Assessing Fraud Risk Management Effectiveness in Logistics: A Case Study of PT. Lestari in Indonesia

Yuwono, M.A.[1,] Rachmawati, D.[2]
[1,2]Faculty of Business, Widya Mandala Catholic University
[1]andika.yuwono@gmail.com, [2]dyna@ukwms.ac.id

Abstract

This study examines how implementing an ISO 31000–based Enterprise Risk Management (ERM) framework enhances fraud risk management at PT Lestari. A qualitative naturalistic case study was conducted, involving semi-structured interviews with three PT Lestari managers (logistics, finance, and internal audit) and analysis of company risk registers and control documents. Applying ISO 31000–aligned ERM enabled systematic identification and prioritization of fraud risks, optimized resource allocation for internal controls, and introduced early warning indicators—collectively strengthening the company's fraud prevention capacity. By empirically validating ISO 31000 ERM in a single-case setting, the study clarifies how a structured risk framework can embed fraud risk management into daily operations. Organizations can adopt the ISO 31000 ERM process to integrate fraud risk assessment into existing workflows and foster a risk-aware culture. The single-case design with three managerial participants constrains the generalizability of results.

Keywords: *Risk management, ISO 31000, Fraud, ERM, Fraud risk management*

Received: 11th September 2024 / **Accepted:** 24th April 2025

Correspondence: andika.yuwono@gmail.com

ORCID of authors: Matias Andika Yuwono. https://orcid.org/0009-0008-1792-0985

DOI: https://doi.org/10.4038/kjm.v14i1.7827

Introduction

Fraud risk has emerged as a critical concern in the corporate environment, particularly as companies expand and face increasingly complex operational dynamics (Association of Certified Fraud Examiners, 2022). In Indonesia, rapid business development is not only characterized by growth opportunities but also by heightened exposure to financial misconduct, especially in core functions such as logistics and procurement (Tarjo et al., 2022). High-profile corporate scandals—such as the collapse of Bank Century in 2008, which incurred a government bailout of IDR 6.7 trillion due to the mismanagement and misappropriation of funds (Firdaus & Agus, 2018), and the case of Garuda Indonesia's revenue manipulation through premature recognition of income (Idris, 2022) — highlight the vulnerabilities in internal control systems and underscore the urgent need for robust fraud risk management (Tarjo et al., 2022).

Fraudulent activities, particularly in operational areas, often arise from gaps in governance and weak implementation of risk management frameworks (John et al., 2008). While literature extensively explores general risk management, the study of *fraud risk*—especially within specific business functions like logistics—remains underdeveloped. As supply chains grow more complex and globally interconnected, logistics divisions become increasingly susceptible to fraud risks such as data manipulation, unethical vendor relationships, and unauthorized procurement actions (Hassan et al., 2022). These risks not only cause direct financial losses but also damage corporate reputation and stakeholder trust (Andry et al., 2022; Hardjomidjojo et al., 2022).

In response to these challenges, Enterprise Risk Management (ERM) has gained prominence as a strategic approach that integrates risk awareness into decision-making processes. The ISO 31000:2018 framework, as a widely recognized standard, provides a structured methodology for identifying, analyzing, evaluating, and treating organizational risks, including those related to fraud (Dişli & Kilit, 2024; Wulandari & Natasari, 2018). However, while ISO 31000 offers a universal framework, it lacks specificity in its application to particular risk domains such as logistics fraud, and empirical studies on its practical integration within fraud risk contexts are still limited (Medina-Serrano et al., 2021).

Furthermore, existing research in Sustainable Supply Chain Risk Management (SSCRM) has primarily focused on environmental and operational risks, leaving fraud risks within the supply chain relatively unexplored. This creates a gap in both theory and practice, particularly regarding how sustainability goals can be embedded into fraud risk mitigation strategies within logistics operations (Ferramosca et al., 2017). Without such integration, logistics divisions remain exposed to vulnerabilities that threaten operational efficiency, cost stability, and long-term sustainability.

This study responds to that gap by examining how the ISO 31000:2018 framework can be operationalized to manage fraud risk within the logistics function. A case study is conducted at PT. Lestari, a company engaged in essential oils trading, where the logistics division plays a crucial role in handling the flow of goods. This division, due to its frequent interactions with suppliers and contractors, is particularly vulnerable to fraudulent activities such as bribery, data tampering, and procurement irregularities. The study explores the implementation of risk identification, analysis, and evaluation processes aligned with ISO 31000:2018 to build a tailored fraud risk management strategy (Medina-Serrano et al., 2021).

Given these considerations, the central Research Question (RQ) posed is: What are the essential elements of an effective Enterprise Risk Management (ERM) strategy for implementing fraud risk management in logistics operations? Accordingly, the

objective of this research is to identify, analyze, and evaluate the practical implementation of ISO 31000:2018 in mitigating fraud risk in the logistics division of PT. Lestari, and to propose a context-specific framework that addresses both the operational and strategic dimensions of fraud risk.

The remainder of this article is structured as follows: Section 2 provides a literature review focusing on ERM, fraud risk, and ISO 31000 applications. Section 3 details the research methodology, including case selection and data collection techniques. Section 4 presents the results based on PT. Lestari's logistics operations. Section 5 discusses the implications of the findings in relation to existing literature and proposes a contextual framework. Finally, Section 6 concludes with practical recommendations and avenues for future research.

Literature Review

Fraud

Fraud is a deliberate and intentional act of deviation aimed at obtaining personal or group benefits at the expense of others. According to Suryana & Sadeli (2015), fraud is a discrepancy between statements and actual conditions that causes harm to other parties. Moeller (2011) defines fraud as a deliberate act of deception that potentially causes loss to others. Karyono (2013) adds that fraud is a deviant action committed intentionally to achieve specific goals, such as misrepresenting information or exploiting certain conditions. Tunggal (2013) describes fraud as dishonest behavior intended to unlawfully acquire the property, intellectual rights, or ownership of others (Wibawa & Tobing, 2023).

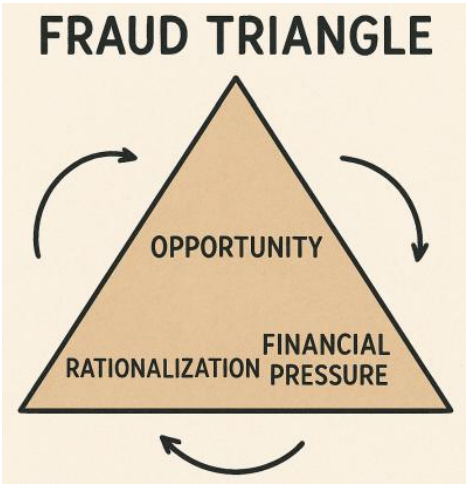


Figure 1: Fraud Triangle
Source: Developed by the researchers

One of the most recognized frameworks explaining the causes of fraud is the Fraud Triangle, introduced by Wells (2017), which includes:

a) Pressure, such as financial burdens, debt, or an extravagant lifestyle (Hermawan & Novita, 2021; Ramadhan, 2022).

b) Opportunity, arising from weaknesses in internal control systems that create the chance for fraud (Ramadhan, 2022).

c) Rationalization, which refers to the moral justification used by perpetrators to legitimize their fraudulent actions (Eltweri et al., 2021; Tarjo et al., 2022).

