International Conference on Economy, Management, and Business (IC-EMBus)
VOL. 1, 2023 p. 2030–2040
https://journal.trunojoyo.ac.id/icembus

Enhancing Company Performance Through Risk Governance Evaluation Based on ERM ISO 31000:2018 Facilitated by Internal Auditors

Matias Andika Yuwono[1], Lena Ellitan[2]
[1,2] Business Faculty, Universitas Katolik Widya Mandala Surabaya

INFO ARTIKEL

Keywords:

Risk Governance, Iso 31000, ERM, Enterprise Risk Management, Three Lines Method, Internal Audit.

Abstract

In increasingly complex and dynamic business developments, this research analyzes the strategic role of internal auditors in assessing risk governance in an organization using the ISO: 31000 enterprise risk management approach and its implications for corporate performance. The assurance process carried out by internal audit can use the three-line method approach. The three-line method approach prioritizes the importance of the role of three interrelated lines of defense, namely: the first line (operational), which is the front part of the company that faces risks; the second line (supervision) which acts as the controller and supervisor of the first line, then the third line, namely internal audit which functions as the party that carries out independent evaluation and analysis of the control performance. The research that has been carried out has shown that internal audit plays a vital role in implementing ERM, such as identifying and assessing risks that may arise in the company and then providing recommendations on internal controls that are not yet effective in delivering added value to the company. Apart from that, practical assurance activities by internal auditors can provide benefits in optimizing risk governance, which can create a sound risk culture in every company's operational activity.

✉ Corresponden Author
(*) Matias Andika Yuwono

Email:
andika.yuwono@gmail.com[1]

E-ISSN: 3026-0965

DOI :

Introduction

Contains In the era of globalization and increasing business complexity, companies must have adaptive capabilities in facing various risks that can hinder achieving organizational goals. Enterprise Risk Management (ERM) has been known as a holistic approach that allows companies to identify, measure, monitor,

and respond to risks from various operational and strategic aspects. Effective ERM implementation can encourage companies to survive potential losses and exploit risks as opportunities for innovation and growth.

Strategic implementation of ERM increases the effectiveness of company performance. With an integrated ERM system, companies can holistically identify, assess, and mitigate business risks, ensuring that every business decision is taken by considering potential risks and opportunities. This reduces losses that may arise from unexpected troubles and maximizes opportunities for growth and innovation. This is also done by Bank Mandiri, which implements ERM to maintain and improve company performance. Implementing ERM aims to create value by managing operational and capital risks by implementing adequate internal controls (Rachman, 2022). The benefits of implementing ERM to improve company performance were also carried out by 46 private companies and State-Owned Enterprises (BUMN), which finally received the ERM Award II in August 2018. For companies that received this award, implementing ERM increased added value for companies needed to have a competitive advantage (Hidayat, 2018). Thus, ERM helps companies to operate more efficiently, save costs, and increase stakeholder confidence, all of which contribute to better and more sustainable business performance.

In addition, rapid changes in the business environment, such as technological disruption and economic fluctuations, require internal auditors to continuously improve their ability to understand and respond to new risks that arise. Therefore, companies must establish corporate governance based on ERM ISO 31000 because establishing authority is based on a holistic approach to identifying, assessing, managing, and monitoring organizational risks (Susilo & Kaho, 2018). Through ISO 31000, companies can understand and manage risk as a whole, not just from the perspective of specific individuals or departments. By understanding the risks faced and how these risks interact with each other, management can make more precise and informed decisions (Hardjomidjojo et al., 2022). This not only reduces potential losses but can also increase profits. Additionally, organizations with good risk governance tend to gain more trust from stakeholders, including investors, customers, and employees. Regulatory compliance across industries also often requires a practical risk management approach, and ISO 31000 enables companies to meet these requirements. Additionally, by understanding risks and how they interact, companies can allocate resources more efficiently, optimize operations, and achieve their strategic goals more effectively (Wicaksono, 2020).

