International Journal of Business and Quality Research

https://e-journal.citakonsultindo.or.id/index.php/IJBQR
E-ISSN: 2985-9468

Strengthening Public-Sector Accountability in Indonesian State-Owned Enterprises: The Role of Fraud Risk Indicators and Technology Capability in Internal Auditing?

Muhammad Arsyad[1]*, Arfandi[2], Asri Usman[3], Darmawati[4]

[1]Acconting Department, Politeknik Negeri Ujung Pandang, Makassar 90245 Indonesia.
[2]Faculty of Economics and Business, Universitas Muhammadiyah, Sorong Indonesia
[3,4]Faculty of Economics and Business, Universitas Hasanuddin, Makassar 90245, Indonesia

*Corresponding author: muhammad_arsyad@poliupg.ac.id
https://orcid.org/0009-0008-9155-3255

Abstract

State-owned enterprises (SOEs) manage state-controlled resources while pursuing commercial, developmental, and public-policy objectives; therefore, effective internal auditing is essential for public-sector accountability. This study examines the effects of Fraud Risk Indicators and Technology Capability on Internal Audit Effectiveness in Indonesian SOEs. Fraud Risk Indicators reflect structured signals of pressure, opportunity, rationalization, capability, arrogance, and collusion, whereas Technology Capability comprises digital infrastructure, data integration, Audit Data Analytics, continuous auditing, and auditor digital competence. Data were collected from 250 internal auditors and audit-related professionals representing 20 Indonesian SOEs and analysed using Partial Least Squares Structural Equation Modelling with 5,000 bootstrap resamples. Both hypotheses were supported. Fraud Risk Indicators positively affected Internal Audit Effectiveness (beta = 0.287, t = 4.348, p less than 0.001), while Technology Capability demonstrated a stronger positive effect (beta = 0.416, t = 6.603, p less than 0.001). The model explained 46.8 percent of Internal Audit Effectiveness variance and demonstrated predictive relevance (Q square = 0.321). The findings indicate that fraud-risk governance and digital audit capability strengthen stewardship, information quality, internal control, and risk-based oversight. Although public accountability was not measured directly, effective internal auditing may support SOE transparency, integrity, and responsible management of state-controlled resources.

Keywords: Public-sector accountability; State-owned enterprises; Fraud Risk Indicators; Technology Capability; Internal Audit Effectiveness

Copyright to the author of some rights reserved This work is licensed under aCreative Commons Attribution-ShareAlike 4.0 International License.

International Journal of Business and Quality Research
https://e-journal.citakonsultindo.or.id/index.php/IJBQR
E-ISSN: 2985-9468

INTRODUCTION

Public-sector accounting is not limited to recording financial transactions and preparing financial reports. It also provides an accountability mechanism through which organizations entrusted with public resources demonstrate transparency, stewardship, integrity, compliance, and responsible decision-making. Public accountability requires organizations to explain how resources are acquired, used, protected, monitored, and reported. It also requires organizational leaders to justify decisions, respond to control weaknesses, and remain accountable to relevant oversight institutions and stakeholders (Grossi et al., 2015; OECD, 2018).

State-owned enterprises, hereafter referred to as SOEs, occupy a distinctive and important position within the public-sector accountability framework. SOEs operate at the intersection of public ownership, commercial operations, national development objectives, and public-policy responsibilities. They are expected to generate financial and operational performance while also protecting state-controlled resources, complying with public mandates, maintaining integrity in reporting, supporting strategic public objectives, and preserving public confidence.

Unlike purely private companies, SOEs face multiple accountability relationships. They are accountable to the state as owner, ownership entities, boards of commissioners, management, regulators, employees, creditors, service users, citizens, and other stakeholders. This hybrid nature creates governance challenges because SOEs must manage economic objectives while simultaneously demonstrating that public resources are used efficiently, transparently, ethically, and in accordance with applicable laws and public-interest objectives (Grossi et al., 2015; OECD, 2018).

The OECD Guidelines on Corporate Governance of State-Owned Enterprises emphasize that SOEs should implement high standards of transparency, accountability, integrity, disclosure, accounting, compliance, internal control, risk management, and auditing. Transparency regarding material matters is important because it strengthens the accountability of SOE boards and management. The OECD further emphasizes that SOEs should maintain reliable financial reporting, appropriate internal control systems, effective risk management processes, and credible audit arrangements (OECD, 2018).

Internal audit is an important component of this accountability infrastructure. Internal auditors provide independent and objective assurance concerning governance, risk management, internal control, compliance, fraud risk, and the reliability of information used in decision-making. In the public-sector context, internal auditing supports stewardship by examining whether organizational resources are properly protected, whether internal

Copyright to the author of some rights reserved This work is licensed under aCreative Commons Attribution-ShareAlike 4.0 International License.

controls are adequate, whether risks are identified and managed, and whether corrective action is taken in response to audit findings.

The Global Internal Audit Standards state that internal auditing creates, protects, and sustains organizational value by providing risk-based and objective assurance, advice, insight, and foresight. The Standards also emphasize that the internal audit function should be positioned independently and should maintain direct accountability to the board or the highest governance body. In public-sector entities, internal audit is expected to contribute to safeguarding public funds and ensuring that resources are used appropriately and effectively (The Institute of Internal Auditors (IIA), 2024).

The accountability role of internal auditing has become more complex in the digital era. SOEs increasingly use enterprise resource planning systems, electronic procurement, digital payment mechanisms, cloud computing, electronic documentation, integrated databases, and interconnected information systems. These technologies generate large volumes of data that may improve internal control, monitoring, risk assessment, reporting, and decision-making. However, digital transformation also creates new fraud risks, including electronic data manipulation, unauthorized access, fictitious transactions, collusion through digital platforms, cyber-enabled fraud, and technology-based financial reporting manipulation (Alles, 2015; Issa et al., 2016; Richins et al., 2017).

Traditional audit procedures remain essential. Documentation review, physical observation, confirmation, interviews, substantive testing, compliance testing, and professional judgment remain important sources of audit evidence. However, traditional audit procedures alone may be insufficient in environments characterized by high transaction volume, complex data structures, interconnected systems, and rapidly changing fraud patterns. Internal auditors need more timely, comprehensive, and systematic information to identify anomalies, assess fraud vulnerabilities, prioritize audit activities, and support management follow-up.

Data-driven internal auditing provides an opportunity to strengthen the accountability role of internal audit. Data-driven internal auditing refers to the use of organizational data, analytical techniques, digital systems, and technology-enabled procedures to support audit planning, fraud-risk assessment, audit testing, continuous monitoring, reporting, and follow-up. It may include Audit Data Analytics, anomaly detection, risk scoring, continuous auditing, dashboard reporting, visualization, and decision-support systems (D. Appelbaum et al., 2017; D. A. Appelbaum et al., 2018; Vasarhelyi et al., 2015).

In the public-sector context, data-driven internal auditing should not be viewed merely as a technical innovation. It should be viewed as a mechanism for strengthening stewardship, improving information quality, supporting fraud prevention, enhancing risk-

Copyright to the author of some rights reserved This work is licensed under aCreative Commons Attribution-ShareAlike 4.0 International License.

International Journal of Business and Quality Research
https://e-journal.citakonsultindo.or.id/index.php/IJBQR
E-ISSN: 2985-9468

based oversight, and improving the ability of SOEs to demonstrate accountable management of state-controlled resources. Data analytics may help auditors move from retrospective review of selected transactions toward more comprehensive analysis, anomaly identification, early warning, and continuous risk monitoring.

The relevance of data analytics to public-sector fraud prevention and internal audit effectiveness has been demonstrated in Indonesia. Sidauruk, (2024) found that data analytics usage was associated with internal audit effectiveness among Government Internal Supervisory Apparatuses. The study also identified that data analytics can improve anomaly detection and audit scope for fraud prevention and detection. This finding is relevant to SOEs because SOEs face similar challenges involving public-resource stewardship, organizational complexity, transaction volume, internal control, fraud vulnerability, and accountability expectations (Sidauruk, 2024).

Nevertheless, the effectiveness of data-driven internal auditing depends on the quality of fraud-risk information and the organizational capability to use technology effectively. A digital audit system cannot support accountability if fraud-risk information is fragmented, data are not integrated, analytical tools are unavailable, information access is limited, or auditors lack digital competence. Accordingly, the public-sector value of data-driven internal auditing depends on two important organizational mechanisms: Fraud Risk Indicators and Technology Capability.

Fraud Risk Indicators represent structured signals that help internal auditors identify potential fraud vulnerabilities. These indicators are based on the Fraud Hexagon dimensions of pressure, opportunity, rationalization, capability, arrogance, and collusion. In SOEs, Fraud Risk Indicators can support accountability by helping auditors identify risks to state-controlled resources, procurement integrity, financial reporting, internal controls, compliance, and public trust (Khamainy et al., 2022).