Common types of fraud include corruption, asset misappropriation, and financial statement fraud (Adebayo et al., 2022).

Risk Management

Risk management refers to a systematic and coordinated set of activities designed to identify, assess, and address risks within an organization (Qintharah, 2019). ISO 31000 outlines six key processes in risk management:

a) Communication and Consultation: Building a comprehensive understanding of risk among stakeholders (Nugroho & Pangeran, 2021).
b) Establishing the Context: Customizing the risk management framework according to the organization's environment (Andry et al., 2022).

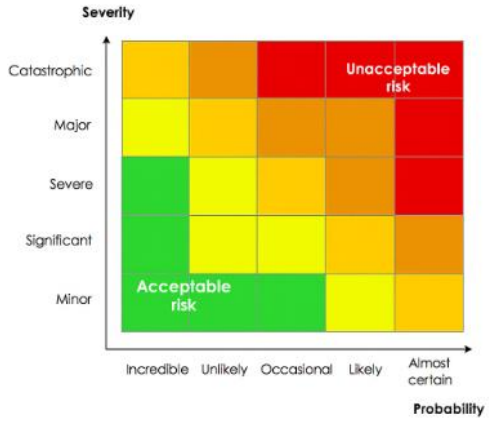


Figure 2: Risk Map
Source: Developed by the researchers

c) Risk Assessment, which includes:
   - Risk Identification using discussions, document reviews, and questionnaires (Susilo & Kaho, 2018).
   - Risk Analysis, evaluating the likelihood and impact of risks, and developing risk maps (Miftakhatun, 2020).
   - Risk Evaluation, comparing risk analysis results with predefined criteria to determine treatment priorities (Putra & Chan, 2017; Susilo & Kaho, 2018).
d) Risk Treatment: Designing and implementing mitigation strategies.
e) Monitoring and Review: Continuously assessing the effectiveness of risk responses and improving the system.
f) Recording and Reporting: Documenting the process as a basis for decision-making and risk communication.

Fraud Risk Management

Fraud Risk Management (FRM) is a structured approach to identifying, assessing, and mitigating fraud risks (Marzuki et al., 2020). Its key components include:

a) Formal policies that distinguish between actual fraud and fraud risk (Oyekan et al., 2023).

b) Risk identification and evaluation using risk questionnaires, process flowcharts, and data from auditors and regulators (Yang & Lee, 2020).

c) Risk assessment based on likelihood and impact, often visualized using a risk matrix (Hess & Cottrell, 2016).

d) Preventive strategies, such as internal controls, employee training, and whistleblower policies (Marzuki et al., 2020).

Through FRM, organizations and auditors can adopt a more proactive stance, foster an anti-fraud culture, and enhance stakeholder trust.

Previous Research

Previous studies have emphasized the importance of risk management and fraud risk management in fraud prevention. David (2017) highlights that risk management helps organizations identify and evaluate risks and increases preparedness for unexpected events. Pua et al. (2017) emphasize that effective fraud risk control strengthens internal audit functions.

Tarjo et al. (2022) find that implementing fraud risk management in local governments in Indonesia improves transparency, accountability, and internal control systems. Similarly, studies by Sulistiyo and Yanti's research (2022) and Alazzabi et al., (2023)

confirm that effective risk management positively impacts fraud prevention.

However, there are several research gaps, including:

a) Limited integration of ISO 31000 and Fraud Risk Management frameworks in specific sectors such as public organizations or manufacturing.
b) Lack of studies evaluating the effectiveness of risk management methods using data analytics or digital technology to detect fraud (Kzykeyeva, 2022).
c) Predominance of descriptive or case study approaches, while quantitative methods such as Structural Equation Modeling (SEM), Partial Least Squares (PLS), or regression analysis remain underutilized (Wijaya, 2015; Zunaedi et al., 2022).

Summary of Key Literature

To better understand the current landscape of research related to risk management, fraud risk management, and fraud prevention, Table 1 summarizes several key studies. These studies vary in focus, methodology, and findings, providing valuable insight into the academic and practical developments within this field.

Table 1: Summary of Previous Studies on Risk Management, Fraud Risk Management, and Fraud Prevention

Researcher & Year	Research Focus	Method	Key Findings
David (2017)	Risk Management (RM)	Literature review	RM is essential for risk identification and decision-making
Pua et al. (2017)	Fraud Risk Control (FRC) & Internal Audit	Survey	FRC strengthens internal audit
Tarjo et al. (2022)	Fraud Risk Management (FRM) in Local Government	Case study	FRM improves transparency and internal control
Sulistiyo & Yanti (2022)	Risk Management and Fraud Prevention	Quantitative	RM positively affects fraud prevention
Alazzabi et al. (2023)	Internal Control Weakness & Fraud	Literature & case study	Weak internal control increases fraud risk
Zunaedi et al. (2022)	Situational Factors Causing Fraud	Survey	Focus needed on highest-risk scenarios to prevent fraud
Marzuki et al. (2020)	Fraud Risk Management Strategy	Conceptual	FRM requires managerial and legal approaches
Oyekan et al. (2023)	Fraud Risk Policy & Governance	Policy study	Importance of separating actual fraud from fraud risk

Source: Developed by the researchers

The table shows that research in this area has employed a variety of approaches, including literature reviews, conceptual studies, case

studies, and quantitative methods. Most studies emphasize the importance of effective risk management and internal control mechanisms in preventing fraud. However, few have integrated both ISO 31000 frameworks and fraud risk management holistically, indicating an opportunity for further exploration in future research.

Recent studies reinforce the significance of digitization and technology-based approaches in enhancing risk management and fraud detection. Alazzabi et al. (2023) emphasize that integrating data analytics into internal audit systems is key to minimizing sophisticated fraud. Kzykeyeva (2022) also suggests that auditors must possess digital competencies and an understanding of big data to anticipate emerging fraud trends.

Methodology

This qualitative study adopts a case study approach focusing on PT. Lestari, particularly its logistics division. The logistics division was selected due to its high exposure to potential fraud risks, stemming from its central role in price negotiation and supplier selection. Strengthening internal controls in this area is thus critical, with risk management—particularly in line with ISO 31000:2018—as a vital mechanism to reduce such risks. The study emphasizes the risk assessment process, including risk identification, analysis, and evaluation.

Research Approach

This research is guided by a naturalistic paradigm, which is fundamentally suitable for qualitative inquiry. The naturalistic paradigm emphasizes understanding phenomena within their natural contexts and from the perspectives of the participants involved (Sugiyono, 2010). It assumes that reality is socially constructed and context-dependent, making it highly appropriate for exploring complex organizational phenomena such as fraud risk and internal control systems.