In the ISO 31000 ERM framework, the role of internal auditors becomes very central and strategic. As the entity responsible for ensuring the integrity and compliance of business processes, internal auditors have a profound vision of company operations. Internal audit has an independent, objective function in providing assurance and consultation to provide added value to improve organizational performance. Internal audit helps organizations achieve their goals with a systematic, disciplined approach to evaluating and enhancing the effectiveness of risk management, control, and governance processes. (Gleim Publications, 2021; Zain, 2022)Therefore, internal audit has a vital role in ensuring that company management has implemented ERM in establishing effective governance with the hope that the company can achieve its expected goals (Hassan et al., 2022).

The research carried out places greater emphasis on the application of ERM ISO 31000 principles in the process of establishing corporate governance. The method of establishing authority that is not by the ERM ISO 31000 principles will cause the emergence of governance risks that have a significant impact on the company, such as weak supervision by directors of company management, the emergence of fraud, and failure to identify strategic risks which can cause the company to fail. Operate optimally (Hubbard, 2020).

Development of Enterprise Risk Management

Risk Governance (RG) is an advanced form of Enterprise Risk Management (ERM), enriched with risk oversight responsibilities by the board of directors and audit committee. (Stein, 2019)revealed that the European Commission first introduced GM in the context of science and society as a macro-social transformation. In 2003, the International Risk Governance Council (IRGC) began to promote awareness regarding RG with a framework that focused on policies to avoid unexpected macro instability in the political and economic spheres, going beyond the scope of micro organizations (. However, after the 2008 financial crisis, the focus on (Stein, 2019; van Asselt & Renn, 2011) RG shifted to the micro-organizational level, especially in financial institutions. RG is a framework in which the board of directors and management establish, monitor, and ensure compliance with risk tolerances and limits and identify, measure, and manage risks. However, RG still retains (Hassan et al., 2022)elements -the essential elements of traditional RM focus on achieving internal control system objectives, such as operational efficiency, reporting, and compliance, while often to the exclusion of corporate strategy (Hassan et al., 2022; Stein, 2019).

Lundqvist (2015)emphasizes integrating RM practices and corporate governance to combine traditional RM with corporate strategic planning. He supports the development of the ERM framework as a governance-based RM approach. As a result, ERM was adopted as a holistic approach to RM, where the organization can address and respond to potential risks to its objectives (Beasley et al., 2023; Horvey & Ankamah, 2020). However, despite significant developments, ERM remains focused on internal control system objectives such as operations, reporting, and compliance (Stein, 2019).

RG includes a company ERM system that is strengthened by a monitoring mechanism by the board of directors. This reflects organizational efforts to align RM across systems, processes, and personnel through oversight bodies, such as audit committees and internal audit divisions.

In 2017, ERM developed an integration of RM practices with corporate governance, strategy, and performance (Karanja, 2017). However, these developments have not prevented risk-related incidents, such as financial fines and lawsuits (Hassan et al., 2022). The incident sparked the emergence of RG as a comprehensive framework to address weaknesses in RM and corporate governance. Failure to manage corporate risk due to deficiencies in RM or corporate governance explains the emergence of RG. RG focuses on “risk behavior” (Sheedy & Griffin, 2018)and integrates RM in operational departments with corporate governance and corporate strategy (Hassan et al., 2022). Stein (2019) defines RG

as “the overall collaborative process between actors involved in addressing the complexity of risks in a company's internal and external environments.”

RG includes a company ERM system that is strengthened by a monitoring mechanism by the board of directors. It reflects an organization's efforts to align RM across systems, processes, and personnel through oversight bodies, such as the board of directors and audit committee. RG provides an objective view to management, the board of directors, and the public regarding the condition of RM and the internal control process. RG aims to apply sound governance principles in risk identification, assessment, management, and communication (IRGC, 2018).

ISO 31000:2018 Risk Management Principles

The definition of risk management is directed and coordinated activities in an organization related to risk (Ramadhan et al., 2020; Susilo & Kaho, 2018). The application of risk management according to ISO 31000:2008 is to create and protect existing value so that it can improve performance, encourage innovation, and support the achievement of goals to be achieved. (Putra & Chan, 2017; Wicaksono, 2020). ISO 31000 sets out several basic principles that organizations must adopt as the core foundation in risk management. These principles are essential to remember when defining risk management structures and procedures. ISO 31000:2018 has eight main tenets, with the central axis being value creation and protection, which means that companies that can implement risk management effectively can protect the organization from threats and can take advantage of opportunities by successfully managing these risks (Hardjomidjojo et al., 2022; Institute of Risk Management, 2018). Value creation and protection requires an essential role from the board of directors in determining governance, culture, and the values adhered to in the organization so that the risk management process can be carried out effectively (Institute of Risk Management, 2018; Susilo & Kaho, 2018). The following describes the eight principles of ISO 31000 risk management, shown in Figure 1.

