Developing an e-commerce risk management framework for online shopping in South Africa

TA Malapane

orcid.org/0000-0003-4605-2917

Thesis accepted in fulfilment of the requirements for the degree *Doctor of Philosophy in Economic and Management Sciences with Business Administration* at the North-West University

Promoter: Dr NK Ndlovu

Graduation: July 2024

DECLARATION

I hereby declare that this research report submitted for the degree of Doctor of Philosophy in Economic and Management Sciences with Business Administration at the North West University, Potchefstroom Campus, is my own original work and has not previously been submitted to any other institution of higher education. I further declare that all sources cited or quoted are indicated and acknowledged by means of a comprehensive list of references.

LETTER OF CONSENT

N, K. Ndlovu, hereby declare that the inputs and efforts of Tshepo Alex Malapane in the writing of this thesis, is of sufficient scope to be a reflection of his own efforts. I hereby grant permission that that he may submit this thesis for examination purposes in partial fulfilment of the requirements for the degree Doctor of Philosophy in Economic and Management Sciences with Business Administration.

DEDICATION

This thesis is dedicated to my late mother, Maropene Lucy Malapane.

Acknowledgements

First of all, I would like to thank Dr Nkanyiso Kaizer Ndlovu who was my mentor and promotor for his guidance throughout this journey. This thesis would not have been completed without his advice, encouragements and immense knowledge. The thesis has given us new knowledge and experience within this field of e-commerce and risk management context and will pave way for future research. I would like to thank everyone who assisted and supported me in compilation and during the course of doing this work. I would like to express my sincere appreciation to all participants who contributed to this study. Your participation has ensured that the investigation was successful and assisted me to collect the required data. Your support, participation and dedication to ensure this study was successful is acknowledged and appreciated. Special thanks to my amazing friends who are now family, you guys are too many to mention, but I am grateful to God for bringing you into my life, and I wish you all the best life has to offer. See you at the top.

To my late mother, Maropene Lucy Malapane, thank you for raising a giant in me and thanks for the immense prayers and declaration you laid over my life. Your prayers are now yielding results. With love in my heart, special mention goes to my son Alex Thato Malapane for his understanding and space he gave me to pursue this degree without demanding much attention from me. At his age, he understood that dad has a goal to achieve, and he made it possible for this thesis to be completed.

Special appreciation goes to the Wholesale and Retail Sector Education and Training Authority (W&RSETA) for awarding me with a sponsorship bursary to pursue this doctoral degree. Without this resource, this accomplishment would have not been made possible. Your commitment to skills development in the wholesale and retail space is notable and appreciated. May you continue to fund other students and make education fashionable and attainable.

Like the expression of the late former President Nelson Mandela "*It always seems impossible until it's done*", this was a long process which required patience and dedication. Indeed, it's done.

