values are above the threshold of 0.70, thus indicating a good level of internal consistency. Thus, all constructs in this study have adequate reliability and are able to measure variables consistently. These results confirm that the measurement model meets reliability criteria and is therefore suitable for testing the structural model (inner model).

Structural Model Evaluation (Inner Model)

Collinearity Assessment (VIF)

Table 5. VIF Value

No	Indicators/Constructs	VIF
1	ITS1	1,928
2	ITS2	1,909
3	ITS3	2,309
4	ITS4	2,004
5	ITS9	1,485
6	FD1	4,315
7	FD12	2,295
8	FD2	2,330
9	FD4	1,713
10	FD5	1,810
11	RBIA (X1) × ITS (X2)	1,000
12	RBIA1	2,695
13	RBIA10	2,747
14	RBIA11	4,443
15	RBIA12	2,891
16	RBIA5	6,488
17	RBIA6	2,047
18	RBIA7	5,053
19	RBIA8	2,011
20	RBIA9	2,984

Before testing the structural model, a multicollinearity evaluation was conducted using the Variance Inflation Factor (VIF) value. According to Hair et al. (2022), a VIF value below 5.00 indicates no multicollinearity problem, while a value up to 10.00 is still tolerable. The test results (Table 5) show that almost all indicators have VIF values below 5.00. The VIF value for the Information Technology System (ITS) construct ranges from 1.485–2.309, while for the Fraud detection capability (FD) construct it ranges from 1.713 – 4.315. The moderating variable RBIA with ITS also has a VIF value of 1.000, indicating no multicollinearity in the interaction construct. For the Risk-Based Internal Audit (RBIA) construct, most indicators have VIF values below the recommended threshold of 5.00. However, RBIA5 (6.488) and RBIA7 (5.053) exceed this threshold, suggesting potential collinearity that warrants caution in interpreting these indicators. Nevertheless, the elevated VIF values were evaluated together with the indicators' theoretical relevance and other measurement criteria rather than used as the sole basis for indicator removal. However, both values are still below the tolerance limit of 10.00 and thus do not indicate serious multicollinearity (Hair et al, 2022).

Overall, the test results indicate that the research model does not experience multicollinearity issues that could affect parameter estimation. Therefore, all constructs are deemed to meet the collinearity assumptions and are suitable for use in the structural model (inner model) and hypothesis testing stages.

Coefficient of Determination (R^2)

Table 6. R Square (R^2)

Dependent Variable	R Square (R^2)	R Square Adjusted
<i>Fraud detection capability (FD)</i>	0.584	0.574

The Fraud Detection Capability construct has an R^2 of 0.584 and an Adjusted R^2 of 0.574, indicating that RBIA, Information Technology Systems, and their interaction explain 58.4% of the variance. Based on Hair et al. (2022), this reflects moderate explanatory power, with the small difference between R^2 and Adjusted R^2 indicating model stability.

Effect Size (f^2)

Table 7. Effect Size (f^2)

Relationship between variables	f^2	Category
RBIA → <i>Fraud detection capability</i>	0.351	Big
ITS → <i>Fraud detection capability</i>	0.238	Currently

The effect size analysis (Table 7) shows that Risk-Based Internal Audit (RBIA) has an f^2 value of 0.351, which exceeds the 0.35 threshold and is therefore classified as a large effect. Information Technology Systems (ITS) has an f^2 value of 0.238, indicating a medium effect, while the RBIA × ITS interaction has an f^2 value of 0.084, indicating a small effect. These results suggest that RBIA contributes substantially to the explained variance in Fraud Detection Capability, whereas ITS has a moderate contribution. The relatively small f^2 value of the interaction term indicates that the incremental contribution of the moderating effect of ITS is limited in magnitude. Thus, although the interaction effect is statistically significant, its effect size should be interpreted as relatively small rather than as a

substantial contribution to the explained variance of Fraud Detection Capability.