Picture 1. ISO 31000:2018 Risk Management Principles

1. Integrated. Every business activity and decision-making across an organization must consider all risks and integrate them into its overall management system (Institute of Risk Management, 2018; Susilo & Kaho, 2018). Essential factors in this principle are: (a) Integrated risk management with relevant business aspects, (b) Affirm responsibility for risk holders (Ramadhan et al., 2020). (c) adapted to actual and contemporary needs, (d) Supports determining the priority order of process steps. (e) Encourage the selection of more feasible action options, (f) improve the quality of decision-making.

2. Structured and comprehensive. A structured and comprehensive framework makes it easier for organizations to understand the division of roles and responsibilities. In addition, this framework provides consistent procedures, from identification and understanding to risk management and communication of relevant information (Institute of Risk Management, 2018; Susilo & Kaho, 2018). Some critical aspects of this principle include: (a) Implement a systematic approach to efficient and consistent risk assessment (Natasya Safitri et al., 2021). Capacity to produce comparable output, (b) Building consistent perceptions across organizational entities.

3. Customized to the needs of its users. This principle emphasizes the importance of adapting the risk management approach to each organization's goals and needs (Institute of Risk Management, 2018; Susilo & Kaho, 2018). Key aspects to consider in this principle include: (a) Adjustment to the organization's internal and external context and risk profie. (b) Establishment of Enterprise Risk Management (ERM) aligned with organizational goals. (c) Adjustment to the culture and values espoused by the organization (Institute of Risk Management, 2018), (d) Fulfillment of legal demands and regulations that apply to the organization. (e)Adjustment to the resource requirements required in the risk management process.

4. Inclusive. Involving stakeholders appropriately and at the right time ensures that diverse perspectives are considered in risk management so that decisions are based on more complete and in-depth information (Institute of Risk Management, 2018; Susilo & Kaho, 2018). Key aspects of this principle include: (a) Strengthen stakeholder involvement in the risk assessment and response process. (b) Promote a cohesive view of risk across all organizational departments and among stakeholders. (c) Ensure that the risk management approach remains appropriate to the threats encountered by the organization and is continuously updated. (d) Develop a comprehensive and comprehensive risk management strategy (Miftakhatun, 2020).

5. Dynamic. The context and situation of an organization change over time, as do the risks it faces. This principle emphasizes the importance of reviewing risks periodically to ensure the achievement of organizational goals (Institute of Risk Management, 2018; Susilo & Kaho, 2018). Essential aspects of this principle include: (a) Maintain risk management responsive to changes, both from external and internal contexts. (b) Ability to detect and anticipate potential risks due to change (Hardjomidjojo et al., 2022). (c) Strengthening organizational resilience to various risks. (d) Ensure that the risk management structure is always responsive and flexible to the dynamics of change, maintaining effectiveness in its implementation.

6. The best information available (best available data). This principle highlights the importance of making decisions based on relevant and accurate information, both from internal and external sources of the organization (Institute of Risk Management, 2018; Susilo & Kaho, 2018). In risk management, it is essential to consider input from stakeholders inside and outside the organization. Key aspects of this principle include: (a) Driving the establishment of a unique database to support risk management. (b) Stakeholder needs for accurate and reliable information in risk management. Acknowledging understanding and limitations in understanding risk. (c) Timely utilization of available information in risk management. (d) Use information to assess the effectiveness of risk controls. (e) Utilize information for monitoring, evaluation, and periodic risk management reporting. (f) Encourage the development of information systems that suit the organization's needs in risk management.