Technology Capability represents the organizational capacity to provide technology infrastructure, data integration, Audit Data Analytics, continuous auditing, secure information access, and digital auditor competence. From a public-sector perspective, Technology Capability is not only an operational resource. It is also an information-governance capability that can improve the availability, reliability, traceability, and timeliness of information used for internal oversight and accountability (Bahardwa j, 2000; Barney, 1991; OECD, 2018).

Internal Audit Effectiveness is positioned as the key outcome variable because it represents the practical capacity of the internal audit function to support governance, risk management, internal control, compliance, fraud prevention, and management follow-up. Internal Audit Effectiveness does not equal public accountability. However, it is an important

Copyright to the author of some rights reserved This work is licensed under aCreative Commons Attribution-ShareAlike 4.0 International License.

organizational mechanism through which SOEs may improve their ability to meet public accountability obligations.

This study therefore examines the relationships among Fraud Risk Indicators, Technology Capability, and Internal Audit Effectiveness in Indonesian SOEs. The study contributes to public-sector accounting literature by explaining how data-driven internal auditing may support public-sector accountability through fraud-risk governance, information governance, technology-enabled oversight, and stronger internal audit effectiveness.

THEORETICAL REVIEW

Public-Sector Accounting, Stewardship, and Accountability in State-Owned Enterprises

Public-sector accounting serves both information and accountability functions. The information function provides data for planning, control, performance evaluation, decision-making, and reporting. The accountability function enables stakeholders to evaluate whether public resources have been managed in accordance with legal requirements, ethical principles, organizational objectives, and public-interest expectations.

In SOEs, public-sector accountability includes financial accountability, managerial accountability, legal accountability, performance accountability, and social accountability. Financial accountability concerns the proper management and reporting of resources. Managerial accountability concerns the responsibility of directors and managers for organizational decisions and performance. Legal accountability concerns compliance with laws, regulations, public mandates, procurement rules, and governance standards. Performance accountability concerns whether SOEs achieve financial, service, developmental, or strategic objectives. Social accountability concerns transparency and responsiveness to citizens, service users, communities, and other stakeholders.

The hybrid nature of SOEs creates a need for strong governance arrangements. SOEs must balance commercial discipline with public objectives and public accountability. The OECD Guidelines state that SOEs should maintain high standards of transparency and disclosure, particularly for material matters relating to financial performance, objectives, governance arrangements, risk factors, sustainability, and the use of resources. High-quality accounting, reporting, internal control, risk management, and audit processes are necessary to support these standards (OECD, 2018).

Internal audit supports the accountability framework by providing assurance regarding governance, risk management, internal control, compliance, operational efficiency, integrity, and fraud risk. The internal audit function may also support accountability through

Copyright to the author of some rights reserved This work is licensed under aCreative Commons Attribution-ShareAlike 4.0 International License.

recommendations, communication of findings, follow-up of corrective action, and evaluation of whether management has addressed identified control weaknesses.

In the context of SOEs, Internal Audit Effectiveness may contribute to public accountability in three ways. First, it supports stewardship by helping to protect state-controlled resources and prevent misuse. Second, it supports transparency by improving the reliability and traceability of information used in decision-making and reporting. Third, it supports oversight by providing boards, audit committees, management, ownership entities, and regulators with assurance concerning risk, control, compliance, and organizational performance.

Fraud Risk Indicators as a Public-Sector Accountability Mechanism

Fraud Risk Indicators represent structured information that helps auditors identify potential fraud vulnerability in organizational activities, transactions, systems, and decision-making processes. In this study, Fraud Risk Indicators are derived from the Fraud Hexagon framework: pressure, opportunity, rationalization, capability, arrogance, and collusion.

In SOEs, fraud risk has public-sector implications because it may affect public assets, public procurement, state investment, public-service obligations, government credibility, and public confidence. Fraud in SOEs may involve procurement manipulation, conflicts of interest, fictitious vendors, inflated contracts, misuse of assets, related-party transactions, unauthorized payments, manipulation of financial statements, collusion, and abuse of authority.

Structured Fraud Risk Indicators can support public accountability by improving the ability of internal auditors to identify warning signs, prioritize high-risk activities, allocate audit resources, and provide timely recommendations. The indicators may also improve the traceability of audit planning because auditors can explain why certain business units, processes, transactions, vendors, projects, or management decisions are classified as high risk.

Fraud Risk Indicators should not be treated as direct proof that fraud has occurred. Instead, they should be understood as risk signals that require professional judgment, additional audit procedures, corroborating evidence, and appropriate investigation. Their public-sector value lies in helping auditors identify risks early, prevent losses, strengthen controls, and protect state-controlled resources. Based on this argument, the following hypothesis is proposed:

H1: Fraud Risk Indicators are positively associated with Internal Audit Effectiveness.

Copyright to the author of some rights reserved This work is licensed under aCreative Commons Attribution-ShareAlike 4.0 International License.

International Journal of Business and Quality Research
https://e-journal.citakonsultindo.or.id/index.php/IJBQR
E-ISSN: 2985-9468

Technology Capability as a Public-Sector Information-Governance Capability

Technology Capability refers to the organizational capacity to acquire, integrate, deploy, and use technological resources effectively. In a public-sector accountability context, Technology Capability should be understood not only as information technology infrastructure but also as a capability for information governance, risk monitoring, control evaluation, fraud prevention, and evidence-based oversight.

Technology Capability in this study includes technology infrastructure, data integration, audit data access, Audit Data Analytics, continuous auditing, secure information systems, digital competence, and the ability to use technology in internal audit activities. These capabilities may enable auditors to obtain relevant data more efficiently, analyse larger transaction populations, identify anomalies, monitor risk indicators, evaluate controls, document audit evidence, and follow up on management actions.

The Resource-Based View suggests that technological resources can create organizational value when they are effectively integrated with processes, human capability, governance arrangements, data quality, and management support. Thus, software or hardware alone does not guarantee effective internal auditing. Technology becomes valuable when it improves the ability of auditors to perform assurance activities and supports governance bodies in making more informed decisions (Bahardwa j, 2000; Barney, 1991; Wade & Hulland, 2004).

In SOEs, Technology Capability can contribute to accountability by improving the reliability, timeliness, accessibility, and traceability of audit-related information. It can help internal auditors assess whether state-controlled resources are managed properly, whether controls are functioning, whether fraud risks are emerging, and whether management has implemented corrective action. Based on this argument, the following hypothesis is proposed:

H2: Technology Capability is positively associated with Internal Audit Effectiveness.

Public-Sector Accounting and Accountability Implications

The findings should be interpreted within the public-sector accountability environment of Indonesian SOEs. Fraud Risk Indicators and Technology Capability are not merely operational or technical variables. They represent organizational mechanisms that may strengthen stewardship, information quality, fraud prevention, internal control, and oversight of state-controlled resources.

Fraud Risk Indicators support the stewardship dimension of public-sector accounting because they help auditors identify potential risks to public resources, procurement integrity, reporting reliability, and compliance. By identifying potential fraud

Copyright to the author of some rights reserved This work is licensed under aCreative Commons Attribution-ShareAlike 4.0 International License.

risks early, internal audit functions may support preventive control, risk-based audit planning, and corrective action before organizational losses or reputational damage become more severe.

Technology Capability supports the information dimension of public-sector accounting because it can improve the availability, reliability, timeliness, and traceability of organizational data. Integrated data systems, Audit Data Analytics, and continuous auditing can help internal auditors obtain more complete evidence, review larger transaction populations, identify anomalies, and communicate risk information more effectively.

Internal Audit Effectiveness supports the oversight dimension of public accountability because it enables internal audit functions to provide assurance regarding governance, risk management, internal control, compliance, fraud prevention, and management follow-up. Effective internal auditing can help boards, audit committees, management, ownership entities, and regulators identify weaknesses and prioritize corrective action.

The findings do not demonstrate that public accountability has increased directly. Public accountability was not measured through disclosure quality, public trust, service-delivery outcomes, fiscal performance, or stakeholder evaluations. However, the findings support the argument that stronger fraud-risk governance and Technology Capability may improve Internal Audit Effectiveness, which is an important mechanism for supporting public-sector accountability in SOEs.

METHOD

Research Design

This study employed a quantitative explanatory research design within a broader Research and Development project. The broader project adopted the ADDIE framework, consisting of Analysis, Design, Development, Implementation, and Evaluation, to develop and evaluate an IT-Based Fraud Diagnostic Decision Support Framework. The framework was implemented through the BUMN Anti-Fraud Intelligence System, hereafter referred to as BAFIS. The ADDIE framework was selected because it provides a systematic process for developing, implementing, and evaluating technology-based systems that are designed to address organizational needs and user requirements (Branch, 2009).

