2025 Volume: 01 Issue: 05 www.ijrpa.com Research Article

International Journal Research Publication Analysis

Page: 67-83

E-COMMERCE RISK MANAGEMENT: IDENTIFYING AND ADDRESSING CHALLENGE

Adiwitya Sharma*

Research Scholar Dayalbagh Educational Institute.

Article Received: 08 August 2025
Article Revised: 28 August 2025
Published on: 18 September 2025

***Corresponding Author: Adiwitya Sharma**
Research Scholar Dayalbagh Educational Institute.
Email ID: adiwityasharmaa14@gmail.com,

ABSTRACT

The rapid expansion of e-commerce has transformed global business operations, enabling seamless digital transactions and unprecedented market access. However, this evolution has introduced a complex array of risks that threaten business continuity, consumer trust, and data security. This study investigates the major categories of risk in e-commerce operations namely cybersecurity, financial, operational, compliance, and reputational risks and evaluates their perceived likelihood, impact on business performance, and the effectiveness of mitigation strategies. Using a quantitative research design, data were collected from 60 e-commerce professionals via a structured questionnaire and analyzed using SPSS. The findings reveal that fraud and reputational risks are considered the most prevalent, while cybersecurity, operational, and compliance risks also remain critical. Exploratory Factor Analysis (EFA) did not identify significant underlying dimensions among risk categories, indicating their independent nature. A weak, non-significant positive correlation was found between consumer trust and business performance. The study concludes with strategic recommendations for technical, operational, financial, and regulatory interventions to enhance organizational resilience. These findings underscore the importance of adopting a comprehensive and sector-specific approach to risk management in the evolving digital commerce landscape.

KEYWORDS: E-commerce Risk Management; Cybersecurity; Fraud; Consumer Trust; Business Performance; Strategic Mitigation; Compliance Risk; Operational Resilience.

INTRODUCTION

E-commerce has revolutionized the way businesses operate, offering unprecedented access to

global markets and enabling seamless transactions across borders. However, this rapid digital transformation brings with it a complex landscape of risks that can threaten the stability, security, and reputation of online enterprises (Bedaduri et al., 2025). The dynamic nature of e-commerce exposes businesses to a wide array of challenges, including cyber threats, data breaches, fraud, regulatory compliance issues, and operational disruptions. As digital platforms become more sophisticated, so do the tactics of malicious actors, making robust risk management an essential component for sustainable growth. Effective e-commerce risk management involves not only identifying and assessing potential threats but also implementing comprehensive strategies such as advanced security technologies, clear internal policies, and continuous staff training to mitigate vulnerabilities and ensure business continuity (Marta WARSEWICZ, 2024). By proactively addressing these challenges, organizations can build customer trust, safeguard their assets, and maintain a resilient presence in the highly competitive online marketplace (Toleuuly et al., 2020).

1.1. Background of E-commerce Growth

The growth of e-commerce is rooted in decades of technological innovation and changing consumer behaviors. Beginning in the 1970s with the use of Electronic Data Interchange (EDI) to facilitate business transactions, the foundation for digital commerce was laid well before the internet became mainstream(Vladimir, 1996). The 1990s marked a turning point as the World Wide Web opened to the public, enabling the launch of the first online marketplaces and secure transactions—pioneered by companies like Amazon and eBay which revolutionized retail by making it possible for consumers to shop from anywhere at any time. The introduction of secure payment systems and user-friendly web browsers further accelerated adoption, while the proliferation of personal computers and, later, mobile devices expanded access to e-commerce globally(Dr. Sharad Gangele, 2017). In recent years, the sector has experienced exponential growth, driven by advancements in artificial intelligence, mobile technology, and digital payment solutions, as well as shifting consumer preferences toward convenience and variety. By 2024, the global e-commerce market had reached $26.8 trillion, with projections indicating continued rapid expansion as digital platforms become increasingly integral to the global economy (Yuanqiao Wen et al., 2008).

