ABM: International Journal of Administration, Business and Management
Vol. 8, No. 1, June 2025 - November 2025
E-ISSN 2774-1664
P-ISSN 2746-2439

Evaluating Cyber Risk Management in Indonesian SOEs: A Case Study of PT Kereta Api Indonesia Using IT Governance Framework

Christin Angelia[1*], Caesar Octoviandy Purba[2], Nur Imam Taufik[3], Hafid Aditya Pradesa[4]

[1,2,3,4] Administration Business Sector Public, Polytechnic STIA LAN Bandung, Indonesia

Abstrak

Amid the rapid advancement of technology that enhances operational effectiveness and efficiency, cybersecurity risks have simultaneously increased, threatening data security. PT Kereta Api Indonesia (Persero), a state-owned enterprise, experienced a significant data leak incident in 2024, underscoring the urgent need for robust IT governance. This study evaluates the company's cyber risk management using the IT Governance Theory framework. A qualitative descriptive approach was employed, incorporating observation, in-depth interviews, and document analysis. Findings show that although PT KAI has implemented an Information Security Management System (ISMS) and provided employee training, key challenges persist, including low employee awareness (IT Principles), limited system integration (IT Architecture), and insufficient adoption of emerging technologies (IT Infrastructure). This study proposes a cyber risk management development model based on the five IT Governance domains: IT Principles, IT Architecture, IT Infrastructure, Business Application Needs, and IT Investment and Prioritization. The proposed model aims to strengthen the organization's ability to identify, detect, respond to, recover from, and adapt to cyber incidents, thereby enhancing IT governance, particularly in the context of Indonesian state-owned enterprises.

Keyword: Cyber Risk Management, IT Governance, ISMS, State-Owned Enterprises, PT KAI

Korespondensi:
Christin Angelia
(christinangelia03@gmail.com)

Submission: 10-08-2025
Revision: 28-10-2025
Received: 27-11-2025
Published: 30-11-2025

1. Introduction

PT Kereta Api Indonesia (Persero) is a state-owned enterprise (BUMN) engaged in the railway transportation sector. In recent years, the company has undergone significant digital transformation, marked by the implementation of digital platforms such as the KAI Access mobile application and internal systems like the Learning Management System (LMS) and Rail Document System (RDS). According to its 2023 annual report, PT KAI experienced a 36.68% increase in passenger volume compared to 2022—an improvement largely attributed to these digital innovations.

However, the rapid advancement of information technology (IT) has concurrently increased the company's exposure to cyber threats, which may compromise system availability, data integrity, and confidentiality(Sutigar et al., 2024). The National Cyber and Crypto Agency (2024) reported that the transportation sector ranks fourth in Darknet exposure, with over 133,000 data records being traded on illicit platforms. IBM Security (2024) noted that the average cost of a data breach in this sector rose from USD 4.18 million in 2023 to USD 4.43 million in 2024. Furthermore, Cybersecurity Guide (2025) recorded a 181% year-over-year increase in cyber incidents within the transportation industry.

In Indonesia, PT KAI became the target of a ransomware attack by the Stormous group on January 14, 2024. The attackers claimed to have gained access to 82 employee credentials, 22,500 customer records, and 50 partner credentials. Although the leaked data was not classified as critical, the incident posed reputational risks and potential financial liabilities due to possible administrative sanctions under Law No. 27 of 2022 concerning Personal Data Protection. As a mitigation effort, PT KAI established a Security Operations Center (SOC) to monitor and investigate cybersecurity incidents.