ABSTRACT

In a developing economy such as South Africa, e-commerce is experiencing rapid growth across different industries. This growth can be attributed to several factors, including the increasing penetration of mobile devices and the rise of mobile commerce. Another factor driving the growth of e-commerce in South Africa is the increasing popularity of social media platforms, such as Facebook and Instagram, as marketing and sales channels. This has made it easier for consumers to access online shopping platforms, leading to a growing demand for e-commerce services. The rapidly developing field of e-commerce has significantly changed the landscape of global trade, opening up previously unimaginable opportunities for businesses and consumers alike. The objective of this research was to develop an e-commerce risk management framework that is robust and adaptable for risk management and is particularly well-suited to the complexities of e-commerce environments. In this context, a mixed method research approach was utilised to analyse the perceived risks associated with online shopping to develop an e-commerce risk management framework for South African online shopping. A sequential exploratory research design was adopted for this study. The study employed an exploratory sequential design integrating quantitative and qualitative phases, utilizing random sampling for online shopping clients and convenience sampling for online shopping/e-commerce organizations, employing structured questionnaires for quantitative data collection and interviews stored through recorded transcripts for qualitative data, followed by meticulous data cleaning and coding for analysis through descriptive and inferential statistics for quantitative data and thematic analysis for qualitative data, resulting in a comprehensive understanding of online shopping adoption in South Africa. The proposed framework adopts a multidisciplinary approach to address the diverse difficulties associated with online transactions, drawing on insights from financial risk management, strategic management, and information security. The framework emphasizes the significance of adopting a proactive approach by offering a methodical and structured procedure for identifying, evaluating, and lowering risks across all stages of the e-commerce value chain. This research presents a major finding derived from significant research done to establish an e-commerce risk management strategy specifically tailored for the South African online shopping market. The aforementioned findings play a crucial role in comprehending the present condition of e-commerce risks in South Africa, as well as evaluating the effectiveness of the suggested framework in alleviating these risks. The study found multiple perceived hazards associated with e-commerce in South Africa. These risks encompassed financial, operational, cybersecurity, compliance, and reputational aspects. The frequency of fraudulent activities and payment scams highlighted the financial risks, whilst issues related to logistics, such as delivery inefficiencies, served as examples of operational risks. The escalating occurrences of data breaches and cyber-attacks have brought attention to the significance of cybersecurity risks. Additionally, the growing regulatory framework regulating e-commerce activities has given rise to compliance concerns.

The success of e-commerce is closely linked to customer trust and happiness, as these factors are crucial in mitigating reputational concerns. The study advocates for ongoing research to continuously refine the risk management framework in line with emerging risks and technological advancements. It also encourages research into the long-term impacts of risk management strategies on consumer behavior and market expansion. In conclusion, the findings from this study provide a comprehensive understanding of the perceived risks associated with South African e-commerce and present a tailored framework for risk management. The recommendations put forth are designed to fortify the e-commerce sector against a myriad of risks, ensuring sustainable growth and bolstering consumer confidence. The study's outcomes are instrumental in charting a course for a resilient, secure, and thriving e-commerce industry in South Africa.

Key terms: E-commerce, Online Shopping, Perceived Risks, Risk Management, Risk Management Framework, Risk Analysis

Table of Contents

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS AND ACRONYMS

CHAPTER 1: INTRODUCTION

1.1. CHAPTER OVERVIEW

South Africa has a rapidly growing e-commerce market, with an increasing number of consumers turning to online shopping for convenience and a wider range of options (Taher, 2021). According to a report in Statista (2022), the e-commerce market in South Africa was valued at approximately R20.8 billion in 2022 and is expected to reach R33.6 billion by 2025. The growth of e-commerce in South Africa can be attributed to several factors, including the increasing penetration of mobile devices and the rise of mobile commerce. A report by the World Bank (2021), states that South Africa has one of the highest mobile phone penetrations in Africa, with more than 80% of the population owning a mobile phone. This has made it easier for consumers to access online shopping platforms, leading to a growing demand for e-commerce services. Another factor driving the growth of e-commerce in South Africa is the increasing popularity of social media platforms, such as Facebook and Instagram, as marketing and sales channels. A survey by the South African Council of Shopping Centre (2020), found that more than 70% of South African consumers are influenced by social media when making a purchase decision. As a result, many businesses are now using social media to reach out to customers and promote their products and services.

The rise of e-commerce in South Africa has also been facilitated by improvements in logistics and payment infrastructure (Liang, et al., 2021). Online payment systems, such as PayFast, have made it easier and more secure for consumers to purchase goods and services online. The growth of e-commerce in South Africa also comes with several risks that both customers and online retailers need to be aware of. One of the main risks is security threats, such as hacking and identity theft, which can result in the loss of sensitive information, such as financial details and personal information. A report by the South African Banking Risk Information Center (SABRIC) (2021), found that cybercrime is one of the fastest-growing crimes in South Africa, with online shopping platforms being a prime target for cybercriminals. Another risk faced by customers and online retailers is privacy breaches. Online retailers may collect and store personal information, such as names, addresses, and payment details, which can be vulnerable to theft or misuse. A