The present article focuses on the implementation and evaluation stages of the broader project. Specifically, the study examines the relationships among Fraud Risk Indicators, Technology Capability, and Internal Audit Effectiveness in Indonesian state-owned enterprises. The study positions these relationships within the context of public-sector

Copyright to the author of some rights reserved This work is licensed under aCreative Commons Attribution-ShareAlike 4.0 International License.

accounting and public accountability because SOEs manage state-controlled resources while pursuing commercial, strategic, and public-policy objectives.

The research model was designed to assess whether structured Fraud Risk Indicators and organizational Technology Capability are associated with Internal Audit Effectiveness. Fraud Risk Indicators represent structured information that supports the identification of potential fraud vulnerabilities. Technology Capability represents the organizational ability to provide technological infrastructure, data integration, Audit Data Analytics, continuous auditing, and digital auditor competence. Internal Audit Effectiveness represents the ability of internal audit functions to provide timely, relevant, reliable, and actionable assurance concerning governance, risk management, internal control, compliance, fraud risk, and management follow-up.

The relationships were analyzed using Partial Least Squares Structural Equation Modeling, hereafter referred to as PLS-SEM, with SmartPLS 4. PLS-SEM was considered appropriate because the study examines relationships among latent constructs and focuses on the explanatory role of Fraud Risk Indicators and Technology Capability in relation to Internal Audit Effectiveness. PLS-SEM is also suitable for research involving predictive analysis, complex latent-variable relationships, and theory development in accounting, auditing, management, and information systems research (Hair Joseph F et al., 2022; Joseph F. Hair et al., 2019; Sarstedt et al., 2020).

The study used cross-sectional data because the questionnaire responses were collected from respondents during one period of data collection. Therefore, the findings should be interpreted as statistically significant associations among Fraud Risk Indicators, Technology Capability, and Internal Audit Effectiveness. The cross-sectional design does not allow definitive causal conclusions.

Research Setting

The research was conducted in Indonesian state-owned enterprises. SOEs are relevant to public-sector accounting and accountability because they combine commercial activities with public ownership, state investment, national development objectives, and public-policy responsibilities. Their accountability is not limited to profitability or operational performance. SOEs are also expected to demonstrate transparency, integrity, compliance, sound governance, stewardship of state-controlled resources, and responsiveness to public-interest objectives (Grossi et al., 2015; OECD, 2018).

The SOE context is particularly relevant for examining data-driven internal auditing. SOEs typically operate through complex organizational structures, large transaction volumes, procurement activities, investment decisions, asset-management processes, digital

Copyright to the author of some rights reserved This work is licensed under aCreative Commons Attribution-ShareAlike 4.0 International License.

systems, and multiple internal-control mechanisms. These characteristics may create fraud vulnerabilities and information asymmetry, making effective internal auditing essential for governance, risk management, internal control, and accountability.

The OECD Guidelines on Corporate Governance of State-Owned Enterprises emphasize that SOEs should maintain high standards of transparency, accountability, integrity, disclosure, internal control, risk management, compliance, and auditing. These standards highlight the importance of internal audit as an organizational mechanism that can support the protection of state-controlled resources and strengthen oversight of management decisions (OECD, 2018).

Participants and Respondent Profile

The final quantitative evaluation involved 250 internal auditors and audit-related professionals from 20 Indonesian SOEs. The respondents were selected because they were involved directly in functions related to internal audit, internal control evaluation, risk management, fraud investigation, and information technology-based auditing.

The diversity of respondent roles is relevant because data-driven internal auditing requires coordination between audit, risk management, internal control, information technology, fraud investigation, and governance-related functions. These functions jointly contribute to fraud-risk identification, evaluation of internal controls, analysis of organizational data, audit planning, monitoring, reporting, and management follow-up.

Table 1 presents the distribution of respondents.

Professional Function	Number of Respondents	Percentage
Internal audit	98	39.2
Internal control evaluation	62	24.8
Risk management	40	16.0
Investigative or fraud audit	22	8.8
IT-based audit	18	7.2
Other audit-related functions	10	4.0
Total	250	100.0

Source: Primary data processed by the authors.

The respondent distribution indicates that most participants were directly involved in internal audit and internal-control evaluation functions. Internal auditors represented 39.2 percent of the sample, while respondents involved in internal-control evaluation represented 24.8 percent. Risk-management professionals accounted for 16.0 percent of the respondents. The participation of investigative or fraud-audit professionals and IT-based

Copyright to the author of some rights reserved This work is licensed under aCreative Commons Attribution-ShareAlike 4.0 International License.

auditors is particularly relevant because the study examines fraud-risk information and organizational technology capability in relation to Internal Audit Effectiveness.

Data Collection

Primary data were collected through questionnaires administered to internal auditors and audit-related professionals in Indonesian SOEs. The questionnaire was used to collect information concerning Fraud Risk Indicators, Technology Capability, and Internal Audit Effectiveness.

The broader Research and Development project also incorporated interviews, observations, documentation studies, and expert validation. These activities were conducted to support the development and evaluation of the IT-Based Fraud Diagnostic Decision Support Framework and the BAFIS prototype. The integration of qualitative and quantitative activities was intended to ensure that the framework reflected actual organizational conditions, user needs, audit processes, fraud-risk characteristics, information-system conditions, and technology implementation challenges (Branch, 2009; Creswell John W. & Creswell J. David, 2018; Fetters et al., 2013; Jhon W. Creswell & Cheryl N. Poth, 2016).

For the present article, questionnaire data constituted the principal source for the quantitative analysis. The use of questionnaires was appropriate because the study examined respondent perceptions concerning organizational fraud-risk information, technology capability, and internal audit effectiveness.

The research addressed sensitive organizational issues, including fraud risk, control weakness, technology capability, and audit performance. Therefore, respondents should be assured that their participation was voluntary, that individual responses would remain confidential, and that the data would be reported only in aggregate form. Such procedural safeguards are important for minimizing respondent concerns and encouraging honest responses in internal-audit and fraud-related research.

Measurement of Constructs

The revised research model included three latent constructs: Fraud Risk Indicators, Technology Capability, and Internal Audit Effectiveness. The three constructs were selected because they have direct relevance to public-sector accounting, fraud-risk governance, stewardship of state-controlled resources, information governance, and internal oversight in SOEs.

Fraud Risk Indicators were identified as FH_RED. This construct consisted of six indicators representing structured fraud-risk information derived from the Fraud Hexagon dimensions of pressure, opportunity, rationalization, capability, arrogance, and collusion.

Copyright to the author of some rights reserved This work is licensed under aCreative Commons Attribution-ShareAlike 4.0 International License.

International Journal of Business and Quality Research
https://e-journal.citakonsultindo.or.id/index.php/IJBQR
E-ISSN: 2985-9468

Fraud Risk Indicators are relevant to SOEs because fraud risk may affect state-controlled resources, procurement integrity, asset management, financial reporting, compliance, and public confidence. Structured fraud-risk information can help auditors identify high-risk areas, prioritize audit procedures, and determine where further examination is required (Khamainy et al., 2022).

Technology Capability was identified as TECH_CAP. This construct consisted of four indicators covering organizational technology infrastructure, data integration, Audit Data Analytics, continuous auditing, and digital auditor competence. Technology Capability is treated as an organizational information-governance capability. It reflects the ability of an SOE to provide reliable, accessible, integrated, and timely data for audit activities, risk monitoring, fraud prevention, internal control evaluation, and evidence-based oversight (Bahardwa j, 2000; Barney, 1991; Wade & Hulland, 2004).

Internal Audit Effectiveness was identified as AUD_EFF. This construct consisted of four indicators measuring the effectiveness of internal audit activities. In this study, Internal Audit Effectiveness refers to the ability of the internal audit function to provide timely, relevant, reliable, and actionable assurance concerning governance, risk management, internal control, fraud risk, compliance, and management follow-up. In the SOE context, Internal Audit Effectiveness supports accountability by helping the organization identify control weaknesses, manage fraud vulnerabilities, protect state-controlled resources, provide useful recommendations, and encourage corrective action (Bonrath & Eulerich, 2024; The Institute of Internal Auditors (IIA), 2024).

Table 2. Construct Definitions and Public-Sector Relevance

Construct	Code	Definition	Public-Sector Relevance
Fraud Risk Indicators	FH_RED	Structured fraud-risk information based on pressure, opportunity, rationalization, capability, arrogance, and collusion	Supports fraud prevention, protection of state-controlled resources, procurement integrity, reporting integrity, and risk-based audit planning
Technology Capability	TECH_CAP	Organizational capability in technology infrastructure, data integration, Audit Data Analytics, continuous auditing, and digital auditor competence	Supports information governance, data reliability, transaction traceability, risk monitoring, and

Copyright to the author of some rights reserved This work is licensed under aCreative Commons Attribution-ShareAlike 4.0 International License.