7. Human and Cultural Factors. Risk management relies on synergy and active participation from stakeholders (Institute of Risk Management, 2018; Susilo & Kaho, 2018). This facilitates a deep understanding of the human dimensions and cultural nuances essential to organizational sustainability and success. This principle also emphasizes the importance of considering the intrinsic characteristics of the organization and human aspects when incorporating risk management into the organizational structure and designing effective risk management processes. Key elements of this principle include: (a) The need to align human resource capabilities with stakeholder expectations and the organization's mission. (b) Maintain alignment between corporate culture, surrounding culture, and the actions of organizational members in risk management strategies. (c) Continuous assessment of the risk management structure ensures that the relationship between culture, actions, and risk governance functions is well integrated within the organization.

8. Continuous Improvement. This principle emphasizes the importance of organizations consistently monitoring, evaluating, and optimizing risk management processes to ensure their relevance, efficiency, and effectiveness in supporting holistic organizational achievements (Institute of Risk Management, 2018; Susilo & Kaho, 2018). Crucial aspects of this principle include. (a) This will increase the level of maturity in implementing risk management. (b) Address stakeholder expectations in protecting the public interest as a whole. (c) Support the aspirations of the organization in fulfilling its responsibilities.(d) Integrate findings from internal audit and other assurance units to facilitate continuous improvement. (e) Risk management must be integrated into the organization's continuous improvement mechanisms.

The Role of Internal Audit in Carrying Out Assurance Risk Governance Based on ERM ISO 31000:2018

An internal audit is a unit or team that performs objective assurance and consulting activities to improve and add value to an organization's operations (Insitute et al., 2022). Its activities are often related to governance, risk, and control (GRC) to provide added value for the company (Eulerich & Eulerich, 2020; Insitute et al., 2022). Internal audit has a vital role in ensuring that organizational governance, especially those based on ERM (Enterprise Risk Management) by

carrying out assurance activities for operational, financial, and compliance activities, has been carried out effectively and efficiently (Eulerich & Eulerich, 2020).

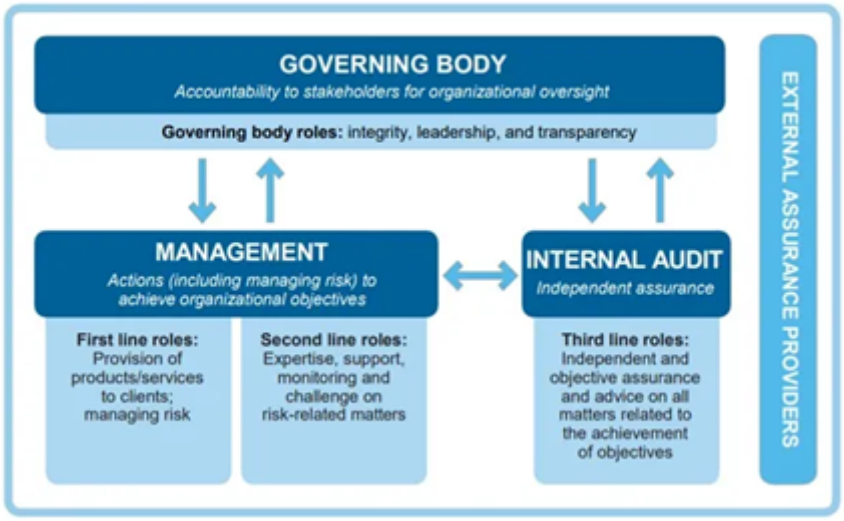
Assurance activities carried out by internal auditors will provide added value for organizations to gain an in-depth understanding of the extent to which ERM has been integrated into daily business processes (Jassem, 2022). In the internal assurance activity, the auditor will determine whether governance in the organization has been established and implemented effectively (Yudianto et al., 2021). This is done by applying the ERM principles ISO 31000:2018, where company leaders must determine what values are adhered to to create a good culture. Organization so that the company's goals can be achieved, and as a company leader, you are also obliged to protect the organization's values (Susilo & Kaho, 2018). Suppose the company's governance has been established and implemented well. In that case, it is also hoped that the company will have good risk governance (RG) because by implementing RG, If a company is good, the company will consistently execute a risk culture in all its daily activities, such as identifying risks, assessing risks carried out objectively, and determining which mitigation strategies to implement are appropriate and effective (Hassan et al., 2022).