survey by KPMG (2020), found that more than 60% of South African consumers are concerned about the security of their personal information when shopping online. Fraud is another risk associated with online shopping. Customers may be tricked into providing their personal information to fake websites or may be conned into purchasing fake goods. Online retailers may also be targeted by fraudsters, who may use fake payment methods or manipulate the online shopping platform to steal goods or financial information. According to a report by the South African Fraud Prevention Service (2021), fraud is a significant issue in the South African e-commerce market, with more than R 100 million lost to online fraud in 2020. To mitigate these risks, both customers and online retailers need to be vigilant and take steps to protect their information and financial details. Customers can protect themselves by only shopping on reputable websites, checking for secure payment methods, and avoiding providing personal information to untrusted sources. Online retailers can reduce the risk of fraud and security threats by implementing robust security systems, such as encryption and secure payment gateways, and by regularly monitoring their systems for suspicious activity.

The concept of perceived risk analysis originated in the field of consumer behavior and marketing, where it was used to understand how consumers evaluate the risks associated with purchasing products or services (Li, 2020). In the context of e-commerce, perceived risk analysis is used to understand the risks perceived by online shoppers and online retailers, and how these risks impact their behaviour and decisions. Perceived risk analysis can be used in e-commerce risk management to identify and prioritize the key risks faced by online shoppers and online retailers. By understanding the risks perceived by these stakeholders, e-commerce companies can develop strategies to mitigate these risks and improve the overall online shopping experience. For example, a perceived risk analysis may identify that online shoppers are concerned about the security of their personal information when shopping online. In response, e-commerce companies may implement robust security systems and communicate these measures to shoppers to reduce their perceived risk and improve their shopping experience. Several studies have used perceived risk analysis in the context of online shopping. A study by KPMG (2020), found that the top perceived risks among South African online shoppers are security, privacy, and fraud. The study also found that perceived risk has a significant impact on the likelihood of an individual shopping online, with those perceiving high levels of risk being less likely to shop online. Yoon and Lennon (2019), found that perceived risk is a

key factor in online shopping behaviour, and that online shoppers are more likely to purchase from websites that have a secure payment system and have good reviews from other shoppers.

Another study by Kim, Lee, and Lee (2021), found that perceived risk is a major factor in the decision to purchase from cross-border e-commerce websites. The study found that perceived risk is influenced by several factors, including the perceived reliability of the website, the perceived security of the payment process, and the perceived privacy of personal information. The study also found that e-commerce companies can reduce perceived risk by providing information on their security measures and by offering secure payment options. The importance of e-commerce risk management cannot be overstated in today's increasingly digital world. With the growth of online shopping, online retailers must ensure that they have implemented a robust risk management framework to increase customer trust and ensure the security of sensitive information and financial transactions. In this background document, this study will discuss the reasons why e-commerce risk management is important and why online retailers should take it seriously. Firstly, e-commerce risk management helps to protect sensitive customer information such as credit card details, addresses, and personal information. In the absence of proper security measures, this information can be vulnerable to theft and fraud, which can cause significant harm to the customers and damage the reputation of the online retailer (Furnell & Warren, 2016). Furthermore, online retailers are often storing large amounts of financial data, which can be an attractive target for cybercriminals. This makes it even more important for online retailers to implement strong security measures to prevent unauthorized access and protect customer information.

Secondly, e-commerce risk management helps to increase customer trust and confidence in online shopping. Customers are more likely to purchase products online if they feel confident that their personal and financial information is secure. A study conducted by the Ponemon Institute found that a significant proportion of customers are reluctant to shop online due to concerns about security (Ponemon Institute, 2016). Therefore, online retailers must implement measures to mitigate risks and increase customer trust in the online shopping process.

