

Analysis of Tokopedia Digital Security Strategy Against Cyber Threats Using the Risk Assessment Framework Approach

Muhammad Mirza Raziq Akbar ^{a*}, Kukuh Yudhistiro ^b, Ahmad Rofiqul Muslikh ^c
^{a*,b,c} Information Study Program, Universitas Merdeka Malang, Malang City, East Java Province, Indonesia.

ABSTRACT

The rapid development of information technology has significantly reshaped the landscape of electronic commerce in Indonesia. Tokopedia, one of the country's largest e-commerce platforms, has demonstrated remarkable growth by enabling online transactions and digital identity management. At the same time, its reliance on digital infrastructure exposes the platform to serious cybersecurity risks. Notable incidents such as the 2020 data breach, which involved millions of leaked user accounts, illustrate how vulnerabilities can undermine consumer trust and disrupt business continuity. This study applies the *Risk Assessment Framework* based on ISO 27001 and ISO 31000 to evaluate Tokopedia's cybersecurity strategy. Employing a qualitative descriptive approach through a literature-based study, the analysis identifies five major threats: data breaches, phishing, ransomware, insider misuse, and system misconfiguration. Using a semi-quantitative scoring method, data breaches emerged as the highest risk with a score of 25, followed by phishing and ransomware at medium levels, and insider misuse at a relatively low level. Mitigation strategies recommended include data encryption, multi-factor authentication, role-based access control (RBAC), and regular security audits. The evaluation further shows that while Tokopedia has adopted important safeguards such as encryption and e-KYC, gaps remain in documented risk management, routine audits, and employee training. Comparisons with platforms like Shopee and Amazon emphasize the need for stronger governance and continuous monitoring. The findings highlight that cybersecurity should be positioned not only as a technical safeguard but also as a strategic business investment. Overall, the study underscores the relevance of ISO-based risk assessment in strengthening e-commerce resilience and provides structured recommendations for enhancing digital security practices in Indonesia.

ARTICLE HISTORY

Received 19 July 2025
Accepted 23 August 2025
Published 30 November 2025

KEYWORDS

Cybersecurity; Risk Assessment; ISO 27001; E-Commerce; Tokopedia.

1. Introduction

The rapid advancement of information technology in the digital era has transformed various sectors, including electronic commerce (*e-commerce*). Tokopedia, one of Indonesia's largest marketplaces, has experienced significant growth by facilitating online transactions, data storage, and user identity management. However, the reliance on digital infrastructure also introduces substantial risks to personal data security and system integrity. The Indonesian National Cyber and Crypto Agency (BSSN) highlights that threats such as *ransomware*, *hacking*, *phishing*, and large-scale data breaches remain major challenges in the country's digital ecosystem (Sukarni & Muslikh, 2024). These concerns became particularly evident during the 2020 data breach, when millions

of Tokopedia user accounts were reported to have been leaked and traded on the dark web, raising serious public concerns about data protection and platform reliability (Fadillah *et al.*, 2022; Ayu & Nasution, 2023). Similar findings have been echoed in legal and economic studies, which emphasize the broader implications of cyberattacks on both consumer trust and market stability (Bestari *et al.*, 2024).

Consumer confidence is highly dependent on the perceived safety of digital platforms, as users face risks such as identity theft, account hacking, and online fraud that may cause financial and reputational harm (Putri *et al.*, 2024). Previous research shows that ineffective risk governance amplifies these threats, while structured mitigation strategies enhance resilience against cyber incidents (Kehista *et al.*, 2023; Lisnawati *et al.*, 2023; Padang *et al.*, 2025). In Tokopedia's case, existing measures such as data encryption and multi-factor authentication have been implemented, yet gaps remain in documented policies, periodic security audits, and employee awareness programs (Soesanto *et al.*, 2023; Derliana & Yulhendri, 2024).

This study applies the *Risk Assessment Framework* based on ISO 27001 and ISO 31000 to evaluate Tokopedia's cybersecurity strategy. This framework enables systematic identification, assessment, and mitigation of risks. Accordingly, the research addresses three core questions: How effective is Tokopedia's cybersecurity strategy in managing cyber threats? What factors support or hinder the implementation of risk mitigation measures? and How can risk assessment outcomes strengthen the company's overall security posture? To answer these questions, the study aims to analyze the effectiveness of Tokopedia's security system, identify supporting and inhibiting factors, and formulate risk-based recommendations for enhancing user data protection and trust.