In the context of this study, the naturalistic paradigm is particularly relevant as it allows for an in-depth understanding of fraud risks and internal control mechanisms through the lived experiences of organizational actors. This paradigm aligns closely with the case study methodology, as both aim to produce rich, contextually grounded insights rather than generalizable truths. The interpretive nature of this paradigm enables the researcher to capture subtle dynamics and contextual nuances that influence risk-related decisions and behavior within the logistics division.

Research Subjects

The study employs purposive sampling to ensure the selection of information-rich cases relevant to the research objectives. Three key informants were selected from managerial positions in the logistics, finance, and internal audit departments based on their direct involvement with operational and control processes, as outlined in Table 2

Table 2: Informant Criteria

Position	Criteria
Logistics Manager (Informant 1)	Directly experiences fraud risks; involved in procurement decisions; affected by operational disruptions; authorized to implement corrective actions.
Finance Manager (Informant 2)	Oversees financial transactions and expenditures; monitors financial anomalies; provides independent and objective insights.

Internal Audit Manager (Informant 3)	Conducts audits and evaluates internal controls; maintains independence from operational departments; offers an objective assessment of fraud risks.

Source: Developed by the researchers

A total of three participants were interviewed. Interviews were conducted face-to-face in private meeting rooms at PT. Lestari's headquarters. Each interview lasted approximately 45–60 minutes and was conducted twice to ensure clarity and completeness. Data saturation was reached when no new themes or insights emerged during the second round of interviews

Data Types and Sources

This research combines qualitative and quantitative data. Qualitative data includes various documents and information related to company operations, such as operational standards, job descriptions, and documentation of activity implementation. Meanwhile, quantitative data is obtained from company financial reports such as purchase invoices, purchase orders, travel documents, purchase requisition data, inventory reports, etc. Data is collected both primarily through direct observation and interviews in the field and secondary through documents such as financial reports, purchase reports, and purchase order reports. Here are some examples of interview questions that are asked :

a) What types of fraudulent actions could occur in the logistics division?
b) Are these fraudulent actions harmful to the company?
c) Are there internal controls in place to prevent such fraudulent actions?
d) What do you think could be done to mitigate these fraudulent actions?
e) In your opinion, do logistics staff understand these fraudulent actions?

Data Collection Procedures

Data were collected through three key methods:

a) Structured interviews – interview guides were developed based on relevant literature and expert consultation. Prior to data collection, the instruments were pilot-tested with non-participant employees for clarity. Informed consent was obtained from all participants, and confidentiality was ensured by anonymizing all data and using pseudonyms.

b) Structured observation – researchers observed operational practices in the logistics division using predefined observation checklists focused on procurement, delivery, and control procedures.

c) Documentation review – internal documents relevant to procurement, finance, and auditing processes were examined to triangulate and contextualize the data.

Ethical approval was granted by the academic institution's ethics committee. Participants were informed about the study's purpose, and their right to withdraw at any time without consequences was clearly communicated.

Research Sites

PT. Lestari is a mid-sized manufacturing company based in West Surabaya, East Java, with approximately 300 employees. It operates in the consumer goods sector and has a complex supply chain that includes raw material procurement, warehousing, and distribution logistics. The logistics division is particularly critical, as it handles high-value

transactions and manages relationships with multiple external suppliers.

PT. Lestari was selected for this case study because it represents a typical medium-sized manufacturing enterprise with inherent fraud risk exposures in its logistics function. Its willingness to provide access to internal operations and documentation made it an ideal setting for studying fraud risk management in practice.

Data Analysis Technique

Data analysis followed the framework proposed by Miles and Huberman, as cited in Sugiyono (2010)., comprising four stages:

a) Data collection – gathering raw data through interviews, observation, and documents.

b) Data reduction – coding and summarizing data by identifying key themes and discarding irrelevant information. Manual coding was performed using color-coded themes, and the codes were reviewed by a second researcher to ensure inter-coder reliability.

c) Data display – organizing findings in matrices, narratives, and thematic summaries to facilitate interpretation.

d) Conclusion drawing and verification – developing provisional conclusions and continuously refining them through cross-verification with data sources and theoretical frameworks.

The data were analyzed manually without the use of software such as NVivo, but thematic consistency and analytical rigor were maintained through peer debriefing and code-checking sessions.

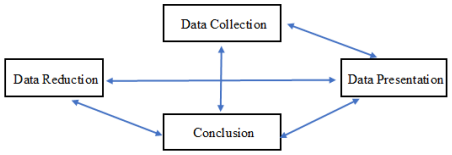


Figure 3: Data Analysis Techniques
Source: Developed by the researchers

Data Validity Criteria

To ensure the trustworthiness of the findings, several strategies were employed:

a) Credibility: achieved through triangulation of data sources (interviews, observations, documents), prolonged engagement with the site, and member checking by sharing summaries of findings with informants for feedback.

b) Dependability: ensured by maintaining an audit trail of the research process, including interview notes, coding frameworks, and reflective memos.

c) Confirmability: enhanced through reflexivity, where researchers critically examined their assumptions and biases throughout the study.

d) Transferability: supported by providing detailed contextual descriptions of PT. Lestari and its logistics operations to allow readers to assess the applicability of findings to similar settings.

Figure 4: Data Triangulation
Source: Developed by the researcher

Results and Discussion

Data Collection Procedures

This research employed qualitative methods through semi-structured interviews with three key informants at PT Lestari: the Logistics Manager, Finance Manager, and Internal Audit Manager. These interviews were conducted in August 2023 to identify fraud risks in the logistics division. The selection of these informants was based on their strategic roles in logistics operations, financial oversight, and risk monitoring. Each manager's role is briefly described below:

a) Logistics Manager: Oversees the flow of goods from the warehouse to the customer, ensuring smooth operations and addressing any logistical challenges.

b) Finance Manager: Responsible for verifying and approving financial transactions, maintaining sufficient operational funds, and ensuring the accuracy and compliance of all financial records.

c) Internal Audit Manager: Conducts periodic evaluations of both operational and financial procedures to assess internal control effectiveness and identify potential risks.

While these perspectives are critical, the decision to limit data collection to only three individuals, all from within the organization, introduces potential bias and limits the external validity of the findings. The exclusion of operational-level staff—such as warehouse supervisors or delivery personnel—may result in an incomplete understanding of day-to-day fraud risks. In addition, supporting documents such as meeting minutes and financial reports — including inventory reports, purchase orders, and other relevant records — were used to corroborate the interview data and enhance the credibility and depth of the analysis.

Despite this limitation, the study followed ISO 31000:2018's component of risk assessment, starting with risk identification, then analysis and evaluation. Initial risk identification was performed by the logistics manager and then analyzed collaboratively by the finance and internal audit managers. This participatory review aligns with the ISO 31000 guideline's emphasis on consultation and communication in risk management (Pribadi & Ernastuti, 2020; Susilo & Kaho, 2018).

Risk Assessment

The ISO 31000 risk assessment aims to identify risks followed by risk analysis and a risk evaluation process so that the company can determine practical actions to overcome these risks. The first process is the fraud risk identification process, which is carried out by interviewing the logistics division manager. From the interview results, six risks of activities in the logistics division that have the potential for fraud are obtained. The results of risk identification and an explanation of the risk of fraud carried out by logistics managers can be seen in Table 3 below.