Additionally, e-commerce risk management helps to comply with regulations and laws regarding data protection and privacy. Many countries have laws and regulations in place to protect the privacy of customers and their personal information, and online retailers must comply with these regulations to avoid legal consequences. For example, the European Union's General Data Protection Regulation (GDPR) sets out strict rules for the protection of personal data, and non-compliance can result in significant fines (European Commission , 2016).

Furthermore, e-commerce risk management can help to mitigate financial risks for the online retailer. In the event of a security breach, an online retailer can incur significant financial losses, including the cost of rectifying the breach, compensating customers, and repairing damage to the retailer's reputation. Implementing a risk management framework can help to minimize the financial impact of security incidents and reduce the likelihood of financial losses. The field of e-commerce risk management has gained considerable attention in recent years as online shopping has become increasingly popular. However, despite the growth of online shopping in South Africa, there is a gap in the literature when it comes to e-commerce risk management in this specific context. This study aims to address this gap by developing an e-commerce risk management framework through perceived risk analysis for South African online shopping. Perceived risk analysis is a well-established concept in the field of marketing, which considers the risks that consumers perceive when making a purchase. This type of analysis has been widely used in the context of online shopping, as it helps to understand the factors that influence consumer trust in online shopping.

The significance of this study lies in the fact that e-commerce risk management is critical to increasing consumer trust in online shopping. Online retailers must be aware of the risks faced by customers and implement measures to mitigate these risks in order to build customer trust. A risk management framework that considers the perceived risks of customers would be a valuable tool for online retailers in South Africa. Moreover, the South African online shopping market is unique in terms of the challenges faced by both customers and online retailers. For example, South Africa has a high level of cybercrime, and this poses a significant risk to customers when shopping online. Online retailers must be aware of these challenges and implement appropriate measures to protect their customers from these risks. This study aims to contribute to the literature on e-commerce

risk management by developing a framework through perceived risk analysis for South African online shopping. The results of this study will be useful for online retailers in South Africa as they strive to increase customer trust in online shopping and overcome the challenges faced by both customers and online retailers.

1.2. BACKGROUND OF THE STUDY

The e-commerce sector is a developing sector universally including in South Africa. Unfortunately, this sector is confronted with several perceived risks that are influencing the sector at large. The current study is expected to add to the comprehension of initial, risks related to online shopping, and also, to develop a model to combat risks related to shopping online. The focal point of the study is consequently, to develop a framework for risk management developed through an analysis of perceived risks. Several studies have been directed in the area of risk management in South Africa and around the globe, nonetheless, a framework to address the difficulties radiating from the perceived risks of online shopping has not been developed (Li, et al., 2020).

In South Africa, e-commerce risk management research has been conducted for e-commerce and its perceived riskThere are about 41.19 million active internet users in South Africa introducing an open door for e-commerce growth as reported by Statista (2023). This growth is probably going to accompany increment cybercrimes. Cybercrime is an expansive term encompassing acts perpetrated or encouraged utilising computer technology (Nukusheva, Zhamiyeva, Shestak, & Rustembekova, 2022). These violations are carried out by people who have extraordinary skills on the internet to carry out the wrongdoing while others use computer programmes to accomplish these criminal objectives. Over the worth chain, these cybercrimes influence the adequacy of e-commerce. Some of these cybercrimes are basically new variations of customary types of bad behaviour, for example, robbery and misrepresentation where computers are utilised to steal personal identifications, passwords and credit card data. On the other hand, more complex cybercrimes happen by culprits in the interests of disrupting or trying to claim ignorance of administration assaults. A requirement for a robust, framework for risk management in the e-commerce space is justified by this reality.