In addition to the *Risk Assessment Framework*, previous studies have employed IT governance frameworks such as *COBIT 2019* to examine Tokopedia's digital infrastructure. Findings revealed weaknesses in the *Deliver, Support, and Service* (DSS) domain, including the absence of standardized operating procedures and insufficient operational support (Wijanarko *et al.*, 2023). While such approaches provide valuable insights, the present study prioritizes the *Risk Assessment Framework* because of its direct relevance to identifying and mitigating cyber threats. This perspective is expected to generate a more targeted analysis that contributes to the development of stronger and more adaptive digital defense mechanisms within Tokopedia.

2. Methodology

This research adopts a qualitative descriptive approach, relying exclusively on a literature-based study to evaluate Tokopedia's cybersecurity strategy against multiple types of threats. The analysis employs the *Risk Assessment Framework* rooted in ISO 27001 and ISO 31000, which provides a systematic structure for identifying, assessing, and mitigating risks. Data were drawn from peer-reviewed journal articles, industry security reports, and relevant case documentation. The study design is descriptive and qualitative in nature, with the primary goal of generating an in-depth understanding of Tokopedia's existing security mechanisms and potential vulnerabilities. No primary data were collected through interviews or direct observation; instead, the research is based entirely on secondary sources that have been reviewed and synthesized through a systematic process.

The data collection process involved targeted literature searches using three main criteria: publication within the last ten years (2015–2025) to maintain relevance, publication in reputable and peer-reviewed journals, and direct discussion of topics related to cybersecurity strategies, risk management frameworks, or case studies on Tokopedia and the Indonesian *e-commerce* sector. Studies addressing ISO-based risk management frameworks (Kholifah & Yulhendri, 2024), methods of early detection in

cyberattacks (Laksana & Mulyani, 2024), and the application of *electronic Know Your Customer (e-KYC)* in financial platforms to strengthen account security (Putra *et al.*, 2023) were included to enrich the discussion. Additional references that discuss broader perspectives on cybersecurity governance in the digital era (Susanto *et al.*, 2023) and the role of emerging technologies such as cloud computing and the Internet of Things in shaping *e-commerce* security strategies (Wulan *et al.*, 2024) were also integrated to strengthen the methodological foundation.

Data analysis was conducted using a descriptive application of the *Risk Assessment Framework*. The process consisted of four stages: risk identification, risk assessment, mitigation design, and policy evaluation. In the identification stage, cyber incidents relevant to Tokopedia, including the 2020 data breach, were mapped alongside other potential threats such as phishing, ransomware, insider misuse, and system misconfiguration. In the assessment stage, each identified risk was assigned a probability and impact score on a five-point scale, and the total risk score was calculated to determine its severity level. The mitigation stage involved formulating technical and organizational strategies aligned with industry best practices, including end-to-end encryption, identity management systems, regular security audits, and access control mechanisms. The final stage focused on evaluating Tokopedia's existing policies by comparing documented practices with industry standards and ISO requirements, thereby identifying gaps and areas for improvement.

Ethical considerations were observed throughout the research process. Since the study did not involve primary data collection such as interviews or direct observation, no personal information was accessed or processed. All materials analyzed were publicly available, including academic journal articles, industry reports, and official publications. Proper citation was maintained to ensure the accuracy and originality of the information. The study was conducted solely for academic purposes, without any intention to harm individuals or institutions, and aims to contribute to scholarly discussions on cybersecurity and risk management in Indonesia's *e-commerce* sector.

3. Results

The cybersecurity risk analysis of Tokopedia was conducted using the *Risk Assessment Framework* based on ISO 27001 and ISO 31000. The analysis followed three main stages: risk identification, risk assessment, and the formulation of mitigation strategies. Since no primary data such as interviews with Tokopedia's internal security team or audit reports were available, the study was entirely literature-based, a limitation that is addressed in the later section.