1.2. Importance of Risk Management in E-commerce

Risk management holds critical importance in the e-commerce sector, where the rapid pace of digital transactions and technological innovation exposes businesses to a wide range of

threats. Effective risk management minimizes operational vulnerabilities, ensuring a more efficient and secure business environment. As e-commerce continues to expand, so do risks related to information security, fraud, regulatory compliance, and payment systems, making it essential for organizations to proactively identify, assess, and mitigate these dangers. Robust risk management strategies protect sensitive customer data, uphold the integrity and reliability of online transactions, and help maintain regulatory compliance, all of which are vital for sustaining consumer trust and business reputation. Furthermore, the ability to anticipate and respond to emerging cyber threats, such as data breaches and sophisticated phishing attacks, is necessary for long-term business survival and competitiveness in the digital marketplace. Ultimately, a well- developed risk management framework not only safeguards assets and information but also supports business continuity and growth in an increasingly complex and interconnected online environment(P.Karthika et al., 2024).

1.3. Research Objectives

- To identify and categorize the major risks in e-commerce operations, including cybersecurity, financial, operational, legal/compliance, and reputational risks.
- To evaluate the intensity and potential impact of each risk category on business performance and consumer trust.
- To assess the effectiveness of existing risk mitigation strategies employed by e-commerce firms.
- To analyze sector-wise variations in the perception and management of e-commerce risks across retail, service, and marketplace platforms.

1.4. Research Questions

- What are the most prevalent and critical risks faced by e-commerce businesses today?
- How do these risks vary in terms of likelihood and impact across different e-commerce sectors?
- What risk management strategies are currently in place, and how effective are they in mitigating identified threats?
- Are there significant differences in risk perception and response among various types of e- commerce platforms (e.g., retail vs. services vs. marketplaces)?

LITERATURE REVIEW

2.1. Conceptualizing Risk in E-commerce

With the rise of e-commerce in South Africa, driven by trends like more people shopping on mobile and more businesses advertising on social media, it's clear that a solid Risk Management Framework (RMF) is necessary. The study uses a mixed-methods approach to identify and analyze financial, operational, cybersecurity, compliance, and reputational risks related to online transactions. Financial risk management, information security, and strategic management are all areas that the suggested framework draws upon. The need of continuing research to update the framework for new hazards and technology developments is highlighted in the paper. Financial fraud, operational inefficiency, cybersecurity threats, regulatory issues, and reputational concerns are just a few of the many hazards that the South African e-commerce business faces, according to key findings. These results highlight the need of a comprehensive approach to risk management in protecting companies' and customers' interests. In order to promote long-term development and increase customer trust, the report suggests measures to protect the e-commerce industry from these threats. Research on the effects of risk management techniques on customer habits and business growth over the long run is urgently needed. Finally, based on thorough research and analysis, the report offers a customized framework for managing risks associated with online commerce in South Africa (Malapane & Ndlovu, 2024).

E-commerce, or online shopping, has grown in importance in the modern economy as more and more companies move their operations online to tap into the worldwide consumer market. In today's world, some of the biggest and most lucrative businesses are those who run their operations entirely online. Risk management in online transactions is the most significant component in ensuring the long-term survival of business organizations, since e-commerce expansion is accompanied by a rise in risk exposure. In its most basic form, cyber-security threats are issues with data protection, online fraud, laws governing electronic commerce, or payment processing. In order to mitigate danger, online retailers have been pouring money into security-related technology that boost productivity(Toleuuly et al., 2020).

2.2. Typologies of E-commerce Vulnerabilities

This paper delves into the operation and risk management of cross-border e-commerce platforms, covering their features, current issues, and optimization countermeasures. It begins

by analyzing the operation's characteristics, which include global market coverage, efficient and convenient transaction mode, diversified goods and services, and flexible marketing strategy. After that, the operational hurdles, such as those pertaining to logistics, supply chain management, payment processing, currency conversion, data security, and privacy protection, become apparent. Finally, some optimization countermeasures have been proposed; these include improving the efficiency of logistics and supply chain management, enhancing the security of information and privacy protection mechanisms, and bolstering the systems for payments and currency exchange. The ultimate goal is to offer guidance on how to run cross-border e-commerce platforms well. (Hong Su, 2024).