1.3. PROBLEM STATEMENT

Globally, selling and buying goods has changed over time with the emergence of e-commerce over time. While e-commerce encompasses a wide range of applications and processes, risk management for online shoppers is one of the biggest problems facing the global community (Wai, et al., 2019). In South Africa, the same problem exists with cybercrimes topping the list of complicated criminal cases (Dlamini & Mbambo, 2019). Perceived risks are among the issues affecting online shoppers. According to Malapane (2019), the specific problem is South Africa does not have a comprehensive e-commerce framework for risk management in place to deal with cybercrimes and other perceived risks affecting online shoppers. Hence the country is faced with the challenges of being unable to deal with or persecute cybercrime activities affecting e-commerce (Salifu, 2008). A report by South African Banking Risk Information Centre (SABRIC), revealed that a total of 16296 acts of cybercrimes were recorded in the banking sector alone in 2018 substantiating the vulnerability of e-commerce in South Africa (SABRIC, 2021).

On the internet and the overall online shopping space, customers experience highlights of vulnerability, frailty and an absence of control adding to risk perceptions of online-based shopping (Glavas, Letheren, Russell-Bennett, McAndrew, & Bedggood, 2020). Online shoppers are targeted by cyber-criminals presenting risks associated with financial, privacy, cybercrime and many other forms of risks. The business landscape is ever-changing with a new phenomenon called “digital disruption” caving in (Bin Che Hasni, 2023). This presents complex challenges regarding how e-commerce and online shopping can improve business performance. The way individuals and organizations see online shopping from a tight viewpoint is that despite all the promotions and guarantees, online shopping might be years from understanding its maximum capacity. Various examinations have been directed in the region of internet shopping as far as seen danger and variables adding to the absence of development in the e-commerce space, nonetheless, a gap exists in studies that seek to address the risk management domain in the online, web-based shopping experience (Malapane, 2019; Kim, et al., 2021; Dlamini & Mbambo, 2019; KPMG, 2020). E-commerce has become a pattern of the current economy. E-commerce is regarded as a new trend and online shop owners as well as online shopping users cannot avoid risks in transactions. The administration of risk in online and web-based business exchanges is the most significant factor for the drawn-out endurance of an e-commerce business. These risks may be identified with web

misrepresentation, data security, installment techniques, or even internet business enactment. Once getting into one of those risks, it would be expensive for businesses to tackle and to recoup. It is assessed that it costs e-commerce and direct marketing-based organizations billions of dollars every year, making it basic for merchants to comprehend the risks related to doing business on the internet (Mandura, 2023).

1.4. RESEARCH AIM AND OBJECTIVES

1.4.1. Research aim

The main aim of the study was to develop a framework for risk management through an analysis of perceived risks in the South African online shopping market.

1.4.2. Research Objectives

To achieve the stated overarching aim, the study pursued the following objectives:

i) To determine perceived risks associated with e-commerce in South Africa.

ii) To determine risk management factors affecting e-commerce in the South African online shopping market.

iii) To determine the impact of perceived risks on e-commerce in South Africa.

iv) To develop a framework for risk management of e-commerce in the South African online shopping market.

v) To offer recommendations to manage perceived risks in e-commerce in South Africa.

1.5. RESEARCH QUESTIONS

To achieve the above-mentioned objectives, the study responded to the following research questions:

i) What are the perceived risks associated with the online shopping market in South Africa?

ii) What are the risk management factors affecting the e-commerce in South African online shopping market?

iii) What effect do perceived risks have on e-commerce in South Africa?
iv) What are the tools and techniques that can be used to mitigate perceived risks on e-commerce in South Africa to develop a framework for risk management?
v) What are the impacts of perceived risks on the quality-of-service delivery of online shopping in South Africa?