The identification process revealed several critical threats faced by Tokopedia. Drawing from prior studies (Fadillah *et al.*, 2022; Ayu & Nasution, 2023; Lisnawati *et al.*, 2023), five main categories of risk were observed: user data breaches caused by external hackers, phishing and identity manipulation conducted through malicious emails, ransomware and malware originating from harmful software, unauthorized insider access from employees or internal systems, and system misconfigurations attributed to IT teams or vendors. These threats are summarized in Table 1.

Table 1. Risk Identification

No	Threat Type	Source of Threat
1	User data breach	External Hackers
2	Phishing and identity fraud	Malicious Emails
3	Ransomware / Malware	Malicious Software
4	Unauthorized insider access	Employees / Contractors
5	System misconfiguration	IT Teams / Vendors

Risk assessment was then conducted using a semi-quantitative method adapted from ISO 27005, combining probability (P) and impact (D) scores on a scale from one to five. The calculation demonstrated that user data breaches scored the highest, with probability and impact both rated at five, resulting in a risk value of twenty-five categorized as high. Phishing and identity theft scored sixteen, ransomware or malware fifteen, and system misconfiguration twelve, each falling under medium risk. Insider access, with a probability score of two and an impact score of three, scored six overall and was therefore considered low risk. This shows that while Tokopedia faces multiple cyber threats, user data breaches remain the most critical and must be prioritized. The complete results of the scoring process are presented in Table 2.

Table 2. Risk Assessment Results

Type of Risk	Probability	Impact	Risk Score (P x D)	Risk Level
User Data Breach	5	5	25	High
Phishing & Identity Theft	4	4	16	Medium
Ransomware / Malware	3	5	15	Medium
System Misconfiguration	3	4	12	Medium
Unauthorized Insider Threats	2	3	6	Low

The mitigation strategies were designed according to ISO 27001 standards and supported by findings in the literature. For data breaches, the use of AES-256 encryption and Data Loss Prevention (DLP) systems was recommended. Phishing and fraudulent identity use could be minimized through AI-based email filtering and the enforcement of two-factor authentication across all logins. Ransomware and malware could be countered through enterprise-grade antivirus systems, routine patching, and network segmentation. Insider misuse could be reduced through Role-Based Access Control (RBAC) combined with continuous monitoring and audit logs, while misconfiguration risks could be managed using automated scanning tools and regular server code reviews. These recommendations are outlined in Table 3.

Table 3. Risk Mitigation Strategies

Threat Type	Mitigation Strategies
Data Breach	AES-256 encryption, <i>Data Loss Prevention (DLP)</i> systems, regular penetration testing
Phishing & Identity Theft	AI-based email filtering, mandatory multi-factor authentication (MFA)
Ransomware / Malware	Enterprise antivirus, system patching, network segmentation, backup management
System Misconfiguration	Automated misconfiguration scanning, code reviews, periodic server audits
Insider Threats	Role-Based Access Control (RBAC), log audits, continuous activity monitoring

The entire process of the *Risk Assessment Framework*, from identification and assessment to mitigation and post-implementation monitoring, can be illustrated as shown in Figure 1.

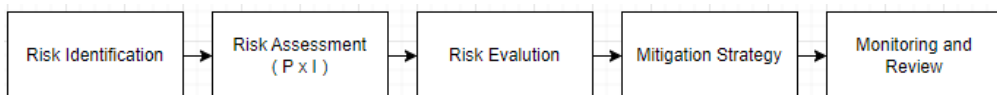


Figure 1. Risk Assessment Framework Process

Evaluation of Tokopedia’s existing security strategies, when compared with international standards such as ISO 27001 and ISO 31000, showed mixed results. On one hand, Tokopedia had already adopted several important practices, including the use of HTTPS protocols, data encryption, e-KYC for user verification, multi-factor authentication, and user privacy policies. On the other hand, significant shortcomings remain, such as the absence of routine internal audits, incomplete documentation of procedures, and the lack of regular employee cybersecurity training. These findings demonstrate that while Tokopedia has adopted essential safeguards, its security strategy is still not fully aligned with ISO-based systematic risk management. The evaluation is summarized in Table 4.