The assurance process carried out by internal audit can use the three-line method (TLM). TLM is an approach many organizations use to understand and organize responsibilities in managing risks and controls (Sekar, 2022). This model divides these responsibilities into three layers as follows:

1. First Layer (first line) - Operational Function: This is the first line of defense. Management and operational staff are responsible for identifying, assessing, and managing risks in their daily activities. They are also responsible for implementing internal controls and ensuring compliance with applicable policies and procedures (Insitute et al., 2022).

2. Second Layer (second line) - Risk Oversight and Compliance Function: This layer involves functions that establish a risk management framework and ensure risks are managed by organizational policies. This includes functions such as risk management, compliance, and financial controls. They provide the guidance, tools, techniques, and training first-liners need to manage their risks (Insitute et al., 2022).

3. Third Layer (third line) – Internal Audit: As the fourth line of defense, internal audit provides independent assurance to the board of directors and senior management about the effectiveness of risk management and control by the two previous lines of defense. They objectively evaluate the effectiveness of risk management processes and internal controls (Insitute et al., 2022).



Picture 2. Three Lines Method

The TLM model can help internal auditors assess whether risk governance has been implemented based on the eight ERM principles of ISO 31000:2018. In addition, with this TLM method, organizations can ensure that risk management responsibilities are more precise and well structured so that risks can be managed effectively throughout the organization so that the company is expected to achieve its stated goals.

CONCLUSION

Effective risk governance is crucial for corporate sustainability in an era of globalization characterized by increasing business complexity. Enterprise risk management (ERM) is emerging as a holistic solution that enables companies to confront, identify, and respond to risks more adaptively. ERM serves as a bulwark against potential losses and a tool for identifying opportunities for innovation and growth.

ISO 31000:2018, as an international standard, provides a framework for companies to ensure that their approach to risk management is structured, comprehensive, and integrated with corporate governance. This standard emphasizes the importance of understanding and managing risk in the context of the entire organization, ensuring that every decision taken is based on the best available information and considers potential risks and opportunities. In this framework, the role of internal audit becomes crucial. As the third line of defense in the Three Lines Method (TLM) model, internal audit provides objective assurance to management and the board of directors that the risk management process is running well and by established standards. Through critical examination and evaluation, internal audit ensures that risk governance and internal controls function effectively, supporting organizational goals.

In addition, the internal auditor also provides recommendations on improving these processes so that the company not only protects itself from potential losses

but also utilizes risks as opportunities for growth and innovation. In other words, internal audit ensures that corporate governance, including risk governance and the implementation of ERM ISO 31000, functions well and provides added value to the organization. Thus, with the combination of solid management, implementation of risk governance, compliance with ERM ISO 31000, and the active role of internal audit, it is hoped that the company can face risks that could hinder it from achieving its goals.

Suggestion

In increasing the effectiveness of risk management, it is essential for companies to regularly hold training sessions on ERM principles, especially those based on the ISO 31000:2018 standard. This will ensure consistent implementation across all lines of the organization. In addition, the capacity of the internal audit team must be increased through training and implementation of the latest tools, emphasizing implementing audit recommendations quickly and efficiently. Effective implementation of the TLM model is also recommended to provide clarification of responsibilities and better coordination in risk management. The importance of regular evaluation of the risk management system must be balanced, ensuring that the system remains relevant and effective in the face of changing risks. Furthermore, promoting a risk culture through open discussions at all levels of the organization will encourage collective awareness and responsibility. Apart from that, company leaders also need to carry out regular risk culture socialization activities to strengthen communication with stakeholders to provide additional insight into potential risks and opportunities that may arise.

.

REFERENCE

Beasley, M., Branson, B., & Pagach, D. (2023). An Evolving Risk Landscape: Insights from a Decade of Surveys of Executives and Risk Professionals. *Journal of Risk and Financial Management*, *16*(1), 29. https://doi.org/10.3390/jrfm16010029

Eulerich, A., & Eulerich, M. (2020). What is the value of internal auditing? – A literature review on qualitative and quantitative perspectives. *Maandblad Voor Accountancy En Bedrijfseconomie*, *94*(3/4), 83–92. https://doi.org/10.5117/mab.94.50375

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 organisational culture. *Journal of Accounting & Organizational Change*, *18*(1), 77–99. https://doi.org/10.1108/JAOC-01-2021-0003

Hidayat, F. (2018, August 4). Penerapan ERM Tingkatkan Value Added Perusahaan. *Https://Www.Beritasatu.Com/Ekonomi/504105/Penerapan-Erm-Tingkatkan-Value-Added-Perusahaan*.