Predictive Relevance (Q^2)

Table 8. Q^2 Value

Endogenous Variables	Q^2 (Cross-Validated Redundancy)	Information
Fraud detection capability (FD)	0.322	Having Predictive Relevance

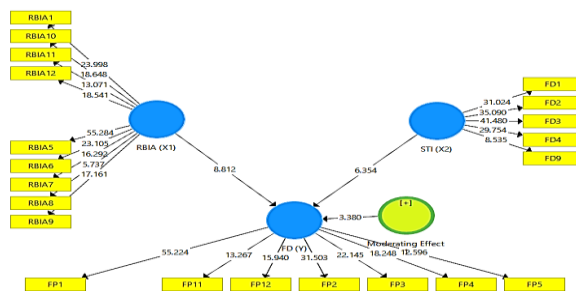


Figure 2. Predictive Relevance

The predictive relevance assessment (Table 8) shows that the Fraud Detection Capability (FD) construct has a Q^2 value of 0.322. Because the Q^2 value is greater than zero, the model demonstrates predictive relevance for the Fraud Detection Capability construct. Based on the commonly used thresholds of 0.02, 0.15, and 0.35 for small, medium, and large predictive relevance, respectively, a Q^2 value of 0.322 indicates medium predictive relevance. This result suggests that the structural model provides meaningful predictive relevance for Fraud Detection Capability, although the value does not reach the threshold commonly associated with large predictive relevance.

Predictive Performance (PLS-Predict)

Table 9. PLS-Predict

Indicator	RMSE PLS	RMSE Linear Model (LM)	Comparison Results
FD1	0.663	0.663	PLS < LM
FD2	0.613	0.667	PLS < LM
FD12	0.684	0.709	PLS < LM
FD4	0.628	0.650	PLS < LM
FD5	0.697	0.727	PLS < LM

The PLSpredict results (Table 9) show that the PLS-SEM model produces RMSE values that are lower than those of the linear model (LM) for almost all indicators of the Fraud Detection Capability construct. For the FD1 indicator, the PLS-RMSE and LM-RMSE values are equal (0.663), indicating comparable prediction error for this indicator. Thus, the PLS-SEM model demonstrates lower or equivalent prediction errors relative to the LM benchmark across all indicators. Following the PLSpredict assessment approach, these results indicate that the model provides meaningful out-of-sample predictive performance for the Fraud Detection Capability indicators. However, the results should not be interpreted as evidence of uniformly high predictive power, since the magnitude of predictive performance should be assessed based on the comparison of prediction errors and, where applicable, the distribution of indicators showing lower PLS-RMSE values than the benchmark model.

Hypothesis Testing

Table 10. Hypothesis Testing

Hypothesis	Path Coefficient	T Statistic	P Values	Decision
RBIA → FD	0.448	8,931	0,000	Supported
ITS → FD	0.352	6,803	0,000	Supported
RBIAxITS → FD	0.170	3,670	0,000	Supported

The test results (Table 10) show that Risk-Based Internal Audit (RBIA) has a positive and significant effect on Fraud detection capability ($\beta = 0.448$; $t = 8.931$; $p < 0.001$). This finding indicates that increasing the implementation of risk-based internal audit will improve the auditor's ability to detect fraud. Thus, H1 is supported. Furthermore, Information Technology Systems (ITS) also had a positive and significant effect on fraud detection

capability ($\beta = 0.352$; $t = 6.803$; $p < 0.001$). These results indicate that effective use of IT can improve fraud detection capabilities by providing faster, more accurate, and more integrated information. Therefore, H2 is supported.

In addition, the RBIA $\times$ ITS interaction effect shows a positive and significant coefficient ($\beta = 0.170$; $t = 3.670$; $p < 0.001$). This finding confirms that Information Technology Systems moderate the relationship between RBIA and Fraud detection capability, where better utilization of information technology strengthens the effect of RBIA implementation on improving fraud detection capabilities. Thus, H3 is supported.

The Influence of Risk Based Internal Audit (RBIA) on Fraud detection capability

The findings indicate a positive and statistically significant association between Risk-Based Internal Audit (RBIA) and Fraud Detection Capability, with a path coefficient of 0.448 ($p < 0.001$). Rather than implying a direct causal effect, this finding suggests that higher levels of RBIA implementation tend to be associated with stronger fraud detection capability among APIP auditors. This relationship can be understood from the way RBIA directs audit attention toward areas with greater exposure to risks and potential control weaknesses. By prioritizing higher-risk activities, transactions, and organizational units, auditors may be better positioned to identify unusual conditions, control deficiencies, and other indicators that warrant further examination.