Table 4. Evaluation of Tokopedia’s Security Strategy

Evaluation Aspect	Tokopedia Practice (Literature)	ISO / Framework Standard	Risk	Remarks
Data Encryption	Implemented	Mandatory		Aligned
Formal Risk Management	Not standardized (Derliana & Yulhendri, 2024)	fully documented &	Documentation required	Needs improvement in documentation & periodic monitoring
Employee Security Training	Not explicitly mentioned	Required regularly		Gap in security awareness
Routine Audits	Not documented openly	Strongly recommended		Inconsistent
Insider threat protection	No clear RBAC system (Wijanarko <i>et al.</i> , 2023)	Role-based authorization needed		Requires implementation

Taken together, the findings reveal that Tokopedia has already integrated several core elements of cybersecurity into its operations but has yet to implement a fully documented and standardized risk management system. This gap highlights the need for greater formalization, continuous audits, and employee training in order to achieve stronger alignment with international best practices.

4. Discussion

The findings of the risk analysis and security strategy evaluation indicate that although Tokopedia has implemented multiple layers of cybersecurity protection, several weaknesses remain that could be exploited by potential threats. Technical measures such as data encryption, two-factor authentication, e-KYC systems, and the use of industry-standard security protocols are already in place. Nevertheless, the risk assessment highlights that certain threats—particularly data breaches caused by insider access, phishing attacks, and third-party intrusions—continue to fall into the high-risk category, carrying significant consequences for data integrity and user trust.

The literature review further reveals that Tokopedia has not yet fully adopted a documented and sustainable risk management framework in line with international standards such as ISO 27001 and ISO 31000. Gaps are especially evident in the absence of regular security audits, formal documentation of risks, and continuous cybersecurity awareness training for employees. These limitations weaken the overall effectiveness of Tokopedia’s security strategy, which remains fragmented and less

adaptive to the increasingly complex and dynamic landscape of cyber threats.

Several factors influence the success and shortcomings of Tokopedia's risk mitigation efforts. On the supportive side, the use of layered authentication, relatively transparent privacy policies, and investments in security technologies demonstrate a serious commitment to protecting user data. Initiatives such as e-KYC also provide an additional verification layer that helps prevent account misuse. However, significant barriers remain, including the lack of routine employee training at the operational level, the absence of a fully integrated and documented risk management system, and limited internal audits or oversight of security SOP implementation. These issues suggest that effective risk mitigation depends not only on technical solutions but also on organizational governance and managerial commitment.

The findings underscore the urgency of adopting the *Risk Assessment Framework* as a proactive rather than reactive strategy. Through structured processes of risk identification, probability assessment, and impact evaluation, Tokopedia has the opportunity to develop more adaptive, risk-based security policies. This structured approach also enables more efficient resource allocation and enhances the effectiveness of protection measures. Strengthening internal SOPs and implementing regular cybersecurity awareness training emerge as essential steps in building a more resilient defense system against evolving threats. Comparative insights from other e-commerce platforms provide further context. Shopee has integrated risk management through early-warning systems and annual employee training, while Amazon enforces strict role-based access control (RBAC) and conducts regular internal audits based on NIST standards. Compared to these benchmarks, Tokopedia lags behind in areas such as employee education and continuous auditing. This comparison illustrates that although Tokopedia's strategy already covers important aspects, there remains significant room for improvement in formalizing risk management practices and ensuring long-term compliance with international standards.

Beyond technical and managerial dimensions, the economic implications of cybersecurity must also be taken into account. Implementing regular audits, employee training, and stronger access controls requires substantial financial resources. However, a *cost-benefit analysis* suggests that these expenses should be viewed as long-term strategic investments rather than short-term costs. The potential benefits include a reduced likelihood of large-scale data breaches, improved consumer trust, and enhanced operational efficiency through more reliable systems. In the context of e-commerce, where security and trust are the backbone of sustainable growth, such investments are not only justified but essential. Taken together, Tokopedia's digital security strategy must evolve from a primarily technical approach toward a comprehensive, integrated model of risk management. This shift would strengthen both technical safeguards and organizational resilience, positioning cybersecurity as a protective mechanism as well as a strategic investment for long-term business sustainability.

5. Conclusion

This study aimed to analyze Tokopedia's digital security strategies in addressing cyber threats through the application of the *Risk Assessment Framework* grounded in ISO 27001 and ISO 31000. By adopting a structured approach that combined risk identification, probability and impact assessment, and strategy evaluation, several conclusions can be drawn. First, Tokopedia has already implemented a range of technical security measures, including data encryption, multi-factor authentication, and user privacy policies. However, the literature indicates that the adoption of a fully documented and systematic risk management framework has yet to be achieved. Second, the main cyber risks facing Tokopedia consist of user data breaches, phishing,

ransomware attacks, unauthorized insider access, and system misconfigurations. Among these, user data breaches represent the highest level of risk, with a score of 25, requiring prioritized attention and mitigation.