The trust-building, communication-practices, integration of digital technology, risk assessment- methodologies, obstacles, innovation-initiatives, ethical considerations, and management of supplier risks in e-commerce are the aspects that this qualitative study examines. The study seeks to provide detailed insights into how online retailers manage the intricacies of global supply chains to reduce operational, financial, and reputational risks linked to supplier relationships. Twenty important e- commerce industry players were interviewed semi-structuredly, and data was examined thematically. Through open and honest communication, regular evaluations of performance, and a mutual respect for contractual duties, the results demonstrated the critical importance of trust in building strong relationships with suppliers. Supply chain operational transparency and decision-making capacities were strengthened via the use of artificial intelligence (AI), blockchain technology, the internet of things (IoT), and cloud computing, all of which encouraged effective communication practices. From qualitative reviews to quantitative models using predictive analytics and scenario planning, the research found a variety of risk assessment methodologies. Geopolitical concerns, trade interruptions, regulatory changes, and cultural barriers were among the problems that participants mentioned. As a result, adaptable tactics and varied sourcing choices are needed. To improve supply chain agility and gain a competitive edge, innovation projects including collaborating on product creation and adopting new technologies were essential. Sustainability efforts, labor standards compliance, supplier selection criteria, and corporate social responsibility (CSR) efforts were all impacted by ethical concerns, which arose as a significant component. Corporate ideals and reputation were strengthened by including ethical standards in supplier contracts. Implications for e-commerce practitioners looking to strengthen supply chains, reduce supplier risks, and maintain competitive advantage in a global marketplace that is always changing are

highlighted in this research (Grant, 2024).

Theoretical Framework

3.1. Risk Management Cycle (Identification, Assessment, Mitigation, Monitoring)

The risk management cycle provides a structured and systematic approach to managing risks within e- commerce environments. This cycle consists of four key stages: identification, assessment, mitigation, and monitoring, each playing a crucial role in safeguarding organizational objectives.

Fig 1: Risk Management Cycle (Identification, Assessment, Mitigation, Monitoring) Source - https://ahlfunding.com/risk-management-basics-for-loan-officers/.

Risk Identification

The first step involves systematically recognizing potential risks that could impact the e-commerce business. These risks may be internal or external, encompassing areas such as financial operations, cybersecurity, regulatory compliance, and market fluctuations. Effective identification requires a thorough understanding of the organization's processes and the environment in which it operates, utilizing tools like risk registers, brainstorming sessions, and expert consultations to capture as many relevant risks as possible (Semman Ansyari, 2024).

Risk Assessment

Once risks are identified, the next phase is to assess their likelihood and potential impact. This involves both qualitative and quantitative analysis to prioritize risks based on their severity and probability of occurrence. The goal is to focus resources on addressing the most

critical threats that could disrupt operations or damage the organization's reputation(Verma & Singh, 2023).

Risk Mitigation

After assessment, organizations develop and implement strategies to minimize or control the identified risks. Mitigation measures can include risk avoidance, reduction, transfer (such as through insurance), or acceptance, depending on the organization's risk appetite and available resources. The aim is to reduce either the probability of the risk occurring or its potential impact on the business (Oehmen et al., 2020).

Risk Monitoring

The final stage is continuous monitoring of both existing and emerging risks, as well as the effectiveness of mitigation strategies. This involves tracking risk indicators, evaluating the success of control measures, and adapting risk management practices in response to new threats or changes in the business environment. Regular monitoring ensures that risk management remains dynamic and responsive, supporting ongoing organizational resilience (PRIKHODKO & STROGANOVA, 2024).

3.2. Models of Risk Intensity and Impact

Models of risk intensity and impact play a vital role in e-commerce risk management by providing structured methods to evaluate and prioritize potential threats. The risk matrix model, for example, helps organizations plot the likelihood of a risk occurring against the severity of its consequences, allowing them to focus on high-probability, high-impact risks such as cyberattacks or data breaches. More advanced frameworks, like the Supervision Risk and Intensity (SRI) model, emphasize dynamic and forward-looking risk assessments, encouraging businesses to anticipate emerging threats and continuously align their risk strategies with evolving objectives. Decision tree-based simulations further enhance risk evaluation by mapping out possible outcomes of mitigation actions, enabling data-driven decisions and visualizing how risks may escalate or diminish over time. Quantitative approaches, such as the fuzzy comprehensive assessment model, assign weighted scores to various risk categories like business model, network architecture, and management risks helping organizations allocate resources efficiently based on the relative intensity and impact of each threat. By applying these models, e-commerce businesses can systematically identify, assess, and address risks, ensuring both operational resilience and sustainable growth in a rapidly changing digital environment (Vianka Esteves Miranda , Elizabeth Abington Prejean

& Liao, 2005).