Table 3: Logistics Division Fraud Risk Identification

ID	Types of Risk	Risk Explanation
F1	Acceptance of kickbacks from suppliers to the logistics division	Compensation from the supplier to the logistics division in the form of money, goods, or other forms should be provided to intervene with the logistics division in

		making decisions regarding the selection of suppliers for the procurement of transportation. This is often referred to as bribery.
F2	Embezzlement in the Delivery Process	Goods can be lost or stolen during shipping, which is then covered up by manipulation of shipping documents.
F3	Fraudulent invoices, such as double invoices,	The logistics division can collect invoices more than once so that the money can go into personal pockets.
F4	The emergence of fictitious orders for transportation vendor orders	This fictitious order did not occur, but payment can be made. Moreover, these payments can go into the Logistics division's pockets.
F5	Deviations in the Goods Receipt Process	Receiving goods from suppliers can be risky, as employees may receive goods that do not meet standards and record them as acceptable in the company system.
F6	Data Manipulation	The logistics division manipulates inventory data, such as stock levels, to cover theft or loss of goods.

Source: Developed by the researchers

The risk identification process carried out by logistics managers in this research was also discussed with financial and internal audit managers. The entire identification carried out by the three managers is subjective. This means that the risks that have been identified are based on personal experience and events that the logistics manager has experienced. Although there is an element of subjectivity in this process, this risk identification method remains by the ISO 31000 risk management standard, especially in the communication and consultation section. In this context, communication and consultation are interpreted as interactive processes in which information and views about potential risks are exchanged between various parties (Pribadi & Ernastuti, 2020; Susilo & Kaho, 2018).

After identifying the risks, an analysis is conducted to assess each risk's impact and likelihood using a semi-quantitative approach with a risk matrix. This matrix categorizes risks based on their impact (high, medium, low) and probability of occurrence (frequent, frequent, infrequent, very infrequent). For example:

- **Acceptance of kickbacks from suppliers (F1)** is evaluated as having a medium impact with a high likelihood. This is due to the frequent interactions between purchasing staff and suppliers, which increases the opportunity for corruption. A real-world scenario might involve a purchasing staff member accepting lavish gifts or money from a supplier in return for awarding contracts at preferential rates. On the other hand,

- **Embezzlement in the shipping process (F2)** is assessed to have a high impact and medium likelihood, mainly because it involves large quantities of high-value goods. An example would be a shipping employee diverting goods to the black market by falsifying shipping documents to reflect shipments that never occurred, thus profiting illegally from selling these goods.

- **Fake invoices (F3) and fictitious orders (F4)** are categorized as having a high impact but a low likelihood. These fraudulent activities demand significant collusion among various parties to be successful. An illustrative case might be logistics staff creating fake invoices for goods never ordered or received and then approving payments to fictitious companies, embezzling money for personal gain.

- **Discrepancies in goods receipt (F5)** and **data manipulation (F6)** are rated with medium impact and likelihood. Though these issues may not occur frequently, their cumulative effect can severely damage company data and inventory integrity. For instance, discrepancies might involve employees recording more goods than received and selling the excess for personal profit. Data manipulation could involve altering inventory records to obscure shortages caused by theft or administrative errors, ultimately undermining the accuracy of inventory management.

After the identification process, the next step in risk assessment is analyzing and evaluating each potential risk previously identified. In this stage, the logistics manager provides an evaluation or score for each possible risk based on the likelihood of its occurrence and the impact it might have if it did occur. This assessment or scoring is based on the probability level of an event or risk event. Table 4 below provides further details on assigning grades or scores based on probability levels.

Table 4: Levels of Risk Occurrence

Risk Level	Level of Possibility of Risk Occurrence	Information
1	Incredible	It can occur only in exceptional circumstances. It has yet to happen in the last five years.
2	Unlikely	It can happen at any time. At least, this has happened in the last five years.
3	Occasional	It can happen at any time. At least this happened in the previous three years
4	Likely	It may happen. At least this happened in the last one year
5	Almost Certain	Happens in most circumstances. It has happened more than once a year

Source: Developed by the researchers

Meanwhile, an explanation of the scoring based on the impact of existing risks can be seen in Table 5 below.

Table 5: Levels of Fraud Risk Impact

Risk Level	Severity	Information
1	Minor	Losses under IDR 1,000,000
2	Significant	Losses between IDR 1,000,000 – IDR 3,000,000

3	Severe	Losses between IDR 3,000,000 - IDR 5,000,000
4	Major	Losses between IDR 5,000,000 - IDR 10,000,000
5	Catastrophic	Losses above IDR 10,000,000

Source: Developed by the researchers

The risk scores in this study were determined by the informants through a collaborative process involving meetings and group brainstorming sessions. Informants were given the opportunity to assess the likelihood and impact of each identified risk based on their experiences, direct observations, and available data within their work environment. This participatory approach enabled consensus among stakeholders involved in the operations of the logistics division.

Based on the predetermined assessment criteria, the logistics division manager carries out a risk assessment from the level of occurrence to the impact resulting from the risks that have been identified. The results of the analysis and evaluation of fraud risk can be seen in Table 6 below.

Table 6: Results of Fraud Risk Analysis and Evaluation for Logistics Division (Informant 1)

Index	Probability (A)	Severity (B)	Risk Score (C = A x B)
F1	4	4	16
F2	2	5	10
F3	3	4	12
F4	3	5	15
F5	1	2	2
F6	2	4	8

Source: Developed by the researchers

Risk assessment applied a quantitative method in which the risk score was calculated by multiplying the likelihood (A) and impact (B), resulting in a Risk Score = A × B. While this approach assumes that likelihood and impact carry equal weight, it was considered valid and appropriate within the context of PT. Lestari, as it aligns with the company's internal risk assessment practices. The risk classification used the following scale: a score of 1–4 is categorized as low, 5–14 as moderate, 15–25 as high.

To facilitate the risk assessment, a risk map can be created with the following results:

PROBABILITY	SEVERITY				
	Minor (1)	Significant (2)	Severe (3)	Major (4)	Catastrophic (5)
Almost Certain (5)					
Likely (4)				F1	
Occasional (3)				F3	F4
Unlikely (2)				F6	F2
Incredible (1)		F5			

Figure 5: Logistics Division Fraud Risk Map

Source: Developed by the researchers

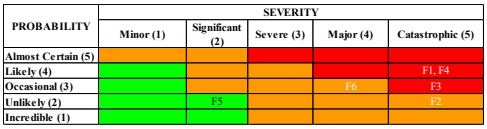
Then, the financial manager also carries out a risk assessment to validate and compare whether the logistics manager's results can be used as a source of accurate information. The results of the risk assessment carried out by the financial manager (informant 2) were as follows:

Table 7: Results of Fraud Risk Analysis and Evaluation for the Logistics Division Based on Informant 2's Assessment