The relationship can be explained through Agency Theory and the Risk-Based Auditing Framework. Information asymmetry between principals and agents

may create opportunities for misuse of organizational resources, making internal audit an important monitoring mechanism in local government. Within this context, RBIA helps auditors identify and prioritize high-risk areas, including activities with potential control weaknesses or fraud indicators. By linking risk assessment with audit planning, evidence gathering, and follow-up procedures, RBIA may help auditors allocate limited resources more effectively and focus their attention on areas requiring greater scrutiny. Thus, the observed association between RBIA and Fraud Detection Capability may reflect the role of risk-based audit planning in directing audit attention toward potential fraud risks.

These findings align with research showing that RBIA implementation improves the effectiveness of the internal audit function by focusing on high-risk areas. These results indicate that risk-based auditing allows auditors to allocate resources more efficiently, thereby improving the quality of the assurance process. Furthermore, (Wahidahwati & Asyik, 2022) found that the auditor's ability to detect fraud is influenced by the auditor's competence in optimally performing their role and the quality of the audit process, indicating that a systematic audit approach will increase the success of fraud identification. Furthermore, (Putra et al., 2022) emphasized that the integration of internal audit with risk management, as included in the RBIA framework, is a crucial element in preventing financial crime through early fraud detection capability mechanisms. In the public sector, (Nadirisyah et al., 2024) also showed that the internal audit function contributes to strengthening internal control

and fraud prevention, thereby improving the quality of public organizational governance (Hakim & Suryatimur, 2022). These findings reinforce the findings of this study that RBIA implementation not only improves audit effectiveness but also enhances the APIP's ability to detect fraud indications at an early stage.

In the context of the Central Maluku Regency Government, the implementation of RBIA becomes increasingly relevant given the vast scope of its oversight and the limited resources of the Internal Audit Agency (APIP). A risk-based approach allows the Inspectorate to prioritize audits of regional government organizations with higher risk levels, thereby enhancing the use of audit resources. Therefore, the regional government needs to continue strengthening the implementation of RBIA by improving auditor competency, refining the risk assessment process, and integrating risk management into audit planning to enhance fraud detection capabilities.

The Influence of Information Technology Systems on Fraud detection capability

The findings indicate a positive and statistically significant association between Information Technology Systems (ITS) and Fraud Detection Capability, with a path coefficient of 0.352 ($p < 0.001$). This finding suggests that greater use of information technology is associated with stronger fraud detection capability among APIP auditors. The relationship may be explained by the ability of information technology to support faster access, processing, integration, and analysis of audit-related information. These capabilities may help auditors identify

unusual transactions, inconsistencies, and patterns that require further examination.

This relationship can be explained through the Technology Acceptance Model (TAM), particularly the concepts of perceived usefulness and perceived ease of use. When auditors perceive information technology as useful and manageable, they may be more likely to incorporate it into audit activities. In public-sector auditing, technology can facilitate the collection and processing of larger volumes of financial and operational data, allowing auditors to examine information more systematically. Thus, the relevance of ITS to fraud detection lies not simply in the availability of technology, but in its ability to provide timely and accessible information that supports risk identification, analytical procedures, and follow-up examination.

The results of this study align with those of Bonrath & Eulerich (2024), who demonstrated that the application of technology-based audit techniques improves the internal audit function's ability to identify risks, prevent, and detect fraud. This finding is also supported by Wu et al. (2024), who explain that information technology capabilities and controls using information technology increase the effectiveness of the audit process by providing more accurate and high-quality information. Furthermore, Harahap & Erlina (2024) found that the use of information technology, combined with the implementation of Risk-Based Internal Audit, contributes to improved fraud detection capabilities in the public sector. These findings reinforce the findings of this study, which demonstrate that information technology systems are a critical factor in

improving audit effectiveness and auditors' ability to detect fraud.

The Moderating Role of Information Technology Systems on the Relationship between Risk-Based Internal Audit and Fraud detection capability

The findings indicate that the interaction between Risk-Based Internal Audit (RBIA) and Information Technology Systems (ITS) is positively associated with Fraud Detection Capability ($\beta = 0.170$, $p < 0.001$). This suggests that the association between RBIA and fraud detection capability may be stronger when adequate technological support is available. RBIA helps auditors identify and prioritize high-risk areas, while ITS facilitates access to, integration of, and analysis of relevant audit data.