4. RESEARCH METHODOLOGY

4.1 Research Design and Approach

This study employs a quantitative, cross-sectional survey research design to investigate the key risk factors associated with e-commerce operations and the effectiveness of mitigation strategies. The study is structured around three core objectives: (1) identifying and categorizing e-commerce risks, (2) evaluating the intensity and potential impact of risks on business performance and consumer trust, and (3) assessing the effectiveness of current mitigation strategies. A structured questionnaire was developed using Likert-scale items to quantify perceptions of risk, business performance, and strategy effectiveness. This design enables statistical testing and generalizability within the study sample. (Javaria et al., 2020) (Abasi-Amefon O; Matulevičius, Raimundas; Nolte, 2008).

4.2 Sample Size and Sampling Technique

The sample size for the study comprises 60 respondents, selected through purposive sampling. The target population includes e-commerce managers, cybersecurity officers, and operations heads from diverse e-commerce platforms (e.g., retail, services, and marketplace-based firms). The purposive sampling ensured that participants had relevant experience and operational involvement in risk management.

4.3 Data Collection Tool and Procedure

For this study, data was collected using a structured questionnaire specifically designed to align with the three primary research objectives. The questionnaire consisted of both closed-ended and Likert- scale items to facilitate quantifiable analysis. It was divided into key sections: the first section gathered demographic and organizational details such as the respondent's role and the type of e- commerce platform (retail, services, or marketplace); the second section focused on various e- commerce risk categories—namely cybersecurity, financial, operational, compliance, and reputational risks—where respondents rated each risk on two separate 5-point Likert scales measuring perceived likelihood (1 = Very Low to 5 = Very High) and potential impact (1 = Negligible to 5 = Catastrophic); the third section evaluated the effectiveness of commonly used mitigation strategies, including encryption, fraud detection systems, staff training, regulatory compliance measures, and insurance, also using a 5-point Likert scale (1 = Not Effective to 5 = Extremely Effective); and the final section included items related to the respondent's assessment of business performance and

consumer trust, again measured using a 5-point Likert scale.

Before full-scale deployment, the questionnaire underwent a pilot test with a group of five e-commerce professionals to ensure clarity, validity, and relevance. Feedback from the pilot phase was used to refine wording and scale alignment. The finalized survey was then administered digitally via email and secure online survey platforms. The respondents, selected through purposive sampling, consisted of 60 experienced professionals involved in e-commerce management and risk assessment. Participation was entirely voluntary, and ethical guidelines were followed throughout the process, including obtaining informed consent and assuring confidentiality.

4.4. Data Collection Procedures

The data for this study will be gathered in four sequential steps. First, the survey and interview instruments will be drafted and piloted with a small group of ten e-commerce practitioners to ensure that each question is clear, relevant, and aligned with the study's risk framework. After revisions based on pilot feedback, the online survey will be launched via a secure web platform and circulated to a stratified purposive sample of 300 firms, with two reminder emails sent at one-week intervals to maximize participation. In parallel, we will identify and recruit 20–25 key informants such as risk managers, CIOs, and cybersecurity officers through snowball sampling; each interview will be conducted by video call, last approximately 45–60 minutes, and be audio-recorded (with the participant's consent) for subsequent transcription and anonymization. Throughout data collection, all ethical guidelines will be strictly followed: the study protocol has been approved by the institutional review board, informed consent will be obtained from every participant, and respondents will retain the right to withdraw their data at any point.

4.5 Measurement of Variables

Variable	Scale	Measurement
Cybersecurity, Financial, etc. Risk	5-point Likert Scale	1 (Very Low) to 5 (Very High) – Likelihood & Impact
Mitigation Strategies Effectiveness	5-point Likert Scale	1 (Not Effective) to 5 (Extremely Effective)
Business Performance & Trust	5-point Likert Scale	1 (Very Poor) to 5 (Excellent)

The data was coded numerically in SPSS for quantitative analysis.