Horvey, S. S., & Ankamah, J. (2020). Enterprise risk management and firm performance: Empirical evidence from Ghana equity market. *Cogent Economics & Finance*, *8*(1), 1840102. https://doi.org/10.1080/23322039.2020.1840102

Hubbard, D. W. (2020). *The Failure of Risk Management: Why It's Broken and How to Fix It* (2nd ed.). Wiley.
Insitute Internal Auditor. (2022). *The IIA's CIA Learning System Part 1*. Insitute Internal Auditor.
Institute of Risk Management. (2018). *A Risk Practitioners Guide to ISO 31000: 2018*. Institute of Risk Management.
Jassem, S. (2022). Influence of internal audit functions on enterprise risk management: evidence from Malaysian transportation industry. *International Journal of Business Excellence*, *26*(2), 196. https://doi.org/10.1504/IJBEX.2022.121583
Karanja, E. (2017). Does the hiring of chief risk officers align with the COSO/ISO enterprise risk management frameworks? *International Journal of Accounting & Information Management*, *25*(3), 274–295. https://doi.org/10.1108/IJAIM-04-2016-0037
Lundqvist, S. A. (2015). Why firms implement risk governance – Stepping beyond traditional risk management to enterprise risk management. *Journal of Accounting and Public Policy*, *34*(5), 441–466. https://doi.org/10.1016/j.jaccpubpol.2015.05.002
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
Natasya Safitri, D., Fitria Sari, R., & Setya Dharmawan, Y. (2021). Analisis Manajemen Risiko Sistem Enterprise Resource Planning Menggunakan Kerangka Kerja ISO 31000 pada PT. XYZ. *Aisyah Journal of Informatics and Electrical Engineering*, *3*(1), 58–67.
Putra, Z., & Chan, S. (2017). DESAIN MANAJEMEN RISIKO BERBASIS ISO 31000 PADA PDAM TIRTA MEULABOH. *Jurnal Ekombis Fakultas Ekonomi Teuku Umar*, *3*(1).
Rachman, V. (2022, March 14). Bank Mandiri, Adopsi Tiga Elemen untuk Perkokoh Ketahanan Bisnis. *Https://Swa.Co.Id/Business-Champions/Companies/Companies-Good-Corporate-Governance/Bank-Mandiri-Adopsi-Tiga-Elemen-Untuk-Perkokoh-Ketahanan-Bisnis*.
Ramadhan, D. L., Febriansyah, R., & Dewi, R. S. (2020). Analisis Manajemen Risiko Menggunakan ISO 31000 pada Smart Canteen SMA XYZ. *JURIKOM (Jurnal Riset Komputer)*, *7*(1), 91. https://doi.org/10.30865/jurikom.v7i1.1791
Sekar, M. (2022). Three Lines of Defense. In *Machine Learning for Auditors* (pp. 3–12). Apress. https://doi.org/10.1007/978-1-4842-8051-5_1
Sheedy, E., & Griffin, B. (2018). Risk governance, structures, culture, and behavior: A view from the inside. *Corporate Governance: An International Review*, *26*(1), 4–22. https://doi.org/10.1111/corg.12200
Stein, V. (2019). Framing risk governance. *Management Research Review*.
Susilo, L. J., & Kaho, V. R. (2018). *Manajemen Risiko. Panduan Untuk Risk Leaders Dan Risk Practitioners*. PT. Gramedia Widiasarana Indonesia.
van Asselt, M. B. A., & Renn, O. (2011). Risk governance. *Journal of Risk Research*, *14*(4), 431–449. https://doi.org/10.1080/13669877.2011.553730
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
Yudianto, I., Mulyani, S., Fahmi, M., & Winarningsih, S. (2021). The Influence of Enterprise Risk Management Implementation and Internal Audit Quality on Universities' Performance in Indonesia. *Journal of Southwest Jiaotong University*, *56*(2), 149–164. https://doi.org/10.35741/issn.0258-2724.56.2.13

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