1.6. SIGNIFICANCE OF RESEARCH

Online businesses have become prevalent in developed and developing economies alike, allowing for an increasing variety of online business options. While the development and expansion of online shopping are picking up energy internationally, purchasers' perceived risk has been considered a key worry of a dynamic cycle during online shopping (Aggarwal, et al., 2020). According to Malapane (2019); Shingange (2022), South Africans are scammed and defrauded daily while shopping online. The interest of this study was to develop a risk management framework for e-commerce in the South African online shopping market in pursuit of developing a risk management model to combat online shopping risk while contributing to the body of knowledge. This area has not been researched extensively and therefore presents an opportunity for ground-breaking and solution-finding. This study contributed to my personal career focus and assisted both companies/firms and consumers who make use of online shopping as their business or preference of shopping in the era of the Fourth Industrial Revolution (4IR). A framework was developed for the risk management industry benefiting both the business and academic community. The current study contributes to the e-commerce and risk management research networks by applying an organized threat-driven way to deal with the Information Systems Security Risk Management (ISSRM) domain model for an internet business system. It gives a comprehension of its arrangement to ISSRM strategy communicating threats, risks and risk treatment ideas utilising modeling and analytical tools.

1.7. DELIMITATIONS

According to Liao and Hitchcock (2018), “delimitations are choices made by the researcher which should be mentioned and describe the boundaries that the researcher has set for the study”. This study was limited to the participants, including online shopping

users and owners of e-commerce businesses in South Africa. The study did not investigate or assess risk management; rather it developed a framework through an analysis of perceived risk.

1.8. LIMITATION OF RESEARCH

The following limitations applied in this research study:

Sample size - the number of units of analysis used in this study is dictated by the type of research problem proposed to be investigated. While the sample size was not too small, it was difficult to find significant relationships from the data, to ensure a representative distribution of the population and to be considered.

Lack of available and/or reliable data - a lack of data or reliable data required the study to limit the scope of analysis, and the size of the sample, and this was a critical impediment in finding a pattern and a significant relationship.

Lack of prior research studies on the topic – There was a limited body of literature in the area of risk management in terms of e-commerce. Although a limitation was not a good thing in research, in this case, this served as *an* important opportunity to describe the need for further research.

1.9. ELIMINATION OF BIAS

This study avoided bias at all costs. Qualitative research of this nature is exploratory research that aims to understand a certain problem, occurrence, or phenomenon by collecting and reviewing subjective information and participant observations (Mohajan, 2018). This research aimed to accurately and correctly interpret the information striving to study the data with limited bias or outside influence.

1.10. ETHICAL CONSIDERATION

The objective of research ethics is to ensure that no adverse consequences or harm follow from the research activities. Human beings are deserving of respect and protection as inalienable rights (Habermas, 2018). This was similar to the situation during research exercises for what it is worth in some other conditions. Ethical considerations in research are critical. Ethics are the norms or standards for conduct that distinguish between right and wrong (Pearson, 2016). They help to decide the contrast between satisfactory and inadmissible practices. For this research, participants were requested and informed

consent was obtained before participation. Permission from the e-commerce business owners and participants was solicited before the study could commence. All participants were asked to give their consent before participating in the study. They were also assured that every response would be recorded with strict confidentiality. The questionnaire was not harmful to the participant and the study will bear sound ethical considerations to all participants. Permission to conduct a study at selected e-commerce businesses was requested.

The data collected for this research was purely utilized for this research and was not shared with external parties. The researcher was open to signing a confidentiality agreement if deemed necessary by the participant. For the duration of the research, the researcher ensured safe keeping of the collected data, and treated the data with confidentially as stipulated in the first draft of an informed consent form. The results in the form of the research findings were shared with the interested participants. The researcher ensured that the University information management policy was employed in managing the data from when it was submitted and facilitated archiving.

1.11. ETHICAL PRINCIPLES FOLLOWED

- All possible ethical issues were identified, those that had the potential to harm participants were identified and eliminated as much as possible and the risks involved were made known to the participants. This was issued together with the research instrument in the form of the “participant information sheet”.
- An informed consent letter was drawn up and accompanied the research instrument selected sample before participants participated in the survey and subsequently the interview. This was to ensure that participants were fully aware of what the research was about, the purpose of the research, who the sponsors of the research were, if any, and their rights around participation in the research.
- The ethical clearance formed part of this research and was facilitated through the North West University ethical committee.
- The research instrument, informed letter of consent, and the information sheet were distributed by email to the participants so that they could familiarise themselves with the research, their rights, and the contents of the research instrument.