Index	Probability (A)	Severity (B)	Risk Score (C = A x B)
F1	4	5	20
F2	2	5	10
F3	3	5	15
F4	4	5	20
F5	2	2	4
F6	3	4	12

Source: Developed by the researchers

Then, from the results of the risk assessment carried out by informant 2, a risk map can be created as follows:



PROBABILITY	SEVERITY				
	Minor (1)	Significant (2)	Severe (3)	Major (4)	Catastrophic (5)
Almost Certain (5)					
Likely (4)					F1, F4
Occasional (3)				F6	F3
Unlikely (2)		F5			F2
Incredible (1)					

Figure 6: Logistics Division, Fraud Risk Map, Based on Informant 2's Assessment
Source: Developed by the researchers

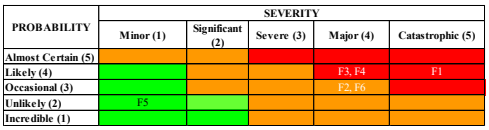
The internal audit manager carries out the following risk assessment as informant 3. Similar to the evaluation carried out by the financial manager, the risk assessment by the internal audit manager aims to validate and compare whether the results of the risk assessment carried out by the logistics manager can be used as a source. Accurate information. The results of the risk assessment carried out by the internal audit manager (informant 3) were as follows:

Table 8: Results of Fraud Risk Analysis and Evaluation for the Logistics Division Based on Informant 3's Assessment

Index	Probability (A)	Severity (B)	Risk Score (C = A x B)
F1	4	5	20
F2	3	4	12
F3	4	4	16
F4	4	4	16
F5	2	1	2
F6	3	4	12

Source: Developed by the researchers

Then, from the results of the risk assessment carried out by informant 3, a risk map can be created as follows:



PROBABILITY	SEVERITY				
	Minor (1)	Significant (2)	Severe (3)	Major (4)	Catastrophic (5)
Almost Certain (5)					
Likely (4)				F3, F4	F1
Occasional (3)				F2, F6	
Unlikely (2)	F5				
Incredible (1)					

Figure 7: Logistics Division, Fraud Risk Map, Based on Informant 3's Assessment
Source: Developed by the researchers

After going through the risk assessment process by the three informants, namely Informant 1, Informant 2, and Informant 3, it was found that the assessment results were similar. In other words, the risk assessment carried out by Informant 1 is generally in line with the evaluation carried out by Informant 2 and Informant 3. This process shows consistency in understanding and interpreting risk between the three informants. Comparing risk assessments is also in line with the stages of consultation in the ISO 31000 risk management standard. This consultation stage aims to reach a mutual agreement between all parties involved in the risk management process. This approach is designed to be systematic, measurable, and controllable (Susilo & Kaho, 2018).

After the three informants have analyzed and evaluated all potential risks, the next step is prioritizing based on the risk value. This prioritization process was carried out by sorting the risk values from highest to lowest based on the assessment results from the three informants. This will help companies determine which mitigation strategies should be addressed first according to their level of importance.

Differences in risk scores among informants were further analyzed to gain a deeper understanding of risk perceptions. For instance, in the case of Risk F3 (document forgery), one informant assigned a higher score due to direct experience with such incidents, while another rated it lower based on the belief that current internal controls were adequate. These variations highlight the importance of considering the background and personal experiences of each individual in risk identification.

Table 9: Comparison of Logistics Division Fraud Risk Priorities

Rank	Informant 1			Informant 2			Informant 3		
	ID	Score	Risk	ID	Score	Risk	ID	Score	Risk
1	F1	16	High	F1	20	High	F1	20	High
2	F4	15	High	F4	20	High	F3	16	High
3	F3	12	Medium	F3	15	High	F4	16	High
4	F2	10	Medium	F6	12	Medium	F2	12	Medium
5	F6	8	Medium	F2	10	Medium	F6	12	Medium
6	F5	2	Low	F5	4	Low	F5	2	Low

Source: Developed by the researchers

From the results of this comparison, the risks with the highest values are the risks F1, F3, and F4. From these results, it is concluded that accepting bribes (kickbacks) from suppliers to the logistics division (Index F1) poses a very high risk and can result in losses for the company of more than IDR 10,000,000, so intensive monitoring of this risk needs to be provided. The same thing also applies to the risk of committing fraud on billing invoices (fraudulent invoices), such as double invoices, which can cause potential losses for the company between IDR 5,000,000 and IDR 10,000,000. Thus, the fraud risk analysis process in the logistics division has been carried out appropriately based on ISO 31000 risk management, where risk analysis aims to understand the nature and behaviour of risks; this includes carrying out risk rankings so that the risk rankings can provide input for the risk evaluation process.(Atmojo & Manuputty, 2020; Susilo & Kaho, 2018)

The final stage in the risk assessment is to carry out a risk evaluation, wherein the company will determine what actions must be taken based on the results of the

risk analysis that has been carried out. Overall, logistics managers choose actions by reducing the five risks with the following details:

1. Risk F1: The company will create a code of ethics for the logistics division and provide strict sanctions for employees who violate it, such as accepting kickbacks or supplier offers. This is done because the company must have a clear and firm anti-bribery policy. This policy should clarify that all forms of bribery, including kickbacks, are illegal and unacceptable.

2. Risk F2: Each stage in the delivery process must be appropriately documented, including the time, date, and person responsible for each step. Then, you can use goods tracking technology such as GPS or RFID to monitor the movement of goods from the warehouse to the customer.

3. Risk F3: Implementing a digital invoice management system, where this system can help track and manage invoices efficiently. With a digital strategy, you can prevent duplicate invoices because each invoice has a unique code, which is then tightened by creating a verification procedure for each invoice received. This should include checking details such as date, quantity of goods, price per unit, and supplier.

4. Risk F4: This is done by ensuring that every transportation service order made by the logistics division is accompanied by a purchase requisition that the authorities have approved, and every transaction ordering transportation services is accompanied by a purchase order that both parties have agreed to.

5. Risk F5: Creating and implementing clear Standard Operating Procedures (SOP) for the goods receipt process. This SOP must cover every step from ordering to receiving and checking goods. In addition, the logistics division must carry out a thorough physical inspection of each item received to ensure that all products comply with the order and that there is no damage or shortages.

6. Risk F6: Separating data management and access duties where field operational officers cannot access the logistics database. Only the logistics admin is given access to the logistics database. Also, logistics admins are given limited access rights by their duties and responsibilities, such as deactivating editing facilities and deleting transactions.

After reducing this risk, PT must follow the following procedure: Lestari is a process of supervision and periodic review (monitoring and review). By regularly monitoring, it is hoped that the risk management implementation process will run according to the plan that has been determined.

Discussion

This Study identifies six key fraud risks in the logistics division of PT. Lestari: acceptance of kickbacks from suppliers, embezzlement in the shipping process, fake invoices, fictitious orders, discrepancies in goods receipt, and data manipulation. These findings are consistent with the literature indicating that logistics activities are vulnerable to various forms of fraud due to operational complexity and the involvement of multiple parties (Jarah et al., 2022; Soetjipto et al., 2021; Tewu et al., 2024). For instance, the risks of accepting kickbacks and embezzlement during the shipping process are expected in contexts where internal controls are weak, or there is a mismatch between company policies and their implementation (Brewster et al., 2021; Kerr et al., 2023).