International Journal of Business and Quality Research
https://e-journal.citakonsultindo.or.id/index.php/IJBQR
E-ISSN: 2985-9468

			evidence-based public-sector oversight
Internal Audit Effectiveness	AUD_EFF	Ability of the internal audit function to provide timely, relevant, reliable, and actionable assurance concerning governance, risk management, internal control, compliance, fraud risk, and management follow-up	Supports stewardship, transparency, internal control, accountability, protection of public resources, and governance oversight

Source: Developed for this study.

The revised three-variable model contains 14 indicators. Fraud Risk Indicators consist of six indicators, Technology Capability consists of four indicators, and Internal Audit Effectiveness consists of four indicators.

Data Analysis Procedure

The data were analysed using SmartPLS 4. The PLS-SEM analysis consisted of two main stages: measurement-model assessment and structural-model assessment. The measurement model was assessed to examine the reliability and validity of the construct indicators. The assessment included outer loadings, Cronbach's alpha, composite reliability, Average Variance Extracted, and the HeterotraitMonotrait Ratio.

Outer loading values above 0.70 indicate that an indicator has a strong relationship with its corresponding construct. Cronbach's alpha and composite reliability values above 0.70 indicate satisfactory internal consistency reliability. Average Variance Extracted values above 0.50 indicate convergent validity because the construct explains more than half of the variance in its indicators. The Heterotrait-Monotrait Ratio was used to assess discriminant validity. Heterotrait-Monotrait Ratio values below 0.85 or 0.90 indicate that the constructs are empirically distinct (Hair Joseph F et al., 2022; Henseler & Chin, 2010).

The structural model was assessed through direct-effect testing. The revised model included two structural relationships:

H1: Fraud Risk Indicators are positively associated with Internal Audit Effectiveness.
H2: Technology Capability is positively associated with Internal Audit Effectiveness.

The significance of the structural relationships was assessed using bootstrapping with 5,000 resamples. The evaluation included standardized path coefficients, t-values, p-values, and bootstrap confidence intervals. A hypothesis was considered supported when

Copyright to the author of some rights reserved This work is licensed under aCreative Commons Attribution-ShareAlike 4.0 International License.

International Journal of Business and Quality Research
https://e-journal.citakonsultindo.or.id/index.php/IJBQR
E-ISSN: 2985-9468

the path coefficient was in the predicted direction, the t-value exceeded 1.96, the p-value was below 0.05, and the confidence interval did not include zero.

The analysis also included inner Variance Inflation Factor values to assess potential collinearity between Fraud Risk Indicators and Technology Capability. Effect sizes were assessed using f square. Explanatory power was assessed using R square for Internal Audit Effectiveness. Predictive relevance was assessed using Q square. The study used the general interpretation that f square values of 0.02, 0.15, and 0.35 represent small, medium, and large effects, respectively. Positive Q square values indicate predictive relevance under the PLS-SEM blindfolding procedure (Hair Joseph F et al., 2022; Joseph F. Hair et al., 2019).

Research Model

The revised research model positions Internal Audit Effectiveness as the primary outcome variable. Fraud Risk Indicators and Technology Capability are positioned as exogenous variables. The model is stated as follows:

Fraud Risk Indicators -> Internal Audit Effectiveness
Technology Capability -> Internal Audit Effectiveness

In the public-sector context, the model proposes that structured fraud-risk information and organizational technology capability may strengthen Internal Audit Effectiveness. Improved Internal Audit Effectiveness may then support public-sector accountability through stronger stewardship, fraud-risk governance, internal control, information quality, audit prioritization, and oversight of state-controlled resources.

The study does not measure public accountability directly. Instead, public accountability is treated as the institutional context and governance implication of Internal Audit Effectiveness in SOEs. This position is consistent with the OECD emphasis on transparency, accountability, integrity, risk management, internal control, and audit in the governance of state-owned enterprises.

RESULTS

Measurement Model Assessment

The measurement model was assessed to evaluate indicator reliability, internal consistency reliability, and convergent validity for the three retained constructs: Fraud Risk Indicators, Technology Capability, and Internal Audit Effectiveness. The assessment used outer loadings, Cronbach's alpha, composite reliability, and Average Variance Extracted.

The measurement-model criteria required outer loadings above 0.70, Cronbach's alpha values above 0.70, composite reliability values above 0.70, and Average Variance

Copyright to the author of some rights reserved This work is licensed under aCreative Commons Attribution-ShareAlike 4.0 International License.

International Journal of Business and Quality Research
https://e-journal.citakonsultindo.or.id/index.php/IJBQR
E-ISSN: 2985-9468

Extracted values above 0.50. These criteria are commonly used in Partial Least Squares Structural Equation Modelling to evaluate whether the measurement instruments adequately represent the latent constructs (Hair Joseph F et al., 2022; Joseph F. Hair et al., 2019).

The results show satisfactory measurement quality for all three constructs. All outer loading values exceeded 0.70. Cronbach's alpha and composite reliability values exceeded 0.90, while all Average Variance Extracted values exceeded 0.50. These findings indicate satisfactory indicator reliability, internal consistency reliability, and convergent validity.

Table 3. Measurement Model Assessment

Construct	Outer Loading Range	Cronbach's Alpha	Composite Reliability	Average Variance Extracted
Fraud Risk Indicators (FH_RED)	0.760 to 0.880	0.924	0.924	0.671
Technology Capability (TECH_CAP)	0.810 to 0.890	0.914	0.914	0.728
Internal Audit Effectiveness (AUD_EFF)	0.820 to 0.890	0.917	0.918	0.736

Source: Primary data processed using SmartPLS 4.

Fraud Risk Indicators consisted of six indicators, with outer loading values ranging from 0.760 to 0.880. The construct obtained Cronbach's alpha of 0.924, composite reliability of 0.924, and Average Variance Extracted of 0.671. These values indicate that Fraud Risk Indicators were measured reliably and demonstrated convergent validity.

Technology Capability consisted of four indicators, with outer loading values ranging from 0.810 to 0.890. The construct achieved Cronbach's alpha of 0.914, composite reliability of 0.914, and Average Variance Extracted of 0.728. These results indicate that Technology Capability explained 72.8 percent of the variance in its indicators.

Internal Audit Effectiveness consisted of four indicators, with outer loading values ranging from 0.820 to 0.890. The construct achieved Cronbach's alpha of 0.917, composite reliability of 0.918, and Average Variance Extracted of 0.736. This result indicates that Internal Audit Effectiveness explained 73.6 percent of the variance in its indicators.

Copyright to the author of some rights reserved This work is licensed under aCreative Commons Attribution-ShareAlike 4.0 International License.

International Journal of Business and Quality Research
https://e-journal.citakonsultindo.or.id/index.php/IJBQR
E-ISSN: 2985-9468

The measurement-model results indicate that the retained constructs meet the criteria for reliability and convergent validity. The result supports the use of Fraud Risk Indicators, Technology Capability, and Internal Audit Effectiveness in the revised public-sector accountability model.

Discriminant Validity Assessment

Discriminant validity was assessed using the Heterotrait-Monotrait Ratio. The Heterotrait-Monotrait Ratio evaluates whether a construct is empirically distinct from other constructs in the model. Values below 0.85 are generally considered evidence of discriminant validity. Values below 0.90 may also be accepted when the constructs are theoretically related but remain conceptually distinct (Henseler et al., 2015).

The results indicate that all Heterotrait-Monotrait Ratio values were below 0.90. Therefore, Fraud Risk Indicators, Technology Capability, and Internal Audit Effectiveness can be treated as empirically distinct constructs.

Table 4. Heterotrait-Monotrait Ratio Assessment

Construct Pair	HTMT Value	Required Criterion	Decision
Fraud Risk Indicators and Technology Capability	0.684	Below 0.90	Discriminant validity established
Fraud Risk Indicators and Internal Audit Effectiveness	0.621	Below 0.90	Discriminant validity established
Technology Capability and Internal Audit Effectiveness	0.706	Below 0.90	Discriminant validity established

Source: Primary data processed using SmartPLS 4.

The highest Heterotrait-Monotrait Ratio value was observed between Technology Capability and Internal Audit Effectiveness, with a value of 0.706. This value remains below 0.90 and indicates that the two constructs, although theoretically related, are empirically distinguishable. The Heterotrait-Monotrait Ratio between Fraud Risk Indicators and Technology Capability was 0.684, while the value between Fraud Risk Indicators and Internal Audit Effectiveness was 0.621.

These results demonstrate that the revised model does not suffer from discriminant validity problems. Fraud Risk Indicators represent structured fraud-risk information, Technology Capability represents the organization's digital audit and information-

Copyright to the author of some rights reserved This work is licensed under aCreative Commons Attribution-ShareAlike 4.0 International License.