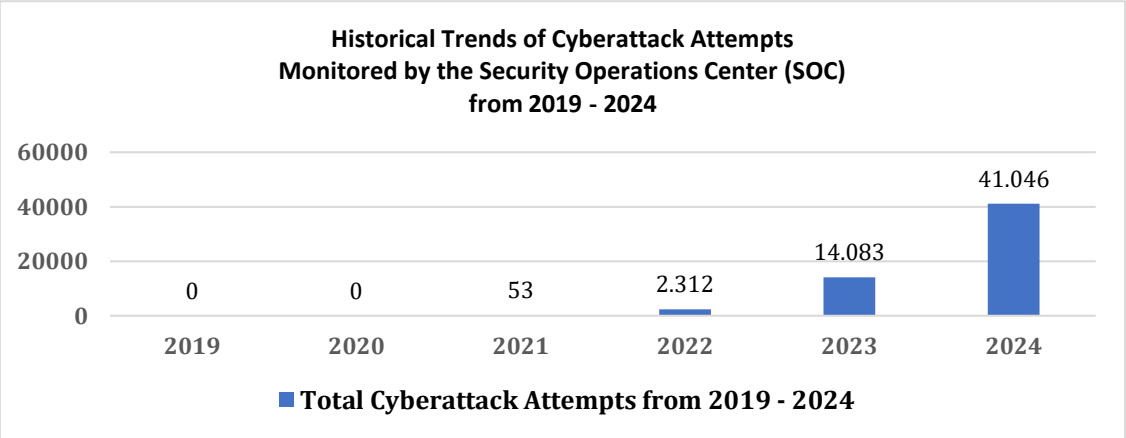

Figure 1.1 Cyber Attack Attempt Statistics (2019–2024)
Source: PT Kereta Api Indonesia (Compiled by the Author, 2025)

Figure 1.1 illustrates the growing trend of cyberattack attempts from 2019 to 2024, most of which exploited outdated or unpatched system vulnerabilities. Internal analysis identified three major contributing factors: (1) low employee awareness of data security; (2) incomplete implementation of the Information Security Management System (ISMS); and (3) outdated security infrastructure that lacks adaptability to current cyber threats. In line with ISO/IEC 27001:2013 standards, PT KAI continues to improve its cyber risk management framework, including initiatives such as a company-wide security audit conducted from December 1–22, 2024.

Figure 1.2. Results of Data Security Sampling Training for PT Kereta Api Indonesia Employees
Source: PT Kereta Api Indonesia (Compiled by the Author, 2025)

Figure 1.2 indicates that although employee awareness of data security is generally high, there remains a need to strengthen continuous training and awareness campaigns. From the user's perspective, security has also been enhanced through the application of One-Time Password (OTP) authentication in internal systems to prevent unauthorized data access.

In this context, the implementation of IT Governance Theory becomes highly relevant as a theoretical foundation for developing a robust and adaptive cyber risk management strategy. According to Weill and Ross (2004), IT Governance Theory provides a comprehensive framework that highlights the significance of structures, processes, and relational mechanisms in managing information technology. This framework not only addresses technical governance but also aligns IT initiatives with organizational objectives and risk management.

Previous studies have discussed the application of IT governance in various contexts. Rabii et al. (2020) presented security maturity models but lacked empirical insights from public institutions. Savira & Anis (2024) focused on governance in sustainable finance but not cybersecurity. Cahyaningrum & Widoatmodjo (2022) and Budiraharjo (2017) applied COBIT and Weill-Ross models in education but did not explore cyber threat mitigation. These gaps underscore the need for case-based studies in high-risk, state-owned sectors.

Therefore, this study aims to contribute both theoretically and practically, particularly in supporting the implementation of IT Governance Theory by addressing these existing research gaps. The primary objective is to evaluate how PT Kereta Api Indonesia (Persero)'s cyber risk management practices respond to real-world data security threats (Weill & Ross, 2004).

This research adopts a qualitative descriptive approach using a case study of PT Kereta Api Indonesia (Persero), with data collection methods including in-depth interviews, document analysis, and observation.

2. Methods

The methodology section outlines the overall design, data collection, and analytical processes employed in this study. The aim is to ensure transparency and reproducibility, allowing readers and other researchers to evaluate the appropriateness and credibility of the findings.

2.1 Research Design

This study uses a qualitative descriptive approach, as defined by Sugiyono (2022), to explore. the implementation of cybersecurity risk management at PT Kereta Api Indonesia (Persero). The qualitative method allows for an in-depth understanding of natural settings by positioning the researcher as the primary data collection instrument through interviews, observation, and document analysis.

2.2 Research Site and Period

The research was conducted at the head office of PT Kereta Api Indonesia (Persero), located at Jalan Perintis Kemerdekaan No.1, Bandung, West Java, Indonesia. The study was carried out from February - July 2025.

2.3 Data Sources and Participants

Two types of data were collected:

1. Primary data, obtained through in-depth interviews and direct observation involving five categories of key informants:

Table 2.1 Research Informants

No	Key Informants	Number	Description
1.	Manager of Networ and Security Operation	1 informant	Acts as the strategic decision-maker regarding IT policies and priorities.
2.	IT Network and Security Operation Team	2 informant	Responsible for the direct management and protection of information technology systems.
3.	IT Policy and Risk Team	2 informant	Directly responsible for drafting information technology system policies.
4.	PT KAI Risk Management Team	2 informant	Responsible for identifying, evaluating, and mitigating risks, including cyber risks.
5.	Operational Employee Using PT KAI IT Systems	1 informant	Active system user in daily operations, providing insight into field-level implementation.