According to the Fraud Triangle model by Wells (2017), opportunity, pressure, and rationalization are the key components that can trigger fraud within an organization, in the case of PT. Lestari, opportunities for fraud arise from weak controls and oversight in the goods receipt and shipping processes. Pressure might stem from high-performance targets or financial strain experienced by employees, while rationalization occurs if employees believe their fraudulent actions are justified or undetected.

In the context of PT. Lestari, these three components are evident in the identified cases. Here is an explanation of each element with examples:

- **Opportunity**: Opportunities for fraud arise from weak controls and oversight in the goods receipt and shipping processes. For example, in embezzlement in the shipping process, employees might exploit the lack of supervision to conceal shipped goods and divert them for personal gain. Without strict verification of the quantity of goods received against shipping documents, the opportunity for embezzlement increases.

- **Pressure**: Employee pressure can arise from high-performance targets or financial stress. For instance, if employees accept kickbacks from suppliers, they might feel pressured to meet unrealistic quota targets. This pressure could drive employees to take supplier bribes in exchange for prioritizing their products or ignoring proper procedures. Similarly, employees might feel compelled to commit fraud to cover their financial needs if they face personal financial problems.

- Rationalization occurs when employees believe their fraudulent actions are justified or not detected. For example, in

the case of fake invoices, an employee might justify submitting fraudulent invoices for services never rendered if they feel the company does not adequately reward their hard work. They might rationalize their actions as a form of "justice" or compensation for personal sacrifices.

Identifying these fraud risks has significant implications for the risk management framework at PT. Lestari. Findings related to kickbacks and embezzlement highlight the need for improvements in monitoring and internal audit processes. ISO 31000 suggests that organizations identify and assess risks and continuously monitor and review the effectiveness of implemented mitigation measures (Albrecht et al., 2010; Wicaksono, 2020). Therefore, PT. Lestari must ensure that existing controls reduce the likelihood and impact of identified risks.

Quantitative risk analysis techniques in this Study allow management to prioritize risks based on severity and likelihood. However, to enhance effectiveness, PT. Lestari should integrate this approach with qualitative reviews involving interviews and in-depth stakeholder discussions to gain a more comprehensive perspective (Austin, 2023; Dewi et al., 2023).

The findings of this Study can be linked to the concept of "Tone at the Top," which emphasizes the importance of leadership attitudes and actions in fostering a culture of ethics and integrity within an organization (Adebayo et al., 2022; Chabachib et al., 2020). Commitment from top management to risk management and fraud prevention will influence the organization to adhere to high ethical standards. Implementing "Segregation of Duties" is also an effective measure to prevent fraud by separating key responsibilities in business processes, thereby reducing opportunities for individuals to commit and conceal fraudulent actions (Gleim Publications, 2021; Zain, 2022).

This Study provides in-depth insights into fraud and risk management by integrating these findings with existing literature. It offers concrete recommendations to enhance the effectiveness of the risk management framework at PT Lestari. In addition to identifying risks, this study also explored the root causes of the risks encountered. Several contributing factors were identified, including weak internal controls, lack of job rotation, inadequate supervision by direct managers, and an organizational culture that heavily relies on interpersonal trust among employees. These root causes were associated with risks such as document falsification, inventory misappropriation, and inconsistencies in the procurement and goods receipt processes.

It is important to note that this study was deliberately scoped to focus exclusively on the logistics division. As such, it did not address the interrelationship of these risks with other departments or their integration into the company's overall risk register. Nonetheless, the company's risk appetite was discussed during the group meetings. Informants indicated that certain risks were still perceived to fall within acceptable boundaries. However, these discussions could not be explored in greater depth due to limitations in available data and time.

Conclusion

It turns out that from the results of implementing ISO 31000-based risk management in the logistics division at PT. Lestari found six fraud risks in the division, with details of two risks having a high impact, three with a medium effect, and one with a low blow. With this risk assessment process, companies can pay more attention or focus on risks with the most significant potential for fraud to reduce potential losses for the company. Focusing on threats with the most critical potential for fraud can help companies allocate resources more efficiently. Better power, such as overhauling the digitalization system during the tender process so that authorized parties can

document and control every transaction process. This aligns with a sound internal control system, and the potential for fraud can be reduced. Apart from that, by implementing risk management, companies can be better prepared to face unwanted surprises because they will continuously monitor all possible fraud within the company.

- **Implications for Management:**

a) Enhanced internal controls. PT Lestari must strengthen its internal controls and monitoring mechanisms to mitigate the identified risks. For instance, implementing a robust code of ethics to prevent kickbacks, utilizing tracking technologies to oversee the delivery process, and adopting digital invoice management systems can effectively address significant fraud risks. Improved segregation of duties and regular audits are essential to maintaining the integrity of operations.

b) Increased oversight and training. Management should invest in training programs to enhance employees' awareness of fraud risks and ethical behaviour. Regular updates and reinforcement of anti-fraud policies will help employees understand and adhere to ethical standards. Additionally, periodic reviews and audits of operational and financial processes will ensure that implemented controls remain practical and relevant.

c) Risk prioritization and resource allocation. The quantitative risk assessment ranks risks based on severity and likelihood. PT. Lestari should prioritize resources and interventions for the highest-risk areas, such as kickbacks and fraudulent invoices. Strategically allocating resources to address these high-priority risks will optimize the effectiveness of risk management efforts.

- **Academic Implications:**

a) Integration of quantitative and qualitative approaches. This Study demonstrates the value of integrating quantitative risk assessment techniques with qualitative interview insights. Combining these approaches offers a comprehensive understanding of risk dynamics and enhances the accuracy of risk evaluations. Future research should explore further integrating quantitative data with qualitative perspectives to improve risk management frameworks.

b) Application of fraud triangle theory. The findings align with the Fraud Triangle model, emphasizing the role of opportunity, pressure, and rationalization in triggering fraud. This application underscores the importance of addressing all three components in risk management strategies. Future studies could investigate how these elements interact in different organizational contexts and contribute to fraud prevention.

c) Impact of "Tone at the Top" and segregation of duties. The concept of "Tone at the Top" and segregating responsibilities are critical in fostering an ethical organizational culture. This Study contributes to the academic understanding of how leadership and structural controls influence fraud risk management. Further research could explore the effectiveness of these measures in various industries and their impact on organizational integrity.

The research has limited subjectivity in logistics, financial, and internal audit managers in providing risk assessments in the risk analysis process. Hence, the results of risk assessments have quite a significant impact. Their estimates are also based on personal experience in daily operational activities. The following limitation is that this research can only be carried out at PT. Lestari, because all operational and financial

activities only occur at that company, the analysis process and approach methodology can only be used at PT. Lestari.