International Journal of Business and Quality Research
https://e-journal.citakonsultindo.or.id/index.php/IJBQR
E-ISSN: 2985-9468

governance capacity, and Internal Audit Effectiveness represents the effectiveness of the internal audit function in supporting governance, risk management, internal control, compliance, fraud prevention, and management follow-up.

Collinearity Assessment

Before testing the structural relationships, collinearity was assessed using inner Variance Inflation Factor values. Collinearity is not considered problematic when Variance Inflation Factor values are below 3.0. Values below 5.0 are generally considered acceptable in PLS-SEM.

The results show that all inner Variance Inflation Factor values were below 3.0. Therefore, collinearity was not a concern in the revised structural model.

Table 5. Inner Variance Inflation Factor Assessment

Predictor	Endogenous Construct	Inner Variance Inflation Factor	Decision
Fraud Risk Indicators	Internal Audit Effectiveness	1.879	No collinearity concern
Technology Capability	Internal Audit Effectiveness	1.879	No collinearity concern

Source: Primary data processed using SmartPLS 4.

The same Variance Inflation Factor value was obtained for both predictors because Fraud Risk Indicators and Technology Capability jointly explain Internal Audit Effectiveness in the revised model. The value of 1.879 is below 3.0, indicating that the correlation between the two predictors does not create a problematic multicollinearity condition.

Structural Model Assessment

The revised structural model examined two hypotheses:

H1: Fraud Risk Indicators are positively associated with Internal Audit Effectiveness.

H2: Technology Capability is positively associated with Internal Audit Effectiveness.

The structural relationships were tested using bootstrapping with 5,000 resamples. The assessment considered beta coefficients, standard deviations, t-values, p-values, and 95 percent bootstrap confidence intervals.

The results show that both hypotheses were supported. Fraud Risk Indicators had a positive and statistically significant relationship with Internal Audit Effectiveness.

Copyright to the author of some rights reserved This work is licensed under aCreative Commons Attribution-ShareAlike 4.0 International License.

International Journal of Business and Quality Research
https://e-journal.citakonsultindo.or.id/index.php/IJBQR
E-ISSN: 2985-9468

Technology Capability also had a positive and statistically significant relationship with Internal Audit Effectiveness.

Table 6. Direct Effects

Hyp.	Relationship	Beta	Std.Deviation	T-value	P-value	Interval Lower Bound	Interval Upper Bound	Decision
H1	Fraud Risk Indicators -> Internal Audit Effectiveness	0.287	0.066	4.348	Less than 0.001	0.158	0.413	Supported
H2	Technology Capability -> Internal Audit Effectiveness	0.416	0.063	6.603	Less than 0.001	0.293	0.536	Supported

Source: Primary data processed using SmartPLS 4.

Fraud Risk Indicators had a positive and statistically significant relationship with Internal Audit Effectiveness, with beta = 0.287, t-value = 4.348, and p-value less than 0.001. The 95 percent bootstrap confidence interval ranged from 0.158 to 0.413 and did not include zero. Therefore, H1 was supported.

This finding indicates that structured Fraud Risk Indicators are associated with higher Internal Audit Effectiveness. In the SOE context, fraud-risk information may help internal auditors identify high-risk activities, prioritize audit procedures, assess potential control weaknesses, direct audit resources toward vulnerable processes, and provide evidence-based recommendations for management action.

Technology Capability had a positive and statistically significant relationship with Internal Audit Effectiveness, with beta = 0.416, t-value = 6.603, and p-value less than 0.001. The 95 percent bootstrap confidence interval ranged from 0.293 to 0.536 and did not include zero. Therefore, H2 was supported.

This finding indicates that organizational technological infrastructure, data integration, Audit Data Analytics, continuous auditing, secure access to audit data, and digital auditor competence are associated with stronger Internal Audit Effectiveness. Technology Capability supports auditors in accessing organizational information, identifying anomalies, conducting more comprehensive audit procedures, improving risk-based audit planning, documenting evidence, and supporting management follow-up.

Technology Capability had a stronger relationship with Internal Audit Effectiveness than Fraud Risk Indicators. The difference between the beta coefficients suggests that

Copyright to the author of some rights reserved This work is licensed under aCreative Commons Attribution-ShareAlike 4.0 International License.

International Journal of Business and Quality Research
https://e-journal.citakonsultindo.or.id/index.php/IJBQR
E-ISSN: 2985-9468

organizational capability in data, technology, analytics, and digital competence represents a particularly important foundation for effective internal audit in SOEs.

Effect Size Assessment

The effect size analysis was conducted using f square to assess the substantive contribution of Fraud Risk Indicators and Technology Capability to Internal Audit Effectiveness. An f square value of 0.02 is interpreted as a small effect, 0.15 as a medium effect, and 0.35 as a large effect.

The results show that Fraud Risk Indicators had a medium effect on Internal Audit Effectiveness, while Technology Capability had a large effect.

Table 7. Effect Size Assessment

Relationship	F Square	Interpretation
Fraud Risk Indicators -> Internal Audit Effectiveness	0.134	Small to medium effect
Technology Capability -> Internal Audit Effectiveness	0.281	Medium to large effect

Source: Primary data processed using SmartPLS 4.

Fraud Risk Indicators had an f square value of 0.134. This result indicates a small to medium substantive contribution to Internal Audit Effectiveness. The result suggests that structured fraud-risk information is an important component of data-driven internal auditing, particularly for identifying risks to state-controlled resources, procurement integrity, reporting quality, and internal controls.

Technology Capability had an f square value of 0.281. This result indicates a medium to large substantive contribution to Internal Audit Effectiveness. Technology Capability therefore represents the stronger predictor of Internal Audit Effectiveness in the revised model.

The result reinforces the importance of viewing Technology Capability as an information-governance capability in SOEs. Investment in technology infrastructure, data integration, Audit Data Analytics, continuous auditing, cybersecurity, and digital auditor competence may improve the ability of internal audit functions to provide timely, relevant, reliable, and actionable assurance.

Explanatory Power and Predictive Relevance

The explanatory power of the revised model was assessed using R square, while predictive relevance was assessed using Q square. The revised model explains 46.8 percent of the variance in Internal Audit Effectiveness. This result indicates that Fraud Risk

Copyright to the author of some rights reserved This work is licensed under aCreative Commons Attribution-ShareAlike 4.0 International License.

International Journal of Business and Quality Research
https://e-journal.citakonsultindo.or.id/index.php/IJBQR
E-ISSN: 2985-9468

Indicators and Technology Capability jointly account for a moderate to substantial proportion of variation in Internal Audit Effectiveness among the participating internal auditors.

The Q square value was positive and above zero, indicating that the revised model had predictive relevance for Internal Audit Effectiveness.

Table 8. Explanatory Power and Predictive Relevance

Endogenous Construct	R Square	Q Square	Interpretation
Internal Audit Effectiveness	0.468	0.321	Moderate explanatory power and good predictive relevance

Source: Primary data processed using SmartPLS 4.

The R square value of 0.468 indicates that nearly half of the variance in Internal Audit Effectiveness was explained by Fraud Risk Indicators and Technology Capability. This finding is meaningful in a public-sector organizational environment, where Internal Audit Effectiveness may also be influenced by other factors not included in the model, such as auditor independence, auditor competence, management support, audit committee effectiveness, organizational culture, internal-control maturity, regulatory support, ethics culture, data quality, and information-technology governance.

The Q square value of 0.321 indicates that the model has good predictive relevance. This result suggests that Fraud Risk Indicators and Technology Capability have meaningful predictive value for Internal Audit Effectiveness in the participating SOEs.

Summary of Hypothesis Testing

Table 9. Summary of Hypothesis Testing

Hypothesis	Statement	Result
H1	Fraud Risk Indicators are positively associated with Internal Audit Effectiveness	Supported
H2	Technology Capability is positively associated with Internal Audit Effectiveness	Supported

Source: Primary data processed using SmartPLS 4.

Copyright to the author of some rights reserved This work is licensed under aCreative Commons Attribution-ShareAlike 4.0 International License.

International Journal of Business and Quality Research
https://e-journal.citakonsultindo.or.id/index.php/IJBQR
E-ISSN: 2985-9468

The results support both hypotheses. Fraud Risk Indicators and Technology Capability were positively and significantly associated with Internal Audit Effectiveness. Technology Capability had the stronger direct relationship and the larger effect size.

The findings indicate that effective internal auditing in Indonesian SOEs is associated with two complementary capabilities. First, internal audit functions require structured fraud-risk information to identify high-risk activities, assess control weaknesses, prioritize audits, and protect state-controlled resources. Second, internal audit functions require Technology Capability to access integrated information, conduct data analytics, monitor transactions, identify anomalies, document evidence, and provide timely assurance.

In public-sector accounting terms, the results suggest that Fraud Risk Indicators support the stewardship and fraud-prevention dimensions of accountability, while Technology Capability supports the information-governance and oversight dimensions of accountability. Together, these capabilities are associated with more effective internal auditing, which may support transparency, integrity, compliance, protection of state-controlled resources, and public-sector accountability in SOEs.