This relationship can be explained through Contingency Theory, which suggests that the effectiveness of a control mechanism depends on its fit with organizational conditions and supporting resources. In this context, RBIA determines where auditors should focus, while ITS supports how efficiently the relevant information can be examined. For example, when RBIA identifies high-risk transactions or units, ITS can help auditors access data, compare transactions, identify unusual patterns, and obtain information for further examination. Thus, ITS may help translate RBIA's risk priorities into more targeted audit procedures.

This mechanism is particularly relevant in Central Maluku Regency, where geographical dispersion across islands can hinder document access and audit coordination. ITS facilitates the sharing and retrieval of audit information, but its effectiveness depends on network

connectivity, digital infrastructure, data quality, and users' technical capabilities.

The findings are consistent with previous studies showing that information technology enhances internal audit effectiveness and fraud detection (Bierstaker et al., 2001; Bonrath & Eulerich, 2024; Wu et al., 2024). Technology-based audit techniques, including AI and machine learning, support risk identification, anomaly detection, and fraud prevention (Shivram, 2024). In the public sector, integrating risk management, RBIA, and information technology further strengthens fraud detection capability (Harahap & Erlina, 2024).

CONCLUSION

This study demonstrates that Risk-Based Internal Audit (RBIA) and Information Technology Systems (ITS) significantly enhance fraud detection capability among the Government Internal Supervisory Apparatus (APIP) of the Central Maluku Regency Government. Consistent with H1 and H2, the findings show that both RBIA and ITS have positive and significant effects on fraud detection capability. Consistent with H3, ITS significantly strengthens the positive relationship between RBIA and fraud detection capability, indicating that technology enhances the effectiveness of risk-based auditing in supporting fraud detection.

Practically, APIP and the Inspectorate should strengthen risk assessment and audit planning to ensure that audit resources are directed toward high-risk areas. The use of digital audit tools and integrated information systems should also be expanded to support

more efficient data access, processing, and analysis. In addition, continuous development of auditor competencies in risk-based auditing, data analysis, and digital audit techniques is needed to maximize the benefits of technology-supported auditing. These measures can strengthen the capacity of APIP to detect potential fraud and improve the effectiveness of internal supervision in local government.

ACKNOWLEDGEMENT

The authors wish to express their sincere gratitude to the Central Maluku Regency Inspectorate for their participation and contribution to this research. We also extend our appreciation to the Central Maluku Regency Government for their support and cooperation throughout the research process. Special thanks are due to Pattimura University, specifically the Faculty of Economics and Business for providing research funding through the Faculty's Flagship Research Program under the Pattimura University (UNPATTI) Flagship Basic Research (PDUU) scheme for 2026. The financial support and institutional assistance provided by Pattimura University were invaluable to the successful completion of this study.

Recommendation: The findings imply that local governments should strengthen the implementation of Risk-Based Internal Audit (RBIA) by improving risk-based audit practices and supporting them with integrated information technology systems. Enhancing auditors' digital competencies and the use of technology-based audit tools can further improve fraud detection capability effectiveness. This study is limited by its

small sample size and focus on a single local government inspectorate. Future research is encouraged to use larger samples from different regions and include additional variables, such as auditor competency, internal control effectiveness, or organizational culture, to provide a broader understanding of fraud detection capability in the public sector.