Suggestion

Suggestions for further research are that the process of implementing risk management can be carried out in the logistics division and other divisions depending on the needs and goals the company wants to achieve. The next suggestion is that in addition to utilizing qualitative approaches, quantitative methods can also be employed in risk management to conduct a data- or financial report-based risk identification process. Using quantitative methods, identifying and assessing risks will involve monetary units, making the outcomes more quantifiable. Cash flow analysis and value at risk (VaR) analysis are examples of quantitative techniques used in risk identification and assessment.

Practically, other triangulation strategies, such as theoretical or methodological triangulation, could minimize interview bias during the risk identification and assessment process.

References

Adebayo, A. O., Olagunju, A., & Bankole, O. E. (2022). Fraud risk management and fraud reduction. *Malaysian Management Journal*, *26*. https://doi.org/10.32890/mmj2022.26.6

Alazzabi, W. Y. E., Mustafa, H., & Karage, A. I. (2023). Risk management, top management support, internal audit activities and fraud mitigation. *Journal of Financial Crime*, *30*(2), 569–582. https://doi.org/10.1108/JFC-11-2019-0147

Albrecht, W., Albrecht, C., & Zimbelman, M. (2010). *Fraud Examination* (4th ed.). South-Western College Publishing.

Andry, J. F., Liliana, L., Tannady, H., & Arief, A. S. (2022). Data Centre Risk Analysis Using ISO 31000:2009 Framework. *Journal of Physics: Conference Series*, *2394*(1), 012032. https://doi.org/10.1088/1742-6596/2394/1/012032

Association of Certified Fraud Examiner. (2022). *Fraud Examiners Manual* (Vol. 1).

Atmojo, S. A., & Manuputty, A. D. (2020). Analisis manajemen risiko teknologi informasi menggunakan ISO 31000 pada Aplikasi AHO Office. *JATISI (Jurnal Teknik Informatika Dan Sistem Informasi)*, *7*(3), 546–558. https://doi.org/10.35957/jatisi.v7i3.525

Austin, A. A. (2023). Remembering fraud in the Future: investigating and improving auditors' attention to fraud during audit testing. *Contemporary Accounting Research*, *40*(2), 925 – 951. https://doi.org/10.1111/1911-3846.12843

Brewster, B. E., Johanns, A. J., Peecher, M. E., & Solomon, I. (2021). do stronger wise-thinking dispositions facilitate auditors' objective evaluation of evidence when assessing and addressing fraud risk?. *Contemporary Accounting Research*, *38*(3), 1679 – 1711. https://doi.org/10.1111/1911-3846.12684

Chabachib, M., Irawan, B. P., Hersugondo, H., Hidayat, R., & Pamungkas, I. D. (2020). Corporate governance, firm performance and capital structure: Evidence from Indonesia. *Research in World Economy*, *11*(1), 48. https://doi.org/10.5430/rwe.v11n1p48

David, R. (2017). Contribution of records management to audit opinions and accountability in government. *SA Journal of Information Management*, *19*(1). https://doi.org/10.4102/sajim.v19i1.771

Dewi, Y., Suharman, H., Koeswayo, P. S., & Tanzil, N. D. (2023). What is the key determinant of Indonesia's credit card fraud risk assessment? An idea for brainstorming. *Banks and Bank Systems*, *18*(1), 26 – 37. https://doi.org/10.21511/bbs.18(1).2023.03

Dişli, G., & Kilit, R. M. (2024). Risk management and preventive conservation of cultural heritage: The case of Karaman Hatuniye Madrasa and Karaman City Museum. *IDRiM Journal*, *14*(1). https://doi.org/10.5595/001c.94366

Eltweri, A., Faccia, A., & KHASSAWNEH, O. (2021). Applications of big data within finance: Fraud detection and risk management within the real estate industry. *2021 3rd International Conference on E-Business and E-Commerce Engineering*, 67–73. https://doi.org/10.1145/3510249.3510262

Ferramosca, S., D', G., Onza, N. A., & Allegrini, M. (2017). The internal auditing of corporate governance, risk management and ethics: comparing banks with other industries. *International Journal of Business Governance and Ethics*, *12*(3), 218. https://doi.org/10.1504/IJBGE.2017.088245

Firdaus, & Agus. (2018, April 25). Kasus Bank Century - Never Ending Story. *Https://Antikorupsi.Org/Id*.

Gleim Publications. (2021). *Study Unit Four Risk Management*.

Hardjomidjojo, H., Pranata, C., & Baigorria, G. (2022). Rapid assessment model on risk management based on ISO 31000:2018. *IOP Conference Series: Earth and Environmental Science*, *1063*(1), 012043. https://doi.org/10.1088/1755-1315/1063/1/012043

Hassan, M. K., Abdulkarim, M. E., & Ismael, H. R. (2022). Risk governance: exploring the role of organizational culture. *Journal of Accounting & Organizational Change*, *18*(1), 77–99. https://doi.org/10.1108/JAOC-01-2021-0003

Hermawan, A., & Novita, N. (2021). The effect of governance, risk management, and compliance on efforts to minimize potential fraud based on the fraud pentagon concept. *Asia Pacific Fraud Journal*, *6*(1), 82. https://doi.org/10.21532/apfjournal.v6i1.196

Hess, M. F., & Cottrell, J. H. (2016). Fraud risk management: A small business perspective. *Business Horizons*, *59*(1), 13–18. https://doi.org/10.1016/j.bushor.2015.09.005

Idris, M. (2022, April 24). Skandal Korupsi di Garuda dari Masa ke Masa. *Kompas.Com*.

Jarah, B. A. F., Jarrah, M. A. AL, & Al-Zaqeba, M. A. A. (2022). The role of internal audit in improving supply chain management in shipping companies. *Uncertain Supply Chain Management*, *10*(3), 1023–1028. https://doi.org/10.5267/j.uscm.2022.2.011

John, K., Litov, L., & Yeung, B. (2008). Corporate governance and risk-taking. *The Journal of Finance*, *63*(4), 1679–1728. https://doi.org/10.1111/j.1540-6261.2008.01372.x

Karyono. (2013). *Forensik Fraud* (1st ed.). CV. Andi.

Kerr, D. S., Loveland, K. A., Smith, K. T., & Smith, L. M. (2023). Cryptocurrency risks, fraud cases, and financial performance. *Risks*, *11*(3). https://doi.org/10.3390/risks11030051

Kzykeyeva, A. (2022). Risk-Based approach to improving the quality of internal audit. *Quality - Access to Success*, *23*(189). https://doi.org/10.47750/QAS/23.189.26

Marzuki, M. M., Majid, W. Z. N. A., Azis, N. K., Rosman, R., & Abdulatiff, N. K. H. (2020). Fraud risk management model: A content analysis approach. *The Journal of Asian Finance, Economics and Business*, *7*(10), 717–728. https://doi.org/10.13106/jafeb.2020.vol7.no10.717

Medina-Serrano, R., González-Ramírez, R., Gasco-Gasco, J., & Llopis-Taverner, J. (2021). How to evaluate supply chain risks, including sustainable aspects? A case study from the

German industry. *Journal of Industrial Engineering and Management*, *14*(2), 120 – 134. https://doi.org/10.3926/jiem.3175

Miftakhatun, M. (2020). Analisis manajemen risiko teknologi informasi pada website ecofo menggunakan ISO 31000. *Journal of Computer Science and Engineering (JCSE)*, *1*(2), 128–146. https://doi.org/10.36596/jcse.v1i2.76

Moeller, R. (2011). *COSO Enterprise Risk Management: Establishing Effective Governance, Risk, and Compliance Processes, 2nd Edition* (2nd ed.).