DISCUSSION

Overview of Findings

This study examined the relationships among Fraud Risk Indicators, Technology Capability, and Internal Audit Effectiveness in Indonesian state-owned enterprises. The study was positioned within the public-sector accounting and public accountability context because SOEs manage state-controlled resources while simultaneously pursuing commercial, strategic, developmental, and public-policy objectives. Therefore, effective internal auditing in SOEs is relevant not only to organizational efficiency but also to stewardship, transparency, integrity, compliance, fraud prevention, and accountability to the state as owner and to other relevant stakeholders.

The results supported both hypotheses. Fraud Risk Indicators had a positive and statistically significant relationship with Internal Audit Effectiveness, with beta = 0.287, t-value = 4.348, and p-value less than 0.001. Technology Capability also had a positive and statistically significant relationship with Internal Audit Effectiveness, with beta = 0.416, t-value = 6.603, and p-value less than 0.001. Technology Capability had the stronger direct relationship and the larger effect size, with f square = 0.281, compared with f square = 0.134 for Fraud Risk Indicators.

The model explained 46.8 percent of the variance in Internal Audit Effectiveness, with R square = 0.468. The Q square value of 0.321 also indicated good predictive relevance.

Copyright to the author of some rights reserved This work is licensed under aCreative Commons Attribution-ShareAlike 4.0 International License.

International Journal of Business and Quality Research
https://e-journal.citakonsultindo.or.id/index.php/IJBQR
E-ISSN: 2985-9468

These findings indicate that Fraud Risk Indicators and Technology Capability jointly represent important organizational conditions associated with Internal Audit Effectiveness in Indonesian SOEs.

The findings should not be interpreted as direct evidence that public accountability has improved. Public accountability was not measured directly through indicators such as public disclosure quality, stakeholder trust, public-service outcomes, fiscal performance, compliance outcomes, or transparency scores. Instead, Internal Audit Effectiveness was examined as an organizational mechanism that may support public accountability. This interpretation is aligned with the OECD Guidelines on Corporate Governance of State-Owned Enterprises, which emphasize that transparency regarding all material matters is essential for strengthening the accountability of SOE boards and management (OECD, 2018).

The findings also respond to recent international discussions concerning the changing role of internal auditing. Internal audit is increasingly expected to operate not only as a compliance-oriented assurance function but also as a strategic governance mechanism that supports organizational learning, risk management, internal-control integration, and accountability. Cantù et al., (2025) argue that internal auditing should be understood as a function that contributes to organizational learning and integration of internal controls rather than merely a periodic inspection activity.

Fraud Risk Indicators and Internal Audit Effectiveness

The results show that Fraud Risk Indicators had a positive and statistically significant relationship with Internal Audit Effectiveness. This finding supports H1 and indicates that structured fraud-risk information is associated with more effective internal audit activities in Indonesian SOEs.

Fraud Risk Indicators are highly relevant in SOEs because fraud and misconduct may threaten state-controlled resources, procurement integrity, asset management, financial reporting, investment activities, public-service obligations, compliance, and public confidence. The OECD identifies SOEs as entities facing distinctive integrity and corruption risks because they often operate in sectors involving substantial public assets, significant public procurement, strategic investments, regulatory interaction, and complex relationships between state ownership and enterprise management (OECD, 2018).

In this study, Fraud Risk Indicators were based on the Fraud Hexagon dimensions of pressure, opportunity, rationalization, capability, arrogance, and collusion. These dimensions provide a broad framework for examining financial, behavioural, organizational, control-related, and collusive conditions that may increase fraud vulnerability (Khamainy et al., 2022).

Copyright to the author of some rights reserved This work is licensed under aCreative Commons Attribution-ShareAlike 4.0 International License.

International Journal of Business and Quality Research
https://e-journal.citakonsultindo.or.id/index.php/IJBQR
E-ISSN: 2985-9468

The positive beta coefficient of 0.287 indicates that structured Fraud Risk Indicators are associated with stronger Internal Audit Effectiveness. This result suggests that auditors may perform more effectively when fraud risk is transformed into operational and observable warning signals. These signals may include unusual transaction values, duplicate or repeated payments, abnormal payment timing, unusual vendor patterns, inconsistent supporting documentation, segregation-of-duty conflicts, management override, unexplained journal entries, unusual contract amendments, related-party transactions, and irregular approval processes.

The result is consistent with Bonrath & Eulerich, (2024), who found that technology-based auditing techniques for risk identification are positively associated with the internal audit function's involvement in fraud prevention and detection. Their study reinforces the proposition that internal audit functions become more capable of fraud prevention and detection when they use technology-supported risk identification approaches.

The findings are also consistent with Sidauruk, (2024), who found that data analytics can improve anomaly detection and audit scope in fraud prevention and detection by Government Internal Supervisory Apparatuses at Indonesian ministries, institutions, and local governments. This evidence is particularly relevant because SOEs and government entities both operate within public-accountability environments in which fraud may affect public resources, institutional legitimacy, and stakeholder confidence.

From a public-sector accounting perspective, Fraud Risk Indicators support the stewardship function of internal audit. Stewardship involves the responsible protection, use, control, and reporting of resources entrusted to an organization. In the SOE setting, these resources include state capital, public assets, strategic investments, procurement budgets, infrastructure resources, and operational assets controlled on behalf of the state.

Fraud Risk Indicators can also support the accountability function of internal audit. Structured indicators provide a clearer basis for explaining why certain transactions, vendors, contracts, projects, subsidiaries, business units, or management decisions have been classified as high risk. This improves the traceability of audit planning and strengthens the evidence base for audit recommendations, management follow-up, and accountability of responsible officials.

Nevertheless, Fraud Risk Indicators should not be interpreted as direct proof that fraud has occurred. A fraud-risk indicator is an early warning signal. It may reflect fraud, error, weak controls, data-quality problems, legitimate exceptional transactions, or changes in organizational processes. Internal auditors should apply professional judgment, perform additional procedures, obtain corroborating evidence, and follow relevant investigative protocols before concluding that fraud has occurred.

Copyright to the author of some rights reserved This work is licensed under aCreative Commons Attribution-ShareAlike 4.0 International License.

International Journal of Business and Quality Research
https://e-journal.citakonsultindo.or.id/index.php/IJBQR
E-ISSN: 2985-9468

The practical implication is that Indonesian SOEs should develop structured Fraud Risk Indicators that are integrated into risk-based audit planning and continuous monitoring. The indicators should be adjusted to the organizational risk profile and cover high-risk areas such as procurement, contract management, vendor selection, expenditure, payroll, inventory, asset management, project implementation, investment, financial reporting, related-party transactions, and information-system access.

Technology Capability and Internal Audit Effectiveness

Technology Capability had the strongest direct relationship with Internal Audit Effectiveness. The result supports H2 and indicates that organizational capability in digital infrastructure, data integration, Audit Data Analytics, continuous auditing, secure audit-data access, and digital auditor competence is associated with more effective internal auditing.

The positive beta coefficient of 0.416 and the medium-to-large effect size of 0.281 indicate that Technology Capability is a substantive predictor of Internal Audit Effectiveness. This finding suggests that Technology Capability should not be treated as a purely technical support function. Rather, it should be understood as a governance and information-management capability that enables internal audit functions to access, analyse, interpret, and communicate relevant organizational information.

The finding is consistent with the Resource-Based View. Barney, (1991) argues that organizational resources create value when they are valuable, appropriately organized, and effectively deployed. Bahardwa j, (2000) similarly explains that information technology capability can improve organizational performance when it is integrated with organizational processes and competencies. In the current study, Technology Capability includes not only technology assets but also data integration, analytics capability, continuous auditing, secure information access, and digital auditor competence.

The finding is also consistent with recent international research on internal audit and organizational learning. Cantù et al., (2025) explain that internal audit functions contribute to organizational learning and internal-control integration when they interact effectively with organizational processes and governance structures. Technology Capability can strengthen this role by enabling internal auditors to identify patterns, trace transactions, analyse control exceptions, and communicate evidence-based findings more efficiently.

Technology Capability is particularly important for public-sector accountability because accountability depends on reliable, timely, relevant, traceable, and accessible information. In SOEs, internal auditors require integrated data to evaluate whether transactions are authorized, whether controls are operating effectively, whether public or

Copyright to the author of some rights reserved This work is licensed under aCreative Commons Attribution-ShareAlike 4.0 International License.

International Journal of Business and Quality Research
https://e-journal.citakonsultindo.or.id/index.php/IJBQR
E-ISSN: 2985-9468

state-controlled resources are adequately protected, whether fraud vulnerabilities are emerging, and whether management has implemented corrective action.