Third, the evaluation of Tokopedia's security practices demonstrates that several areas remain underdeveloped, particularly the absence of comprehensive documentation of risks, the lack of routine internal audits, limited cybersecurity training for employees, and the incomplete implementation of role-based access control (RBAC). Addressing these shortcomings is critical to improving the company's resilience to cyber threats. Fourth, the application of the *Risk Assessment Framework* has proven effective in identifying and prioritizing risks based on probability and impact. This framework provides Tokopedia with a foundation for developing proactive and sustainable digital security strategies, moving beyond reactive approaches.

From a theoretical standpoint, this study reinforces the relevance of using the *Risk Assessment Framework* as a systematic tool for evaluating digital security strategies in *e-commerce* companies. The framework enables the identification of security gaps and offers structured guidance for improvements, thereby contributing to the growing body of literature on risk management in the digital sector. For future research, it is recommended to adopt a quantitative or comparative approach by including multiple *e-commerce* platforms to expand the generalizability of findings. Further studies may also examine the practical effectiveness of implementing the proposed recommendations over time, allowing for an evaluation of their long-term impact on corporate cybersecurity resilience. In conclusion, the study highlights that ISO-based risk assessment can serve as an effective evaluation tool for assessing the readiness of digital security strategies against cyber risks. These findings are expected to provide a foundation for developing more adaptive, structured, and sustainable security strategies within the *e-commerce* industry.

Acknowledgements

The author wishes to express the deepest gratitude to Allah SWT for His grace and blessings, which have provided strength, health, and guidance throughout the preparation and completion of this research. Without His will, this work would not have been successfully accomplished. Special appreciation is extended to Mr. Kuku Yudhistiro, S.Kom., M.Kom., the supervising lecturer, for his invaluable guidance, advice, and constructive feedback throughout the entire process—from the initial formulation of ideas to the finalization of this study. His support has not only enriched the academic aspects of this research but has also provided meaningful moral encouragement. The author also conveys sincere thanks to Mr. Ahmad Rofiquil Muslikh, S.Kom., M.Kom., the examiner, for his critical insights and constructive suggestions, which have greatly contributed to improving the quality of this work. Profound respect and gratitude are dedicated to the author's beloved parents for their prayers, unwavering support, and endless encouragement. Their sacrifices and sincerity have been the foundation that enabled the author to reach this point. The author is also grateful to colleagues and friends, both within and outside the university, who have provided support, encouragement, and assistance—technical as well as non-technical—throughout the course of this research. The discussions, collaborations, and companionship shared have been an integral part of this academic journey. Finally, the author acknowledges that this study still has limitations. Suggestions and constructive feedback for future improvement are therefore highly welcomed. It is hoped that this research will contribute positively to the development of knowledge, particularly in the areas of digital security and cyber risk management.