REFERENCES

- Al-hajaya, K. (2019). The Impact of Audit Committee Effectiveness on Audit Quality: Evidence from the Middle East. *International Review of Management and Marketing*, 9(5), 1–8.
- Bierstaker, J. L., Burnaby, P., & Thibodeau, J. (2001). The impact of information technology on the audit process: an assessment of the state of the art and implications for the future. *Managerial Auditing Journal*, 16(3), 159–164. <https://doi.org/10.1108/02686900110385489>
- Bonrath, A., & Eulerich, M. (2024). Internal auditing's role in preventing and detecting fraud: An empirical analysis. *International Journal of Auditing*, 28(4), 615–631. <https://doi.org/https://doi.org/10.1111/ija.u.12342>
- Hakim, L. N., & Suryatimur, K. P. (2022). Efektivitas Peran Audit Internal Dalam Pencegahan Fraud. *Jurnal Ilmiah Akuntansi Kesatuan (JIAKES)*, 10(3), 523–532. <https://doi.org/10.37641/jiakes.v10i3.1412>
- Handoyo, S. (2024). Mapping the landscape of internal auditing effectiveness study : a bibliometric approach. *Cogent Business & Management*, 11(1), 1–30. <https://doi.org/10.1080/23311975.2023.2289200>
- Harahap, A. J. S., & 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(03), 653–664.
[https://doi.org/10.21511/ppm.22\(3\).2024.50](https://doi.org/10.21511/ppm.22(3).2024.50)
- Le, T. T., Mai, T., & Nguyen, A. (2020). The Adoption of Risk Based Audit Approach in the Independent Audit Firms : A Study of Case of Vietnam. *Journal of Asian Finance, Economics and Business*, 7(2), 89–97.
<https://doi.org/10.13106/jafeb.2020.vol7.no2.89>
- Lowe, D. J., James, L. B., Diane, J. J., & Greg, J. (2018). Information technology in an audit context: Have the big 4 lost their advantage? *Journal of Information Systems*, 32(1), 87–107.
- Manita, R., Elommal, N., Baudier, P., & Hikkerova, L. (2020). Technological Forecasting & Social Change The digital transformation of external audit and its impact on corporate governance. *Technological Forecasting & Social Change*, 150, 119751.
<https://doi.org/10.1016/j.techfore.2019.119751>
- Nadirsyah, Indriani, M., & Mulyany, R. (2024). Enhancing fraud prevention and internal control : the key role of internal audit in public sector governance. *Cogent Business & Management*, 11(1), 1–22.
<https://doi.org/10.1080/23311975.2024.2382389>
- Pratama, G. E., Ferriswara, D., & Kamariyah, S. (2025). Dynamics Social : International Journal of Social Sciences and Communication Risk-Based Internal Oversight of Local Government Finance : A Literature Review on Fraud Prevention and Control. *Dynamics Social : International Journal of Social Sciences and Communication*, 02(01), 67–88.
<https://doi.org/https://doi.org/10.70062/dynamicsocial.v2i1.265>
- Putra, I., Sulistiyo, U., Diah, E., Rahayu, S., & Hidayat, S. (2022). The Influence Of Internal Audit, Risk Management, Whistleblowing System and Big Data Analytics on The Financial Crime Behavior Prevention. *Cogent Economics & Finance*, 10(1), 1–27.
<https://doi.org/10.1080/23322039.2022.2148363>
- Shivram, V. (2024). Auditing With AI: A Theoretical Framework For Applying Machine Learning Across The Internal Audit Lifecycle. *EDPACS*, 69, 22–40.
<https://api.semanticscholar.org/CorpusID:267642485>
- Sidauruk, D. L. (2024). Data Analytics in Fraud Prevention and Detection by Government Internal Supervisory Apparatuses at Ministries/Institutions/Local Governments: A Mixed-Method Study. *Asia Pacific Fraud Journal*, 9(2), 241–260.
<https://doi.org/10.21532/apfjournal.v9i2.340>
- Wahidahwati, W., & Asyik, N. F. (2022). Determinants of Auditors Ability in Fraud Detection Determinants of Auditors Ability in Fraud Detection. *Cogent Business & Management*, 9(1), 1–20.
<https://doi.org/10.1080/23311975.2022.2130165>
- Wu, T.-H., Huang, S. Y., Chiu, A.-A., & Yen, D. C. (2024). IT governance and IT controls: Analysis from an internal auditing perspective. *International Journal of Accounting Information Systems*, 52, 100663.
<https://doi.org/https://doi.org/10.1016/j.aacinf.2023.100663>
- Zahra, S. A. (2025). The Role of Risk Based Internal Audit and Risk Management in the Prevention and Detection of Fraud in Auction Companies (Study Case at PT JBA Indonesia). *Indonesian Journal of Economics, Social, and Humanities*, 7(2), 187–199.
<https://doi.org/https://doi.org/10.31258/ijesh.7.2.187-199>