DIJMS: Dinasti International Journal of Management Science
E-ISSN: 2686-522X
P-ISSN: 2686-5211
https://dinastipub.org/DIJMS dinasti.info@gmail.com +62 811 7404 455

DOI: https://doi.org/10.38035/dijms.v7i2.6056

Operational Risk Management in Digital Logistics Companies

Rahmaddiansyah Rahmaddiansyah[1], Budi Supriyatno, Aziz Hakim[3]
[1]Universitas Krisnadwipayana, Jakarta, Indonesia, email. rdiansyah559@gmail.com
[2]Universitas Krisnadwipayana, Jakarta, Indonesia, email. budisupriyatno@gmail.com
[3]Universitas Krisnadwipayana, Jakarta, Indonesia, email. dr_azishakim@unkris.id

Corresponding Author: rdiansyah559@gmail.com[1]

Abstract: The development of the digital logistics industry, driven by the rapid growth of e-commerce, has led to increasing complexity of operational risks that directly affect service quality and corporate performance. This study aims to analyze operational risk management in digital logistics companies, with a particular focus on the processes of risk identification, assessment, and mitigation arising from operational activities, especially in last-mile delivery, warehouse management, and information technology systems. The research adopts a descriptive approach, employing data collection techniques such as interviews, observations, and document analysis. Risk analysis is conducted using a risk matrix to determine the likelihood and impact levels of operational risks. The results indicate that the dominant risks faced by the company include delivery delays, digital system disruptions, scanning errors (mis-scans), courier human error, and an increase in return-to-sender (RTS) cases. Risk mitigation strategies implemented by the company include improving the reliability of information technology systems, providing courier training, standardizing operational SOPs, and conducting real-time monitoring of delivery processes. However, the effectiveness of these mitigation measures is still constrained by high shipment volumes, dependence on third-party applications, and environmental variables in the field. This study recommends strengthening enterprise risk management, integrating AI-based tracking systems, and developing periodic risk evaluation mechanisms to enhance operational efficiency and sustainability in digital logistics companies.

Keyword: Risk Management, Operational Risk, Digital Logistics, Last-Mile Delivery, E-Commerce.

INTRODUCTION

The development of information technology and the increasing use of e-commerce platforms have driven significant growth in the digital logistics industry. Logistics companies no longer function solely as delivery service providers but have become an integral part of the digital ecosystem that connects sellers, customers, and data-driven technological systems. Digital logistics business models demand high levels of speed, accuracy, transparency, and real-time tracking capabilities. This condition creates an increasingly complex operational

environment that is vulnerable to various risks.

Operational risks in digital logistics companies may arise from multiple sources, including information technology system disruptions, scanning process errors (mis-scans), delivery delays, data discrepancies, courier errors, goods damage, and the increasing incidence of return-to-sender (RTS) cases. These risks have a direct impact on corporate reputation, operational costs, efficiency, and customer satisfaction levels. As shipment volumes continue to increase annually, a company's ability to manage operational risks becomes a critical factor in maintaining business sustainability and competitiveness.

Operational risk management plays a strategic role in ensuring that business processes operate in accordance with established standards, minimizing operational disruptions, and anticipating potential losses. International standards such as ISO 31000 and COSO ERM provide frameworks that companies can adopt to identify, assess, mitigate, and monitor risks on an ongoing basis. However, in many digital logistics companies, the implementation of risk management is often constrained by field operational dynamics, dependence on third-party applications, variations in courier behavior, and limitations in system integration.

Changes in consumer behavior in the digital era have also increased pressure on logistics companies to achieve higher levels of delivery speed and accuracy. Minor errors in operational processes can significantly affect customer experience and may lead to financial losses and declining customer loyalty. Therefore, the implementation of effective operational risk management has become an unavoidable necessity.

Based on the above discussion, this study is important to analyze the types of operational risks faced by digital logistics companies, evaluate the mitigation strategies that have been implemented, and provide recommendations to enhance the effectiveness of operational risk management in a dynamic digital context. This research is expected to contribute both theoretically and practically to the development of risk management practices in the modern logistics industry.

METHOD

This study employs a descriptive qualitative approach aimed at analyzing and providing an in-depth description of the operational risk management processes in digital logistics companies. This approach is selected because it enables a comprehensive understanding of operational risk phenomena, including their occurrence, handling mechanisms, and the factors influencing them within a technology-based logistics environment.

1. Type and Research Approach

This study is a qualitative descriptive research focusing on data collection through observations, interviews, and document analysis. The qualitative approach is employed to explore contextual, in-depth, and dynamic information related to operational activities, operational challenges, and the risk mitigation strategies implemented by the company.

2. Research Location and Subjects

The research was conducted at one of the digital logistics companies in Indonesia that provides last-mile delivery services, sorting operations, and digital system integration. The research subjects consisted of operational managers, warehouse supervisors, information technology staff, and couriers who are directly involved in daily operational activities and risk management processes: a) Operational supervisors; b) Couriers or riders; c) Warehouse staff; d) Information technology staff or system support teams; and e) Risk managers or operational managers.