Source: Compiled by the author (2025)

2. Secondary data**,** derived from documents such as cybersecurity policies, incident reports, training outcomes, and Information Security Management System (ISMS) strategies and guidelines.
   Informants were selected using purposive sampling, a non-probability sampling technique based on specific criteria relevant to the research topic**.**

2.4 Data Collection Techniques

Three main techniques were employed:

1. Observation: Conducted directly in the working environment of the IT and risk management units.
2. Interview: Performed through structured and in-depth conversations with selected informants.
3. Document Analysis: Involving systematic review of relevant documents, including incident reports, IT governance policies, and training records.

2.5Research Instruments

The instruments used include

1. The researcher: Acting as the primary instrument responsible for data collection, evaluation, interpretation, and analysis.
2. Interview and observation guidelines: To maintain focus and consistency during data collection.
3. Supporting tools: Such as smartphones, notebooks, and laptops to assist in the research process.

2.6 Data Analysis Techniques

Data were analyzed using the Miles & Huberman model, which consists of four stages:

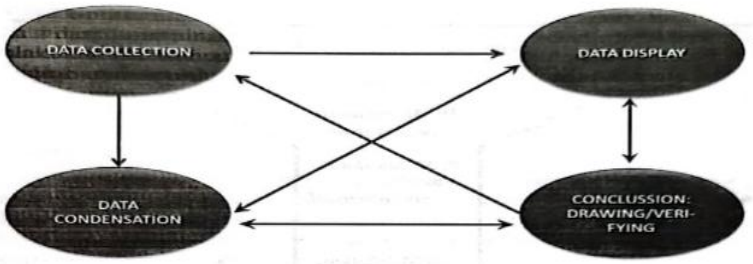

Figure 2. 1 Miles & Huberman Data Analysis Model
Source: Adapted from Sugiyono (2022)

1. Data collection: From interviews, observations, and documentation.
2. Data condensation: To summarize and focus on essential information.
3. Data display: In the form of brief narratives, diagrams, and flowcharts.
4. Conclusion drawing and verification: Involving continuous review to ensure credibility and validity.

2.7 Data Validity Techniques

To ensure the trustworthiness of the data, triangulation techniques were applied:
1. Source triangulation: By comparing data from informants with different roles in cybersecurity governance.
2. Technique triangulation: By comparing findings from interviews, observations, and documentation.

3. Results and Discussion

3.1 Evaluasi Domain Tata Kelola IT di PT Kereta Api Indonesia (Persero)

This study evaluates cyber risk management based on the five main domains of IT Governance Theory by Weill and Ross (2004), namely: IT Principles, IT Architecture, IT Infrastructure, Business Application Needs, and IT Investment and Prioritization.

3.1.1 IT Principles

IT Principles are general rules or guidelines that define the role of IT in supporting business. In relation to cyber risk, these principles reflect whether information security has been integrated into the organization's strategic values and direction.

Formal policies related to information security are already in place and documented internally. PT KAI has even conducted a webinar titled "Data Breach Mengancam Pidana" (Data Breaches May Lead to Criminal Charges) on November 13, 2024, and sent mass WhatsApp messages to employees as a form of awareness and education. In addition, observations indicate that IT Principles at PT Kereta Api Indonesia are also supported by the vision and mission stated in the RSTI, which are as follows:

Figure 3.1 RSTI PT KAI 2025–2029
Source: Internal Document of PT KAI (Interview, July 2025)

However, based on observations, general rules or guidelines on information security - specifically formal policies regarding IT usage principles - remain limited. This is evident in the lack of public advisories on safeguarding personal accounts.

Table 3.1 Percentage of Instagram Post Types by PT KAI

No	Type of Post	Count
1.	Operational Information	44
2.	Service Promotion	40
3.	Press Release	6

Source: Instagram kai121 (Compiled by the Author, 2025)

Table 3.1 shows that there are no independent advisories for the public regarding data security. However, during the research, the IT planning and network teams stated that they only deliver security advisories through the KAI Access application. This is supported by the following data they provided:

"We do not post independently on social media. Usually, we include notifications within the KAI Access app." – IT Planning Team (Interview, 2025)

"The reason is related to the Personal Data Protection Law and also due to previous data breach incidents in other institutions." – Commercial Team (Interview, 2025)