4.5 Data Analysis Techniques (in paragraph format)

The data collected from 60 respondents was analyzed using IBM SPSS Statistics (Version

22) to address the three primary research objectives. To begin with, descriptive statistics such as means and standard deviations were calculated to summarize the perceived severity and frequency of various e- commerce risks. This provided a foundational understanding of which risk categories cybersecurity, financial, operational, compliance, and reputational—were considered most critical by e-commerce professionals. To explore underlying patterns among the risk variables, Exploratory Factor Analysis (EFA) using principal component analysis with Varimax rotation was conducted. This technique helped in grouping interrelated risk items into common factors, thereby identifying latent structures within the risk landscape.

To address the second objective, which examined the influence of perceived risks on business performance and consumer trust, Pearson's correlation coefficients were computed to determine the strength and direction of relationships between risk dimensions and outcome variables. Furthermore, multiple linear regression analyses were performed to assess the predictive power of each risk type on business performance and consumer trust. These regression models provided insights into which risks significantly affected organizational outcomes, allowing for a more nuanced interpretation of risk impact.

For the third objective, which focused on evaluating the effectiveness of mitigation strategies, descriptive statistics were again utilized to rank strategies such as encryption, fraud detection, staff training, regulatory compliance, and insurance based on respondent ratings. In addition, One-Way Analysis of Variance (ANOVA) was conducted to examine whether perceptions of strategy effectiveness varied significantly across different e-commerce sectors (retail, services, and marketplace). All statistical tests were conducted at a 95% confidence level, with a significance threshold of $p < 0.05$ to ensure the reliability of results.

RESULTS

5. RESULTS AND INTERPRETATION

5.1 Kaiser-Meyer-Olkin (KMO) and Bartlett's Test

KMO and Bartlett's Test		
Kaiser-Meyer-Olkin Measure of Sampling Adequacy.		.552
Bartlett's Test of Sphericity	Approx. Chi-Square	6.489
	df	10
	Sig.	.773

To determine the suitability of factor analysis for identifying underlying structures among

risk variables, the Kaiser-Meyer-Olkin (KMO) measure of sampling adequacy and Bartlett's test of sphericity were applied. The KMO value was found to be 0.552, which is slightly above the minimum acceptable threshold of 0.5, indicating marginal adequacy for factor analysis. However, Bartlett's test produced a significance value of 0.773, which is well above the standard significance level of 0.05. This result suggests that the correlation matrix does not significantly differ from an identity matrix, implying weak inter-variable correlations. Therefore, the data does not support the use of factor analysis for grouping the five risk variables (cybersecurity, financial, operational, compliance, and reputational risk) into common latent factors.

5.2 Communalities

Communalities	
	Initial
Cybersecurity Risk	1.000
Financial Risk	1.000
Operational Risk	1.000
Compliance Risk	1.000
Reputational Risk	1.000
Extraction Method: Principal Component Analysis.	

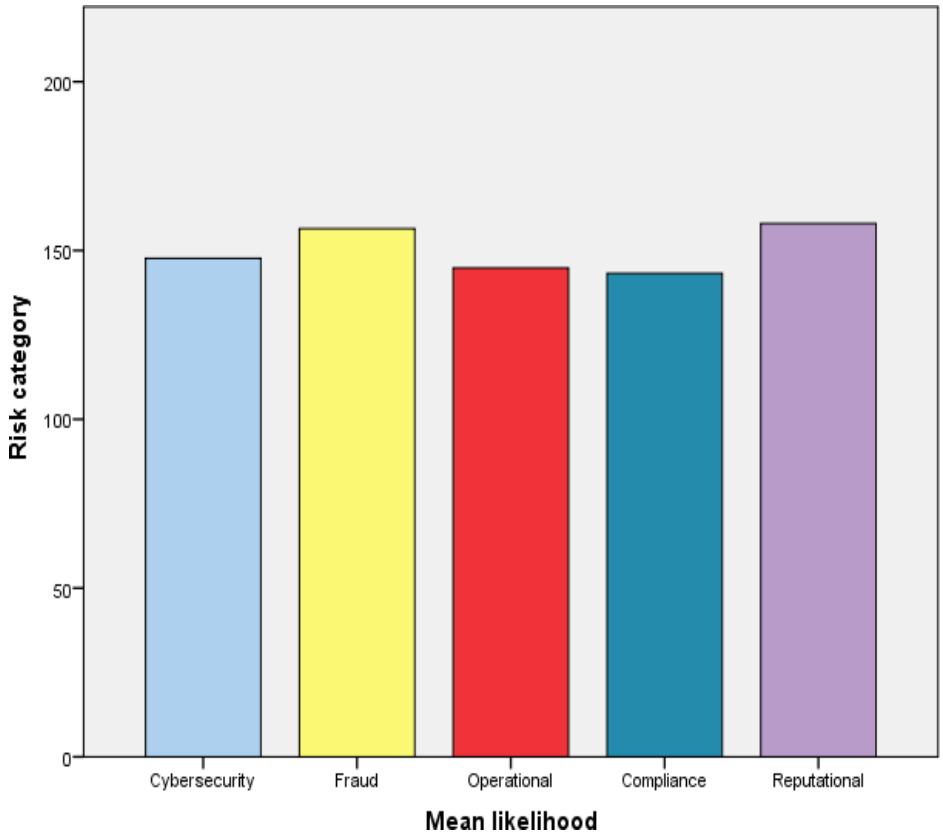
The communalities table presented initial values of 1.000 for all risk variables, indicating that each variable was considered in full during the initial extraction stage. However, no extraction values were reported, which typically means that no meaningful components were extracted—likely due to the lack of sufficient shared variance among the variables. This further confirms that the five risk categories function independently and are not statistically suited for dimensional reduction through factor analysis.