The selection of research subjects was conducted using purposive sampling, based on the relevance of their roles in the operational risk management process.

3. Data Collection Techniques

a. In-depth Interviews
In-depth interviews were conducted with key informants, including operational managers, warehouse leaders, and information technology staff, to obtain data regarding operational procedures, potential risks, and risk mitigation strategies.

b. Field Observation
Field observations were conducted during package sorting processes, inbound–outbound operations, line haul activities, and last-mile delivery to directly identify sources of operational risk.

c. Documentation

d. Document analysis was carried out using the following sources: 1) Operational standard operating procedures (SOPs); 2) Delivery delay reports; 3) Return to Sender (RTS) data; 4) System error logs; 5) Organizational structure documents; 6) Company risk reports.

Data triangulation was employed to ensure the credibility and validity of the information obtained.

4. Data Analysis Techniques

Data analysis was conducted using the Miles and Huberman interactive model, which consists of the following stages:

a. Data reduction: Selecting and focusing on data relevant to operational risks.
b. Data display: Organizing research findings into narrative texts, tables, and risk categories.
c. Conclusion drawing and verification: Interpreting risk patterns, underlying causes, and the effectiveness of mitigation strategies.

Risk assessment was carried out using a 5×5 risk matrix that evaluates:

1) Likelihood (probability of occurrence),
2) Impact (severity of consequences).

The results of this assessment were used to determine risk levels, categorized as low, moderate, high, and extreme.

5. Data Validation Techniques

Data validity was ensured through:

a. Source triangulation,
b. Method triangulation,
c. Informant discussions for member checking.

This approach ensures that the research findings are accurate, credible, and accountable.

RESULTS AND DISCUSSION

1. Overview of Operational Risks in Digital Logistics Companies

The research findings indicate that digital logistics companies face more complex operational risks compared to conventional logistics firms. This complexity arises from a high dependence on digital systems, real-time data interactions, and increasing fluctuations in shipment volumes. Operational risks can be classified into several main categories, namely:

a. Information technology risks: server disruptions, application failures, tracking system errors, and delays in data updates.
b. Operational process risks: scanning errors (mis-scans), sorting errors, package misplacement, data inconsistencies, and route inaccuracies.
c. Human resource risks: courier errors, non-compliance with standard operating procedures (SOPs), moral hazard, and unpreparedness in handling shipment surges.
d. Customer service risks: increasing customer complaints, return-to-sender (RTS) cases, and discrepancies in delivery status.

These findings demonstrate that operational risks emerge from the interaction of both internal and external factors within a dynamic digital logistics environment.

2. Analysis of Operational Risk Identification

The company has implemented risk identification processes through operational reports, customer complaint data, internal audits, and real-time monitoring systems. However, the identification process has not yet been fully structured and does not employ a framework-based approach such as ISO 31000 or COSO ERM. Risk identification is predominantly reactive, occurring after operational incidents have taken place, rather than being conducted proactively through periodic risk mapping. This condition affects the company's ability to achieve an optimal and comprehensive understanding of the root causes of operational risks. For example, recurring mis-scan incidents could have been identified at the courier training stage; however, investigations are typically initiated only after customer complaints are submitted.

3. Risk Assessment Analysis

Risk assessment was conducted using a risk matrix to map the levels of likelihood and severity of impact. The analysis identified several risks categorized as high, including:

a. Application and server disruptions, which affect delays in package status updates.
b. Delivery delays, particularly during peak seasons.
c. Courier human errors, such as incorrect addresses, data input errors, and routing mistakes.
d. High levels of Return to Sender (RTS), which increase logistics costs and operational burdens.

Risks classified as moderate include minor goods damage, sorting errors, and delays in warehouse processing. Meanwhile, low-level risks, such as minor scanner device malfunctions, can be addressed promptly through quick responses from the internal IT team. The risk assessment results indicate that the most dominant risks affecting company performance are those related to the reliability of digital systems and the behavior of field couriers

4. Analysis of Operational Risk Mitigation Strategies

The company has implemented several risk mitigation strategies; however, their effectiveness varies. The following discussion outlines the effectiveness of mitigation efforts based on the research findings:

a. Information Technology Risk Mitigation
   The company has increased server capacity, implemented data backup systems, and strengthened application security encryption. Nevertheless, challenges continue to arise during periods of high traffic, particularly during e-commerce promotional campaigns. The main weaknesses include the absence of adequate redundant systems and limited auto-scaling capabilities.
b. Operational Process Risk Mitigation
   Package scanning procedures have been standardized; however, their implementation in the field is often inconsistent. The company has begun deploying automated sensors in warehouses (barcode gates), but coverage remains limited across all operational areas. A key weakness is that standard operating procedures (SOPs) are not consistently followed by couriers when delivery workloads are high.

c. Human Resource Risk Mitigation
Courier training programs are conducted periodically; however, not all couriers participate due to the high proportion of outsourced personnel. Weaknesses include limited field supervision and the presence of moral hazard, such as couriers failing to deliver packages directly to customer addresses while marking them as delivery failures.