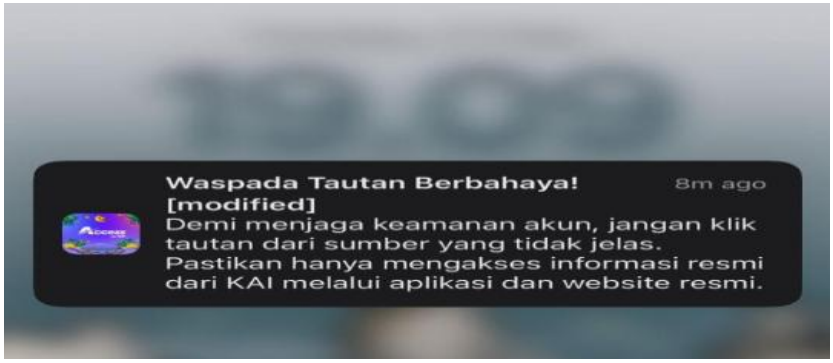

Figure 3.2 Data Security Notification via KAI Access
Source: Document Analysis during Interview

Figure 3.3 Data Security Reminder Banner
Source: Document Analysis during Interview

From the two reminders, it is evident that PT KAI has implemented public awareness efforts regarding data security. However, these efforts are still limited and uneven, being conducted only through the KAI Access application without a fixed or routine schedule. This can be observed from the notifications and banners, which appear only at specific times and are not provided regularly.

Although these measures indicate that PT Kereta Api Indonesia (Persero) does have IT Principles in place, their limited frequency suggests that further reinforcement is needed—both in terms of formal written policies and consistent awareness campaigns—aimed at the public as service users and employees as service providers.

3.1.2 IT Architecture

IT Architecture is the main design framework for information systems and technology used throughout the organization. In relation to cyber risk, IT architecture must support the integrity, confidentiality, and availability of information.

Based on interviews with the IT network team, IT planning team, operational staff, and risk management team, it was found that PT KAI has implemented standardization and integration of its information systems. This was conveyed by a Team Member of IT Security:

"From server preparation to production, each stage already follows security standards for users." – Team Member of IT Security (Interview, 2025).

However, based on document analysis, it was found that “The Information Security Management System (ISMS) has not yet covered all units within the company.” – (Internal Document, Pre-Research). Nevertheless, during the data collection period, the team explained that an update to the IT ISO certification had been carried out—from ISO 27001:2013 to ISO 27001:2022—effective since May 2025.

Figure 3.4 ISO 27001:2022 Certification
Source: Observation at IT Planning Unit Room

3.1.3 IT Infrastructure

IT Infrastructure refers to the hardware, networks, storage, servers, and cloud services that form the foundation of IT operations. In the context of cyber risk, infrastructure must have the ability to detect, respond to, and mitigate cyber threats.

Based on pre-research document analysis, the information security technology at PT KAI has met basic information security requirements. However, it has not yet fully adapted to the latest developments in information system technology. Nonetheless, several improvement efforts have been made as follows:

1. Strengthening existing IT security systems through the implementation of Modernized Security Operation and Threat Intelligence.
2. Enhancing secure coding principles in every application development within the company.
3. Updating computer network security technology across all business units.
4. Preparing an immutable backup system to support the contingency plan and business continuity plan.

Based on interviews with the IT network team, IT planning team, operational staff, and risk management team, it is known that PT KAI already has fairly adequate infrastructure. This is supported by the statement of Specialist of Security Operation:

“The infrastructure is fairly reliable, but there are still gaps that need to be addressed.” – Specialist Security Operation (Interview, 2025)

Figure 3.5 Digital Transformation Implementation Roadmap
Source: Internal Document PT KAI (Interview, July 2025)

This was reinforced by Team Member of IT Security, who explained:
“Other efforts, such as the use of data masking, server redundancy, and the adoption of the new ISO 27001:2022 standard, indicate that the direction of reinforcement is appropriate — although it remains partial in nature.”

3.1.4 Business Application Needs

Business Application Needs refer to the selection and development of applications based on operational or strategic business requirements. In relation to cyber risks, it is essential to assess whether security considerations have been integrated during the planning and implementation phases of these applications.

Based on observations, PT Kereta Api Indonesia (Persero) has adopted various digital platforms such as KAI Access, as well as internal systems including the Learning Management System (LMS) and the Rail Document System (RDS) to support business operations. However, in practice, users still encounter technical issues and access difficulties, which indicate that not all applications have been fully optimized in terms of usability and security resilience.