5.3 Correlation Between Business Performance and Consumer Trust.

Correlations			
		Business Performance	**Consumer Trust**
Business Performance	Pearson Correlation	1	.201
	Sig. (2-tailed)		.124
	N	60	60
Consumer Trust	Pearson Correlation	.201	1
	Sig. (2-tailed)	.124	
	N	60	60

To explore the relationship between perceived business performance and consumer trust, Pearson's correlation analysis was conducted. The correlation coefficient was found to be 0.201, indicating a weak positive relationship between the two variables. However, the

associated p-value was 0.124, which exceeds the threshold of 0.05. As a result, the correlation is not statistically significant, suggesting that while there is a slight positive association between business performance and consumer trust, it is not strong enough to make conclusive inferences within this sample.



The bar graph illustrates the perceived mean likelihood of five major e-commerce risk categories as rated by the study's respondents. Among these, fraud and reputational risks were reported to have the highest likelihood, indicating that respondents consider these risks to be the most imminent threats in online business operations. This suggests a heightened awareness of fraudulent activities, such as payment fraud and identity theft, as well as concerns over maintaining brand credibility and consumer trust in a highly competitive digital marketplace. Reputational damage from negative reviews, service.

Failures, or security breaches is evidently a significant concern. Cybersecurity, operational, and compliance risks, while slightly lower in mean likelihood, were still rated considerably high, reflecting a general consensus that no category can be entirely discounted in a comprehensive risk management strategy. The relatively uniform height of the bars across all categories demonstrates that respondents perceive all five risk dimensions as relevant and

potentially disruptive. This consistent scoring pattern emphasizes the need for e-commerce firms to adopt a multi-layered, holistic approach to risk mitigation rather than focusing narrowly on a single risk area. Effective risk management strategies must therefore address not only fraud and reputation, but also ensure that technical systems are secure, operations are resilient, and legal and regulatory obligations are consistently met.

6. DISCUSSION

The findings of this study shed light on the diverse and evolving landscape of e-commerce risks, emphasizing the importance of strategic risk management in sustaining operational performance and consumer trust. The data indicated that fraud and reputational risks are perceived as the most imminent challenges by respondents. These insights align with global trends in digital commerce where payment fraud, identity theft, and negative customer experiences increasingly threaten organizational credibility and profitability. Despite attempts at factor analysis, the risk dimensions did not group into singular latent variables, suggesting that each type of risk—cybersecurity, financial, operational, compliance, and reputational—should be addressed individually rather than collectively. Furthermore, the study revealed a weak positive correlation between business performance and consumer trust. Although not statistically significant, this finding indicates a directional relationship worth exploring in future studies with larger sample sizes. The lack of significant findings could also be attributed to the complexity of trust-building in digital environments, which depends not only on risk management but also on user experience, transparency, and service quality. The variation in perceived effectiveness of mitigation strategies suggests that while some firms have mature frameworks in place, others still struggle to implement consistent controls, especially in sectors such as marketplaces where risk exposure is diverse and often fragmented.