Technology Capability can enable internal auditors to move beyond manual and sample-based procedures toward broader transaction-population analysis, anomaly detection, continuous monitoring, risk scoring, dashboard reporting, and evidence-based audit planning. These capabilities are increasingly important in SOEs that operate through enterprise resource planning systems, digital procurement systems, electronic payments, complex supply chains, strategic investments, and geographically dispersed operational units.

The result is also supported by technology-acceptance research in auditing. Afsay et al., (2023) found that organizational factors, facilitating conditions, technology readiness, technology-task fit, Perceived Usefulness, and Perceived Ease of Use are among the factors affecting information-technology acceptance in auditing. Kim et al., (2009) similarly found that technology features and complexity affect technology acceptance among internal auditors. Although the present study does not examine technology acceptance as a separate construct, these studies support the broader conclusion that organizational technology conditions influence the effectiveness of technology-enabled audit work.

The practical implication is that Indonesian SOEs should build an integrated digital audit ecosystem. This ecosystem should include data integration, master-data governance, data-quality controls, secure audit-data access, analytics tools, continuous auditing protocols, risk dashboards, cybersecurity measures, documentation standards, and continuous professional development for internal auditors.

Technology investment should not be evaluated only in terms of software acquisition, licensing cost, or infrastructure availability. It should be evaluated using audit and governance outcomes, including improvements in risk identification, anomaly detection, audit coverage, control evaluation, quality of audit evidence, timeliness of audit reporting, implementation of audit recommendations, and reduction in recurring control weaknesses.

Relative Importance of Fraud Risk Indicators and Technology Capability

The comparative results indicate that Technology Capability had a stronger direct relationship with Internal Audit Effectiveness than Fraud Risk Indicators. Technology Capability had beta = 0.416 and f square = 0.281, while Fraud Risk Indicators had beta = 0.287 and f square = 0.134.

This result does not imply that Fraud Risk Indicators are less important for public-sector accountability. Instead, it indicates that structured fraud-risk information requires sufficient technological and information-governance capability before it can be translated

Copyright to the author of some rights reserved This work is licensed under aCreative Commons Attribution-ShareAlike 4.0 International License.

into effective audit work. Fraud Risk Indicators can help auditors understand where potential risks are located, but Technology Capability determines whether auditors can access relevant data, analyse transaction patterns, validate anomalies, document evidence, monitor controls, and communicate findings in a timely manner.

The findings therefore suggest that Fraud Risk Indicators and Technology Capability are complementary. Fraud Risk Indicators provide risk intelligence for audit planning and fraud prevention. Technology Capability provides the infrastructure, data availability, analytical capacity, and professional capability necessary to convert risk intelligence into audit procedures, audit evidence, recommendations, and management action.

This complementarity is important in SOEs. Technology infrastructure without fraud-risk orientation may lead to excessive data collection without strategic audit focus. Conversely, fraud-risk indicators without adequate data integration and analytical capability may result in fragmented risk assessment and delayed audit responses. SOEs should therefore align fraud-risk governance, data governance, technology investment, internal-control evaluation, and audit planning.

Public-Sector Accounting and Accountability Implications

This study contributes to public-sector accounting literature by positioning data-driven internal auditing as part of the accountability infrastructure of SOEs. Fraud Risk Indicators and Technology Capability should not be viewed solely as management or information-technology variables. In an SOE setting, they may support the stewardship, information, integrity, compliance, and oversight dimensions of public-sector accountability.

The first implication concerns stewardship. Fraud Risk Indicators may support the early identification of risks that threaten state-controlled resources. These risks may include procurement fraud, asset misuse, unauthorized expenditure, financial-reporting manipulation, collusion, conflicts of interest, contract irregularities, and non-compliance with policies or regulations. By identifying such risks early, internal auditors can support prevention, control improvement, and responsible management of state resources.

The second implication concerns information quality. Technology Capability can strengthen the availability, reliability, timeliness, completeness, and traceability of audit-related information. This is important because public accountability depends on the ability of governance bodies to obtain relevant information concerning how resources are used, whether controls are functioning, whether fraud risk is increasing, and whether management has responded to identified weaknesses.

The third implication concerns oversight. Internal Audit Effectiveness enables the internal audit function to provide risk-based assurance to boards of commissioners, audit

Copyright to the author of some rights reserved This work is licensed under aCreative Commons Attribution-ShareAlike 4.0 International License.

committees, management, ownership entities, and regulators. Effective internal audit functions can identify control weaknesses, communicate findings, recommend corrective action, and monitor whether management has implemented recommendations.

The OECD Guidelines on Corporate Governance of State-Owned Enterprises emphasize that transparency regarding material matters is essential for strengthening the accountability of SOE boards and management. The Guidelines also emphasize transparency, disclosure, integrity, professional ownership, sound internal controls, risk management, compliance, and audit arrangements (OECD, 2018).

The findings suggest that structured Fraud Risk Indicators and Technology Capability may assist SOEs in operationalizing these governance expectations. Data-driven internal auditing can convert transactional data, fraud-risk signals, and internal-control information into usable evidence for risk-based decisions, audit prioritization, accountability of management, and oversight by governance bodies.

This study does not measure public accountability directly. It does not establish that transparency, disclosure quality, public trust, service delivery, fiscal performance, or stakeholder satisfaction has improved. Rather, it demonstrates that Fraud Risk Indicators and Technology Capability are associated with Internal Audit Effectiveness, which is an organizational mechanism that may contribute to public accountability.

Practical Implications for Indonesian SOEs

The results provide several practical implications for Indonesian SOEs. First, SOEs should integrate Fraud Risk Indicators into annual and continuous risk-based audit planning. Audit plans should not be based only on periodic audit schedules, historical findings, or management requests. They should use structured fraud-risk signals to identify high-risk transactions, processes, vendors, projects, subsidiaries, and business units. The indicators should be reviewed periodically to reflect emerging fraud patterns, regulatory changes, system changes, procurement practices, and evolving organizational risks.

Second, SOEs should develop Technology Capability as a strategic governance resource. This requires investment in system interoperability, data integration, data governance, data-quality management, secure audit access, analytics tools, continuous auditing, cybersecurity, and digital competence development. Technology investments should be assessed according to their contribution to fraud prevention, risk identification, audit coverage, control evaluation, evidence quality, audit-report timeliness, and management follow-up.

Third, internal audit functions should collaborate closely with risk management, compliance, finance, procurement, legal, human resources, operational management, and

Copyright to the author of some rights reserved This work is licensed under aCreative Commons Attribution-ShareAlike 4.0 International License.

information technology functions. Fraud prevention and public accountability require coordinated organizational action. Internal audit can provide independent assurance, but management remains responsible for establishing effective controls, responding to audit findings, and ensuring that corrective action is implemented.

Fourth, boards of commissioners, audit committees, and ownership entities should evaluate internal-audit performance using outcome-oriented measures. Relevant measures include the timeliness of audit reporting, quality of audit recommendations, implementation rate of audit recommendations, number of anomalies identified, number of recurring findings, fraud losses prevented or recovered, improvement in internal controls, and quality of reporting to governance bodies.

CONCLUSION

This study examined the relationships among Fraud Risk Indicators, Technology Capability, and Internal Audit Effectiveness in Indonesian state-owned enterprises. The study was positioned within the public-sector accounting and public accountability context because SOEs manage state-controlled resources while simultaneously pursuing commercial, strategic, developmental, and public-policy objectives. Accordingly, internal auditing in SOEs should not be viewed only as an organizational control function. It is also an accountability-supporting mechanism that may contribute to stewardship, transparency, integrity, compliance, fraud prevention, and governance oversight.

The results supported both proposed hypotheses. Fraud Risk Indicators had a positive and statistically significant relationship with Internal Audit Effectiveness, with beta = 0.287, t-value = 4.348, and p-value less than 0.001. This finding indicates that structured fraud-risk information is associated with stronger internal audit performance. Fraud Risk Indicators may help auditors identify vulnerable transactions, high-risk processes, procurement irregularities, control weaknesses, potential collusion, unusual approvals, and other warning signals that require further examination.

Technology Capability also had a positive and statistically significant relationship with Internal Audit Effectiveness, with beta = 0.416, t-value = 6.603, and p-value less than 0.001. Technology Capability had the stronger direct relationship with Internal Audit Effectiveness and had a medium-to-large effect size, with f square = 0.281. This finding indicates that technological infrastructure, data integration, Audit Data Analytics,

Copyright to the author of some rights reserved This work is licensed under aCreative Commons Attribution-ShareAlike 4.0 International License.

International Journal of Business and Quality Research
https://e-journal.citakonsultindo.or.id/index.php/IJBQR
E-ISSN: 2985-9468

continuous auditing, secure audit-data access, and digital auditor competence are important organizational capabilities for improving internal audit performance in SOEs.