d. Customer Service Risk Mitigation
The company provides digital complaint features and live chat support; however, complaint resolution processes remain slow. A significant limitation is the absence of an AI-based risk assessment system to detect potential delivery delays or failures before they occur. Overall, while risk mitigation strategies have been implemented, they have not yet been fully integrated into a comprehensive enterprise risk management framework

5. Supporting and Inhibiting Factors in the Implementation of Risk Management

a. Supporting Factors
1) The availability of digital technology support that enables real-time shipment monitoring.
2) Management commitment to improving the reliability of applications and operational systems.
3) A data-driven work culture that accelerates incident reporting and decision-making processes.
4) Investment in warehouse automation, such as conveyor systems and automatic sorting technologies

b. Inhibiting Factors
1) Extremely high shipment volumes, particularly during promotional periods.
2) Dependence on outsourced couriers, resulting in inconsistent service quality control.
3) Reliance on third-party APIs for tracking and data integration.
4) Lack of coordination between operational and IT teams, leading to delays in resolving system disruptions.
5) The absence of regular, in-depth risk evaluations aligned with international standards.

6. Research Implications

a. Theoretical Implications
This study reinforces the theory that operational risks in digital industries possess unique characteristics, particularly their strong dependence on information systems and real-time data interactions. These findings extend the discussion of ISO 31000 and COSO ERM concepts within the specific context of digital logistics.

b. Practical Implications
The study proposes several recommendations that can be implemented by digital logistics companies, including:
1) The implementation of AI-based predictive risk systems;
2) Enhanced integration between internal applications and third-party platforms;
3) Strengthened courier training and evaluation mechanisms;
4) The establishment of Key Risk Indicators (KRIs).

c. Implikasi Kebijakan
Hasil penelitian dapat menjadi dasar bagi regulator untuk menyusun panduan manajemen risiko operasional di industri logistik digital, termasuk standar pelacakan, keamanan data, dan sertifikasi kurir.

7. Policy Implications

The findings of this study may serve as a reference for regulators in formulating operational risk management guidelines for the digital logistics industry, including standards for tracking systems, data security, and courier certification.

CONCLUSION

Based on the research findings and discussion on operational risk management in digital logistics companies, several conclusions can be drawn:

a. Digital logistics companies face complex operational risks due to their high dependence on information technology, increasing shipment volumes, and dynamic field operations. The main risks include digital system disruptions, delivery delays, scanning errors (mis-scans), courier human errors, and high levels of Return to Sender (RTS).
b. Risk identification processes have been implemented; however, they remain largely reactive and have not fully aligned with established risk management frameworks such as ISO 31000 or COSO ERM. Risk identification tends to occur after incidents arise, resulting in suboptimal risk mapping.
c. Risk assessment results indicate that the most dominant risk categories are those affecting the reliability of digital systems and courier performance, as these risks have a direct impact on service quality and customer satisfaction.
d. The company has implemented various risk mitigation strategies, including improving application reliability, standardizing SOPs, conducting courier training, and implementing real-time monitoring. Nevertheless, the effectiveness of these mitigation efforts remains limited due to inconsistencies in SOP implementation, technological constraints, high shipment volumes, and dependence on third-party applications.
e. Supporting factors for the implementation of risk management include digital technology support, management commitment, an incident-reporting culture, and investment in warehouse automation. In contrast, inhibiting factors include reliance on outsourced couriers, suboptimal data integration, the lack of periodic risk evaluations, and ineffective internal coordination.

Overall, this study demonstrates that a more systematic, measurable, and sustainable implementation of operational risk management is essential to enhance efficiency, accuracy, and operational sustainability in digital logistics companies.

Based on the research findings, several recommendations can be proposed as follows:

a. Adopt internationally recognized risk management frameworks such as ISO 31000 or COSO ERM to strengthen proactive processes of risk identification, analysis, mitigation, and monitoring.
b. Enhance the reliability of information technology systems through the implementation of redundant servers, auto-scaling features to handle traffic surges, and more stable data integration between internal applications and third-party platforms.

c. Strengthen courier supervision and training, particularly for outsourced couriers, by establishing competency standards, certification mechanisms, and performance monitoring based on Key Risk Indicators (KRIs).
d. Develop AI-based predictive risk technologies to identify potential delivery delays, scanning errors, and delivery failures at an early stage, enabling corrective actions before risks materialize.
e. Improve consistency in the implementation of operational SOPs through periodic internal audits, regular performance evaluations, and the involvement of all business units in risk assessments.
f. Conduct periodic risk evaluations, at least on a quarterly basis, involving operational teams, IT personnel, risk management units, and customer service departments to ensure that mitigation strategies are implemented effectively and aligned with organizational objectives.
g. Build stronger interdepartmental coordination, particularly between operational and IT teams, to ensure that operational disruptions are addressed more quickly and effectively.

REFERENCE

Anwar, M. (2020). *Operational risk analysis in the logistics industry in Indonesia* [in Indonesian].

Sutanto, A. (2021). *The impact of digital systems on operational performance of logistics companies* [in Indonesian].

Wijaya, F. (2022). *Risk management in goods distribution processes of expedition service companies* [in Indonesian].