References

- Ayu, S. S., & Nasution, M. I. P. (2023). Analisis kebocoran data privacy pada e-commerce Tokopedia. *JUEB: Jurnal Ekonomi dan Bisnis*, 2(3), 21–24. <https://doi.org/10.57218/jueb.v2i3.716>
- Bestari, Q., Putri, D. A., & Kurnia, K. A. (2024). Analisa kasus kebocoran data pengguna Tokopedia. *Jurnal Hukum Progresif*, 7(1), 45–60. <https://law.ojs.co.id/index.php/jhp/article/view/130>
- Derliana, & Yulhendri. (2024). Analisis manajemen risiko berbasis ISO 27001 pada aspek keamanan sistem informasi pada perusahaan Tokopedia. *Scientica: Jurnal Ilmiah Sains dan Teknologi*, 2(2), 139–151. <https://doi.org/10.572349/scientica.v2i2.907>
- Fadillah, F., Adelya, H. N. K., & Shahira, R. (2022). Dampak Cyber Attack bagi ekonomi perdagangan elektronik: Studi pada bocornya data di platform Tokopedia. *Jurnal Hukum Statuta*, 1(2), 122–136.
- Kehista, A. P., Fauzi, A., Tamara, A., Putri, I., Fauziah, N. A., Klarissa, S., & Damayanti, V. B. (2023). Analisis keamanan data pribadi pada pengguna e-commerce: Ancaman, risiko, strategi keamanan (literature review). *Jurnal Ilmu Manajemen Terapan*, 4(5), 625–632. <https://doi.org/10.31933/jimt.v4i5.1541>
- Kholifah, S. N., & Yulhendri. (2024). Analisis manajemen risiko teknologi informasi pada PT Jakarta Notebook menggunakan framework ISO 31000. *Scientica: Jurnal Ilmiah Sains dan Teknologi*, 2(2), 126–138. <https://doi.org/10.572349/scientica.v2i2.90>
- Laksana, T. G., & Mulyani, S. (2024). Pengetahuan dasar identifikasi dini deteksi serangan kejahatan siber untuk mencegah pembobolan data perusahaan. *Jurnal Ilmiah Multidisiplin*, 3(1), 109–122. <https://doi.org/10.56127/jukim.v3i01.1143>
- Lisnawati, T., Husaen, S., Nuridah, S., Pramanik, N. D., Warella, S. Y., & Bahtiar, M. Y. (2023). Manajemen risiko dalam bisnis e-commerce: Mengidentifikasi, mengukur, dan mengelola risiko-risiko yang terkait. *Jurnal Pendidikan Tambusai*, 7(2), 8252–8529. <https://doi.org/10.31004/jptam.v7i2.7534>
- Padang, F. K. N., Anggara, A., Gimnastiar, N. A., Simanjuntak, N. F., Charesyah, A. L., & Arsyadona. (2025). Strategi manajemen risiko siber dalam perusahaan e-commerce di Indonesia: Tinjauan sistematis dan perbandingan dengan praktik global. *Kohesi: Jurnal Sains dan Teknologi*, 6(7), 11–20.
- Putra, D. B., Hakim, M. A. M., & Nurdewanto, B. (2023). Implementasi electronic-know your customer pada aplikasi fintech untuk meningkatkan keamanan akun user. *Journal of Information System and Application Development*, 1(2), 114–123. <https://doi.org/10.26905/jisad.v1i2.11112>
- Putri, N. C. R., Fauzi, A., Ali, M. K., Ramadhan, N. A., Salsabilla, P. J., Cahya, L. J., & Ernawati, F. A. (2024). Strategi peningkatan keamanan data pelanggan dalam penjualan online di Tokopedia. *Jurnal Siber Multi Disiplin*, 2(1), 54–67. <https://doi.org/10.38035/jsmd.v2i1.136>
- Soesanto, E., Lande, A., Sanjaya, H. T., & Hermawan, M. R. (2023). Analisis sistem manajemen keamanan di perusahaan Tokopedia dalam meningkatkan proteksi data

dan privasi pengguna. *Jurnal Mahasiswa Kreatif*, 1(3), 21–29.

Sukarni, Y., & Muslikh, A. R. (2024, December). Evaluasi efektivitas implementasi platform e-learning di FTI Universitas Merdeka Malang menggunakan metode decision tree. In *Seminar Nasional Sistem Informasi (SENASIF)* (Vol. 8, pp. 4621–4631).

Susanto, E., Antira, L., Kevin, K., Stanzah, E., & Majid, A. A. (2023). Manajemen keamanan cyber di era digital. *Journal of Business and Entrepreneurship*, 11(1), 23–33. <https://doi.org/10.46273/job.e.v11i1.365>

Wijanarko, R., Audina, I., Saputri, D. E., Rabbanii, N. N., & Suryanto, T. M. (2023). Implementation of the COBIT 2019 framework to improve information technology performance in Tokopedia. *International Journal of Electrical Engineering and Information Technology*, 6(2), 51–62.

Wulan, W., Hadita, H., Fauzi, A., Putri, A. M., Fitriyani, F., Astriyani, R., & Cahyani, Y. I. (2024). Tinjauan ancaman dan risiko pada sistem keamanan internet of things berbasis cloud computing dalam penggunaan e-commerce dan rencana strategis. *Jurnal Kewirausahaan dan Multi Talenta*, 2(2), 126–137.