Figure 3.6 Customer Complaints Related to Login Access
Source: X kai121 (Observation, July 2025)

It was found that the existing applications do not yet fully meet user needs. Several issues were identified in the use of the KAI Access app, including login failures and deducted balances without ticket confirmation. This indicates a need for re-evaluation of the application selection process to better address user requirements.

The use of applications such as KAI Access, LMS, and RDS has supported operational activities. However, public complaints still arise, particularly regarding login errors and deducted balances.

"Risks are first identified, aligned with the risk appetite, and only then can we proceed to the design phase." – Tim IT (Interview, 2025)

"Business users submit their IT Business Requirements through IT Pro before they are forwarded to the IT Planning Team." – IT Planning Team (Interview, 2025). This means that the application procurement process has included security considerations; however, further evaluation is still needed regarding user experience and system reliability. This means that the application procurement process has included security considerations; however, further evaluation is still needed regarding user experience and system reliability.

3.1.5 IT Investment and Prioritization

IT Investment and Prioritization refer to decision-making related to budgeting and selection of IT projects. In terms of cyber risk, it concerns how the organization sets priorities and allocates budgets for IT projects, including those related to information security. Based on pre-research document analysis, PT KAI has demonstrated adequate investment and prioritization in IT, particularly in human resource development through the following programs:

1. Certified Ethical Hacker (CEH) training attended by 3 IT Operations staff (24–28 February 2025).
2. Certified Incident Handler (ECIH) training + exam attended by 2 IT Operations staff
3. Computer Hacking Forensic Investigator (CHFI) training + exam attended by 3 IT Operations staff.

This is supported by the interview statement from Specialist in Security Operations:

"Regarding investment, especially related to data security at KAI, we already have the RSTI (Strategic Plan for Information Technology), which aligns with the RJPP (Corporate Long-Term Plan)."

3.2 Analysis of Challenges and Obstacles in Cyber Risk Management

The cyber risk management model implemented by PT KAI faces several weaknesses and challenges, despite existing policies and infrastructure. Based on the findings, there are key elements that need improvement to make the cyber risk management model at PT KAI more effective in responding to increasingly complex cyber threats.

3.2.1 Challenges and Obstacles Faced by PT KAI

1. Low Employee Awareness
2. Limited Integration Between Units
3. Suboptimal Technological Adaptation to Emerging Threats.

3.3 Recomendations for Developing an Optimal Cyber Risk Management Model

Based on the evaluation of the current model, the following are recommendations to improve cyber risk management at PT KAI:

1. Enhanced Continuous Education and Awareness Programs for Employees
   Recommendation: PT KAI should involve more parties in training and introduce deeper practical learning methods (e.g., cyber-attack simulations and crisis management exercises).
2. Strengthening IT Infrastructure and System Integration.
   Recommendation: Conduct technical audits of existing IT infrastructure to identify integration gaps, and plan more comprehensive updates to ensure adaptability to evolving threats.
3. Implementation of Advanced Real-Time Security Systems
   Recommendation: Invest in AI-based threat detection and response technologies to identify attack patterns more accurately and rapidly.

Table 3.2 Improvement Model

Domain IT Governance	Identified Issues	Improvement Plan
IT Principles	Existing policies are present but lack strong socialization and monitoring mechanisms.	- Strengthen risk-based security policies. - Establish a Data Privacy Committee. - Design a Security Policy Communication Plan.
IT Architecture	Integration across units is inconsistent.	- Develop an Enterprise IT Blueprint. - Implement a Zero Trust Architecture. - Review system interoperability every 6 months.
IT Infrastructure	Threat detection is not real-time and lacks adaptation to emerging technologies.	- Upgrade to an AI-based Threat Intelligence system. - Add a risk-based SOC dashboard. - Implement multi-layered defense mechanisms.