Nugroho, R. L., & Pangeran, P. (2021a). Improving the performance of the balanced scorecard through implementing ISO 31000 risk assessment at shofa pharmacy. *EUREKA: Social and Humanities*, *1*, 23–36. https://doi.org/10.21303/2504-5571.2021.001635

Nugroho, R. L., & Pangeran, P. (2021b). Improving the performance of the balanced scorecard through implementing ISO 31000 risk assessment at shofa pharmacy. *EUREKA: Social and Humanities*, *1*, 23–36. https://doi.org/10.21303/2504-5571.2021.001635

Oyekan, M., Momoh, Z., Chinanuife, E., Jooji, I., & Okwara, E. C. (2023). Impact of fraud risk management and sustainability of small and medium enterprises in Abuja, Nigeria. *International Journal of Professional Business Review*, *8*(9), e03385. https://doi.org/10.26668/businessreview/2023.v8i9.3385

Pribadi, H. I., & Ernastuti, E. (2020). Manajemen Risiko Teknologi Informasi Pada Penerapan E-Recruitment Berbasis ISO 31000:2018 Dengan FMEA (Studi Kasus PT Pertamina). *Jurnal Sistem Informasi Bisnis*, *10*(1), 28–35. https://doi.org/10.21456/vol10iss1pp28-35

Pua, B. Y., Sondakh, J. J., & Pangerapan, S. (2017). Evaluasi fungsi auditor internal dalam pendeteksian dan pencegahan fraud PADA PDAM AIRMADIDI. *GOING CONCERN : JURNAL RISET AKUNTANSI*, *12*(2). https://doi.org/10.32400/gc.12.2.17881.2017

Putra, Z., & Chan, S. (2017). Desain manajemen risiko berbasis ISO 31000 pada pdam tirta meulaboh. *Jurnal Ekombis Fakultas Ekonomi Teuku Umar*, *3*(1).

Qintharah, Y. N. (2019). Perancangan penerapan manajemen risiko. *JRAK: Jurnal Riset Akuntansi Dan Komputerisasi Akuntansi*, *10*(1), 67–86. https://doi.org/10.33558/jrak.v10i1.1645

Ramadhan, D. (2022). Strengthening integrity and fraud awareness in preventing fraud during the covid-19 pandemic. *Asia Pacific Fraud Journal*, *7*(2), 213. https://doi.org/10.21532/apfjournal.v7i2.266

Soetjipto, N., Sulastri, S., Prastyorini, J., Soedarmanto, S., & Riswanto, A. (2021). Implementation of enterprise human resources management standards to achieve supply chain excellence in fertilizer companies in Indonesia. *Uncertain Supply Chain Management*, 107–114. https://doi.org/10.5267/j.uscm.2020.11.004

Sugiyono. (2010). *Metode Penelitian Pendidikan Pendekatan Kuantitatif, kualitatif, dan R&D.* Alfabeta.

Sulistiyo, A., & Yanti, H. B. (2022). Pengaruh pengendalian internal, manajemen risiko dan wistleblowing system terhadap pencegahan fraud. *Jurnal Akuntansi Dan Pajak*, *3*.

Suryana, A., & Sadeli, D. (2015). Analisis faktor - faktor yang mempengaruhi terjadinya fraud. *Jurnal Riset Akuntansi & Perpajakan (JRAP)*, *2*(02), 127–138. https://doi.org/10.35838/jrap.2015.002.02.12

Susilo, L. J., & Kaho, V. R. (2018). *Manajemen Risiko. Panduan Untuk Risk Leaders Dan Risk Practitioners*. PT. Gramedia Widiasarana Indonesia.

Tarjo, T., Vidyantha, H. V., Anggono, A., Yuliana, R., & Musyarofah, S. (2022). The effect of enterprise risk management on prevention and detection fraud in Indonesia's local government. *Cogent Economics & Finance*, *10*(1). https://doi.org/10.1080/23322039.2022.2101222

Tewu, M. L. D., Suwarno, S., Lisdiono, P., Friska, R., & Pramono, A. J. (2024). Enterprise risk management and supply chain management: The mediating role of competitive advantage and decision making in improving firms performance. *Uncertain Supply Chain Management*, *12*(2), 1131–1140. https://doi.org/10.5267/j.uscm.2023.11.021

Tunggal, A. W. (2013). *Pengendalian Internal: Mencegah dan Mendeteksi Kecuranga*. Harvarindo.

Wells, J. T. (2017). *Corporate fraud handbook* (5th ed.). John Wiley & Sons.

Wibawa, A. T., & Tobing, A. N. L. (2023). Maturity Level of Fraud Risk Management in Tax Institutions in Indonesia. *Ilomata International Journal of Tax and Accounting*, *4*(3), 584–598. https://doi.org/10.52728/ijtc.v4i3.765

Wicaksono, A. Y. (2020). Applying ISO:31000:2018 as Risk Management Strategy on Heavy Machinery Vehicle Division. *International Journal of Science, Engineering, and Information Technology*, *4*(2), 198–202. https://doi.org/10.21107/ijseit.v4i2.6871

Wijaya, A. (2015). Implementasi fraud risk management untuk meminimalkan risiko kecurangan (fraud) pada bagian produksi dan penjualan perusahaan makanan wanda putra kencana surabaya . *Jurnal Ilmiah Mahasiswa Universitas Surabaya*, *3*(2).

Wulandari, R., & Natasari, D. (2018). Desain dan Arsitektur untuk Memitigasi Fraud pada Organisasi Bisnis. *Jurnal Gama Societa*, *1*(1), 80. https://doi.org/10.22146/jgs.34052

Yang, C.-H., & Lee, K.-C. (2020). Developing a strategy map for forensic accounting with fraud risk management: An integrated balanced scorecard-based decision model. *Evaluation and Program Planning*, *80*, 101780. https://doi.org/10.1016/j.evalprogplan.2020.101780

Yesuf, A. S., Serna-Olvera, J., & Rannenberg, K. (2017). *Using Fraud Patterns for Fraud Risk Assessment of E-services* (pp. 553–567). https://doi.org/10.1007/978-3-319-58469-0_37

Yusuf, A. M. (2017). *Metode Penelitian: Kuantitatif, Kualitatif, Dan Penelitian Gabungan*. Kencana.

Zain, M. (2022). *Study Book CIA Part 1*.

Zunaedi, B. N. F., Annisa, H. R., & Dewi, M. (2022). Fungsi internal audit dan manajemen risiko perusahaan: sebuah tinjauan literatur. *Jurnal Bisnis Dan Akuntansi*, *24*(1), 59–70. https://doi.org/10.34208/jba.v24i1.1159