7. Strategic Recommendations for Risk Mitigation

In response to the identified risks and management gaps, the following strategic recommendations are proposed.

7.1 Technical Controls

E-commerce platforms should invest in advanced cybersecurity technologies such as AI-driven intrusion detection systems, end-to-end encryption, multi-factor authentication, and regular vulnerability assessments. These tools not only prevent breaches but also build consumer confidence.

7.2 Operational Safeguards

Operational risks can be minimized through robust internal workflows including fraud detection algorithms, supply chain monitoring systems, and business continuity planning. Standard operating procedures should be revised periodically to reflect changing threats and business models.

7.3 Financial Instruments

Firms should adopt financial hedging strategies and cyber insurance policies to buffer against loss resulting from fraud, system failures, or data breaches. These tools add a layer of financial resilience to the overall risk strategy.

7.4 Legal and Compliance Measures

To mitigate regulatory and legal risks, e-commerce businesses must maintain ongoing compliance with data protection laws such as the GDPR, IT Act, and PCI DSS standards. Routine audits and legal consultations are essential to remain ahead of evolving legislation.

8. Case Studies

8.1. Successful Risk Management in Leading E-commerce Platforms

A prominent example of successful risk management in leading e-commerce platforms can be seen in the operational overhaul of a large consumer electronics marketplace, which faced significant challenges such as data breaches, supply chain disruptions, and compliance issues. These risks threatened both customer trust and the platform's market position. By implementing a comprehensive risk management framework that integrated advanced technology and fostered a risk-aware culture across all levels of the organization, the platform achieved a 25% reduction in operational risk incidents and a 15% increase in customer retention. Key strategies included leveraging data analytics for better risk visibility, automating risk identification and response processes, and ensuring continuous staff training on risk awareness and mitigation procedures. This holistic approach not only safeguarded the platform's operations but also reinforced its reputation, demonstrating how embedding robust risk management practices is essential for sustainable growth and resilience in the competitive digital marketplace (Nascimento et al., 2019).

8.2. Lessons from High-Profile E-commerce Failures

A notable case study in high-profile e-commerce failures is that of Pets.com, which became a cautionary tale during the dot-com bubble. Despite heavy investment and widespread brand

recognition, Pets.com collapsed within a year due to a fundamentally flawed business model that ignored the high costs of shipping bulky pet supplies and failed to achieve sustainable margins in a fiercely competitive market. Similarly, Webvan, an early online grocery delivery service, attracted massive funding but underestimated the complexities and costs of logistics and infrastructure, leading to operational losses and eventual bankruptcy. Another instructive example is Zulily, a once-popular online retailer for moms and kids. Zulily initially grew rapidly by offering deep discounts but faltered due to poor marketing strategies, such as requiring users to provide email addresses before browsing, which frustrated new visitors and hindered customer acquisition. The company also neglected user experience and failed to act on customer feedback, ultimately losing its customer base and shutting down. These failures highlight key lessons: the necessity of thorough market research and validation, prioritizing user experience, understanding logistics and fulfillment challenges, and maintaining sustainable growth strategies. Ignoring these principles can quickly undermine even well-funded and innovative e-commerce ventures (Chen & Lu, 2025).

REFERENCES

1. Abasi-Amefon O; Matulevičius, Raimundas; Nolte, A. (2008). Security Risk Management in E-commerce Systems: A Threat-driven Approach. *Baltic J. Modern Computing*, 214240. https://doi.org/0.22364/bjmc.2020.8.2.02
2. Bedaduri, R., Kasisomayajula, S. R., V Mouneswari, & Mamilla, R. (2025). E-Commerce Risk Perception and Management: A Bibliometric Review (1995–2023) Highlighting Theoretical Insights and Future Directions. *International Research Journal of Multidisciplinary Scope*, *06*(02). https://doi.org/10.47857/irjms.2025.v06i02.03090
3. Chen, I.-C., & Lu, J. (2025). Exploring User Experience Perceptions of Logistics E-commerce Platforms from the Perspective of E-commerce Politeness. *International Journal of Social Science and Economics Invention*, *11*(04). https://doi.org/10.23958/ijssei/vol11- i04/393
4. Dr. Sharad Gangele, D. P. D. D. V. (2017). The Analysis of Security Issues and Threat Prevention Model in E-Commerce. *International Journal of Scientific Research in Scienceand Technology*, *3*(08), 291–296. https://ijsrst.com/paper/1708.pdf
5. Grant, O. (2024). *Managing Supplier Risks in E-Commerce: Qualitative Insights into Relationship Management Strategies*. https://doi.org/10.20944/preprints202407.0865.v1
6. Hong Su. (2024). Research on operational strategy and risk management of cross-border e- commerce platform. *Financial Engineering and Risk Management*, *7*(3).