Source: Compiled by the Author 2025

4. Conclusion

Based on the findings from the evaluation of cyber risk management at PT Kereta Api Indonesia (Persero) using the IT Governance Theory framework proposed by Weill & Ross (2004), several conclusions can be drawn:

1. Implementation of IT Governance Theory in Cyber Risk Management at PT Kereta Api Indonesia (Persero)

a. The implementation of IT Governance Theory at PT KAI has been carried out across various aspects of cyber risk management, although it has not yet reached an optimal level.
b. IT Principles: PT KAI has formal information security policies in place, disseminated through platforms such as the Rail Document System (RDS) and KAI Access. However, public outreach and internal employee education efforts remain limited and inconsistent.
c. IT Architecture: Internal information systems have been developed and integrated. Nevertheless, some business units are not yet covered by the Information Security Management System (ISMS), leading to gaps in cyber risk control.
d. IT infrastructure components such as firewalls, Security Operations Centers (SOC), and monitoring systems have been implemented. However, they have not yet fully adapted to detect and respond to cyber threats in real time.
e. Business Application Needs: Applications like the Rail Document System (RDS) have been utilized to support business operations. Yet, there is a lack of early integration of security considerations during the initial design phases of such applications.
f. IT Investment and Prioritization: Investments in the IT sector are continuously being made, supported by the Strategic Information Technology Plan (RSTI). These investments aim to enhance IT capabilities, particularly in areas of security, capacity building, and infrastructure modernization.

2. Challenges and Obstacles in Cyber Risk Management

Cyber risk management at PT KAI faces significant technical and non-technical challenges.

a. IT Principles: PT KAI has formal information security policies in place, disseminated through platforms such as the Rail Document System (RDS) and KAI Access. However, public outreach and internal employee education efforts remain limited and inconsistent.
b. IT Architecture: Internal information systems have been developed and integrated. Nevertheless, some business units are not yet covered by the Information Security Management System (ISMS), leading to gaps in cyber risk control.
c. IT infrastructure components such as firewalls, Security Operations Centers (SOC), and monitoring systems have been implemented. However, they have not yet fully adapted to detect and respond to cyber threats in real time.
d. Business Application Needs: Applications like the Rail Document System (RDS) have been utilized to support business operations. Yet, there is a lack of early integration of security considerations during the initial design phases of such applications.
e. IT Investment and Prioritization: Investments in the IT sector are continuously being made, supported by the Strategic Information Technology Plan (RSTI). These investments aim to enhance IT capabilities, particularly in areas of security, capacity building, and infrastructure modernization.

3. Recommendations

Theoretical Implications

This study contributes to the development of IT Governance Theory in the context of the public sector, particularly within state-owned enterprises (BUMN), by focusing on cyber risk management. Future research is encouraged to expand the scope by comparing different BUMN in order to develop a more applicable and adaptive IT governance model.

Pratical:

a. Enhancing IT Infrastructure and Architecture
b. Employee Training and Awareness Campaigns
c. System and Application Review
d. Policy Strengthening and IT Investment Prioritization

Daftar Pustaka

Badan Sandi dan Siber Negara. (2024). *Laporan Bulanan Publik Mei 2024*. www.idsirtii.or.id

Budiaraharjo, R. (2017). Penerapan Weill-Ross Model dalam Tata Kelola Teknologi Informasi di Perguruan Tinggi. *Jurnal Nasional Teknologi Dan Sistem Informasi*, *3*(1), 109–116. https://doi.org/10.25077/TEKNOSI.v3i1.2017.109-116

Cahyaningrum, M., & Widoatmodjo, S. (2022). *Analisis Keefektifan Dan Kemudahan Implementasi IT Governance Di Instansi X*. E-Journal Untar.

IBM Security. (2024). Cost of a Data Breach Report 2024. *IBM Security*, 1–73. https://www.ibm.com/security/data-breach

Rabii, A., Touhami, S., & Roudies, O. (2020). Information and cyber security maturity models: a systematic literature review. *Information and Computer Security*, *28*(4), 627–644. https://doi.org/10.1108/ICS-03-2019-0039

Savira, M., & Anis, I. (2024). Penerapan Strategic It-Governance Competence 2.0 Pada Bank First-Movers on Sustainable Finance Di Indonesia. *Jurnal Ekonomi Trisakti*, *4*(2), 531–540. https://doi.org/10.25105/v4i2.20845

Sugiyono. (2022). Metode Penelitian Kualitatif (Untuk penelitian yang bersifat: eksploratif, enterpretif, interaktif dan konstruktif). *Alfabeta*, 1–274. http://belajarpsikologi.com/metode-penelitian-kualitatif/

Sutigar, M. B. B., Bhisma, V. A., Firmansyah, A. N., & Wulansari, A. (2024). Studi Literature Review It Risk Management Di Instansi Pemerintahan. *JATI (Jurnal Mahasiswa Teknik Informatika)*, *8*(1), 75–79. https://doi.org/10.36040/jati.v8i1.8734

Weill, P., & Ross, J. (2004). *IT governance: How top performers manage IT decision rights for superior results*. Harvard Business School Press.