Fraud Risk Indicators had an f square value of 0.134, indicating a small-to-medium effect on Internal Audit Effectiveness. Although Technology Capability had the stronger effect, Fraud Risk Indicators remain substantively important because technology-based auditing requires risk intelligence to identify where audit attention should be directed. Fraud Risk Indicators and Technology Capability should therefore be treated as complementary capabilities. Fraud Risk Indicators provide the information needed to identify potential fraud vulnerability, while Technology Capability enables auditors to access data, analyze transactions, validate anomalies, document evidence, monitor controls, and communicate findings to relevant governance bodies.

The model explained 46.8 percent of the variance in Internal Audit Effectiveness, with R square = 0.468. The Q square value of 0.321 indicated good predictive relevance. These results suggest that the combination of Fraud Risk Indicators and Technology Capability provides a meaningful explanation of Internal Audit Effectiveness among the participating internal auditors and audit-related professionals in Indonesian SOEs.

The study contributes theoretically to public-sector accounting and public accountability literature by positioning data-driven internal auditing as part of the accountability infrastructure of SOEs. The study demonstrates that Fraud Risk Indicators and Technology Capability should not be interpreted solely as operational or information-technology variables. In an SOE setting, Fraud Risk Indicators support the stewardship and fraud-prevention dimensions of accountability, while Technology Capability supports the information-governance and oversight dimensions of accountability.

The study also contributes to the Resource-Based View by showing that Technology Capability may create organizational value when it is integrated with audit processes, risk management, internal-control evaluation, data governance, analytical tools, and auditor competence. Technology infrastructure alone is not sufficient. Its value depends on whether internal audit functions can use integrated, reliable, timely, and traceable information to support risk-based audit planning, evidence gathering, control assessment, fraud prevention, audit reporting, and management follow-up.

The findings have direct relevance to SOE governance. Boards of commissioners, audit committees, management, ownership entities, and regulators should regard Internal Audit Effectiveness as an important accountability mechanism. The OECD Guidelines on Corporate Governance of State-Owned Enterprises emphasize that transparency regarding material matters is essential for strengthening the accountability of SOE boards and management. The Guidelines also emphasize integrity, disclosure, internal control, risk

Copyright to the author of some rights reserved This work is licensed under aCreative Commons Attribution-ShareAlike 4.0 International License.

management, compliance, and audit arrangements as central elements of sound SOE governance.

REFERENCES

Afsay, A., Tahriri, A., & Rezaee, Z. (2023). A meta-analysis of factors affecting acceptance of information technology in auditing. International Journal of Accounting Information Systems, 49, 100608. https://doi.org/10.1016/j.accinf.2022.100608

Alles, M. G. (2015). Drivers of the Use and Facilitators and Obstacles of the Evolution of Big Data by the Audit Profession. Accounting Horizons, 29(2), 439–449. https://doi.org/10.2308/acch-51067

Appelbaum, D. A., Kogan, A., & Vasarhelyi, M. A. (2018). Analytical procedures in external auditing: A comprehensive literature survey and framework for external audit analytics. Journal of Accounting Literature, 40(1), 83–101. https://doi.org/10.1016/j.acclit.2018.01.001

Appelbaum, D., Kogan, A., & Vasarhelyi, M. A. (2017). Big Data and Analytics in the Modern Audit Engagement: Research Needs. Auditing: A Journal of Practice & Theory, 36(4), 1–27. https://doi.org/10.2308/ajpt-51684

Bahardwa j, A. S. (2000). A Resources-Based Perspective on Information Technology Capability and Firm Performance. Information Systems Research, 11(2), 169–196.

Barney, J. (1991). Firm Resources and Sustained Competitive Advantage. Journal of Management, 17(1), 99–120. https://doi.org/10.1177/014920639101700108

Bonrath, A., & Eulerich, M. (2024). Internal auditing's role in preventing and detecting fraud: An empirical analysis. International Journal of Auditing. https://doi.org/10.1111/ijau.12342

Branch, R. M. (2009). Instructional Design: The ADDIE Approach. Springer US. https://doi.org/10.1007/978-0-387-09506-6

Cantù, E., Langella, C., & Vannini, I. E. (2025). Making Sense of the Internal Audit Function: Toward Internal Controls Integration and Organizational Learning. Financial Accountability & Management, 41(2), 262–273. https://doi.org/10.1111/faam.12413

Copyright to the author of some rights reserved This work is licensed under aCreative Commons Attribution-ShareAlike 4.0 International License.

Creswell John W., & Creswell J. David. (2018). Research Design: Qualitative, Quantitative, and Mixed Methods Approaches (5th Edition). SAGE Publications. https://us.sagepub.com/en-us/nam/research-design/book25567

Fetters, M. D., Curry, L. A., & Creswell, J. W. (2013). Achieving Integration in Mixed Methods Designs—Principles and Practices. Health Services Research, 48(6pt2), 2134–2156. https://doi.org/10.1111/1475-6773.12117

Grossi, G., Papenfuß, U., & Tremblay, M.-S. (2015). Corporate governance and accountability of state-owned enterprises. International Journal of Public Sector Management, 28(4/5), 274–285. https://doi.org/10.1108/IJPSM-09-2015-0166

Hair Joseph F, G.Thomas M, Ringle Christian M., & Sarstedt Mark. (2022). A Primer on Partial Least Squares Structural Equation Modeling (PLS-SEM) (3th ed.). SAGE Publications. https://us.sagepub.com/en-us/nam/a-primer-on-partial-least-squares-structural-equation-modeling-pls-sem/book270548

Henseler, J., & Chin, W. W. (2010). A Comparison of Approaches for the Analysis of Interaction Effects Between Latent Variables Using Partial Least Squares Path Modeling. Structural Equation Modeling: A Multidisciplinary Journal, 17(1), 82–109. https://doi.org/10.1080/10705510903439003

Henseler, J., Ringle, C. M., & Sarstedt, M. (2015). A new criterion for assessing discriminant validity in variance-based structural equation modeling. Journal of the Academy of Marketing Science, 43(1), 115–135. https://doi.org/10.1007/s11747-014-0403-8

Issa, H., Sun, T., & Vasarhelyi, M. A. (2016). Research Ideas for Artificial Intelligence in Auditing: The Formalization of Audit and Workforce Supplementation. Journal of Emerging Technologies in Accounting, 13(2), 1–20. https://doi.org/10.2308/jeta-10511

Jhon W. Creswell, & Cheryl N. Poth. (2016). Qualitative Inquiry and Research Design : Choosing Among Five Approaches (4th ed.). SAGE Publications.

Joseph F. Hair, William C. Black, Barry J. Babin, & Rolp E. Anderson. (2019). Multivariate_Data_Analysis (8th ed.). United Kingdom Cengage Learning EMEA.

Khamainy, A. H., Amalia, M. M., Cakranegara, P. A., & Indrawati, A. (2022). Financial Statement Fraud: The Predictive Relevance of Fraud Hexagon Theory. Journal of Accounting and Strategic Finance, 5(1). https://doi.org/10.33005/jasf.v5i1.249

Copyright to the author of some rights reserved This work is licensed under aCreative Commons Attribution-ShareAlike 4.0 International License.

Kim, H.-J., Mannino, M., & Nieschwietz, R. J. (2009). Information technology acceptance in the internal audit profession: Impact of technology features and complexity. International Journal of Accounting Information Systems, 10(4), 214–228. https://doi.org/10.1016/j.accinf.2009.09.001

OECD. (2018). State-owned enterprises and corruption : what are the risks and what can be done? OECD Publishing.

Richins, G., Stapleton, A., Stratopoulos, T. C., & Wong, C. (2017). Big Data Analytics: Opportunity or Threat for the Accounting Profession? Journal of Information Systems, 31(3), 63–79. https://doi.org/10.2308/isys-51805

Sarstedt, M., Hair, J. F., Nitzl, C., Ringle, C. M., & Howard, M. C. (2020). Beyond a tandem analysis of SEM and PROCESS: Use of PLS-SEM for mediation analyses! International Journal of Market Research, 62(3), 288–299. https://doi.org/10.1177/1470785320915686

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

The Institute of Internal Auditors (IIA). (2024). International Professional Practices Framework (IPPF): Global Internal Audit Standards, Requirements, and Guedance. https://www.theiia.org/en/standards/

Vasarhelyi, M. A., Kogan, A., & Tuttle, B. M. (2015). Big Data in Accounting: An Overview. Accounting Horizons, 29(2), 381–396. https://doi.org/10.2308/acch-51071

Wade, M., & Hulland, J. (2004). Review: The Resource-Based View and Information Systems Research: Review, Extension, and Suggestions For Future Research1. MIS Quarterly, 28(1), 107–142. https://doi.org/10.2307/25148626

Copyright to the author of some rights reserved This work is licensed under aCreative Commons Attribution-ShareAlike 4.0 International License.