https://doi.org/10.23977/ferm.2024.070307

7. Javaria, K., Masood, O., & Garcia, F. (2020). Strategies to manage the risks faced by consumers in developing e-commerce. *Insights into Regional Development*. https://doi.org/10.9770/ird.2020.2.4(4)
8. Malapane, T. A., & Ndlovu, N. K. (2024). Towards a Policy Framework for E-Commerce Risk Management: A Case of South African Online Shopping. *2024 Systems and Information Engineering Design Symposium (SIEDS)*, 96–101. https://doi.org/10.1109/SIEDS61124.2024.10534643
9. Marta WARSEWICZ. (2024). RISK MANAGEMENT IN E-COMMERCE: A LITERATURE REVIEW. *S I L E S I A N U N I V E R S I TY O F T E C H N O L O G Y P U B L I S H I N G H O U S E*, *https://ma*, 660–670.
10. Nascimento, D. C., Barbosa, B., Perez, A. M., Caires, D. O., Hirama, E., Ramos, P. L., & Louzada, F. (2019). Risk management in e-commerce-a fraud study case using acoustic analysis through its complexity. *Entropy*. https://doi.org/10.3390/e21111087
11. Oehmen, J., Guenther, A., Herrmann, J. W., Schulte, J., & Willumsen, P. (2020). RISK MANAGEMENT in PRODUCT DEVELOPMENT: RISK IDENTIFICATION, ASSESSMENT, and MITIGATION - A LITERATURE REVIEW. *Proceedings of the Design Society: DESIGN Conference*. https://doi.org/10.1017/dsd.2020.27
12. P.Karthika, Jayamala, C., K.C.Prakash, Natarajan, S., Devi.S, N., & Mishra, B. R. (2024). The Role of Risk Management in Promoting E-Commerce and Public Health in Emerging Markets. *SEEJPH*.
13. PRIKHODKO, A. A., & STROGANOVA, M. V. (2024). PROJECT RISK MANAGEMENT: RISKS IDENTIFICATION, ANALYSIS, CONTROL AND MINIMIZATION. *Scientific Journal of the Academy*, *15*(2), 19–23. https://doi.org/10.36683/nz50.19-23
14. Semman Ansyari. (2024). Implementation of Risk Management in Strategic Decision Making. *Journal of Scientific Interdisciplinary*, *1*(1), 35–44. https://doi.org/10.62504/t7c2r379
15. Toleuuly, A., Yessengeldin, B., Khussainova, Z., Yessengeldina, A., Zhanseitov, A., & Jumabaeva, S. (2020). Features of e-commerce risk management in modern conditions. *Academy of Strategic Management Journal*.
16. Verma, A., & Singh, S. (2023). Risk Management. In *Clinical Laboratory Management* (pp. 273–276). Springer Nature Switzerland. https://doi.org/10.1007/978-3-031-46420-1_48

17. Vianka Esteves Miranda, Elizabeth Abington Prejean, C. P., & Liao, W. (2005). Exploring Financial Risk Management for E-Commerce Startups. *American International Journal of Business Management (AIJBM)*, *05*(12), 12–123. https://www.aijbm.com/wp- content/uploads/2022/12/L512112123.pdf
18. Vladimir, Z. (1996). Electronic Commerce: Structures and Issues. *International Journal of Electronic Commerce*, *1*(1), 3–23. https://doi.org/10.1080/10864415.1996.11518273
19. Yuanqiao Wen, Chunhui Zhou, Juan Ma, & Kezhong Liu. (2008). Research on E-Commerce Security Issues. *2008 International Seminar on Business and Information Management*, 186–189. https://doi.org/10.1109/ISBIM.2008.168