- The identity of the participants was protected by ensuring that the data capturing only focused on variables being measured and not the names of the participants, their race, or the name of the organization.
- The participants were requested to send an email response to the researcher as an indication of their voluntary willingness to participate in the interview.
- Once the willingness response was obtained, the researcher scheduled a reasonable time for the interview session so that the participants could have enough time to check that the proposed time suits their schedule.
- Before the beginning of the interview session, the researcher allowed the participant to ask for clarity if there were areas that needed to be cleared and to check if the participant was still comfortable to continue with the interview.

1.12. OUTLINE OF THE THESIS

Chapter 1: Introduction: This chapter provides the scope of the thesis, in which the background information, statement of the problem, research aim, and objectives were provided. This area of research defined as well as the necessity to execute the study flowing from identified problems, which act as motivation to execute the study. The objectives for the study are set and the demarcation of the study was presented.

Chapter 2: Literature Review: This chapter provides the theoretical framework underpinning the research problem. This chapter provides a basis for the development of the conceptual framework of the study. It also provided an in-depth literature review. This was guided by the research questions applicable to this study.

Chapter 3: Research Methodology: This chapter detailed the research design, data collection methods, analysis techniques and ethical considerations employed in conducting the research. The chapter further presented the methodology the study employed. This is characterised by an in-depth research methodology and process followed to carry out this study.

Chapter 4: Results: In this chapter, the results obtained in this study were presented and provided. The chapter further presented results, discussion and interpretation of findings.

Chapter 5: Analysis: This chapter presented an analysis of all the results and findings of the study. The chapter contains full discussions, interpretations and evaluations of the results regarding the literature. This chapter also included theory building.

Chapter 6: Conclusions: This chapter contains conclusions, limitations, and recommendations. The chapter further analysed, discussed and evaluated the research findings in the light of the theoretical framework established in chapter two. It also presented the recommendations and conclusion of the study. These are preceded by discussions.

CHAPTER TWO: LITERATURE REVIEW

2.1. CHAPTER INTRODUCTION

This chapter provides a context of the e-commerce industry and its growth in a global and South African context. It closely examines previous scholarly work on the trajectory of growth within the e-commerce sector, paying close attention to the perceived risks of e-commerce from the perspective of consumers. It also examines previous bodies of knowledge to explain how the Fourth Industrial Revolution (4IR) is significantly expanding the e-commerce trade. The previous bodies of knowledge indicate policies that e-commerce traders should implement in business models for the continuous growth of e-commerce trading within a South African context.

2.2. LITERATURE REVIEW

The Internet is a worldwide correspondence medium that is progressively being utilised worldwide as a creative apparatus for showcasing merchandise and ventures (Clemes, et al., 2014). While there is a remarkable increment in the e-commerce development, Doherty, Ellis-Chadwick, Allred, Smith and Swinyard (2006) accept that like the customary shopping channel, at the digital shopping condition, perceived risk is characterised as the potential for misfortune in seeking after an ideal result while occupied with online or web-based shopping. It is generally accepted that numerous organisations are rapidly embracing the web as the method through which they can proficiently and financially lead their advertising exercises, and this accompanies numerous risks related to utilising it (Gorla, Chiravuri & Chinta, 2017). Shopping on the web presents risks and threats that should be overseen and relieved against. E-commerce has seen a gigantic development in recent years. Numerous elements have added to this extraordinary development like expanded web and advanced smart-phones, efficient, accessibility of shifted and less expensive items, comfort and simplicity of shopping, and no weight from the salesman (McQuitty & Peterson, 2000).

The study on e-commerce in South Africa is anchored in several theoretical frameworks to understand its rapid growth and associated risks. The growth of e-commerce in developing economies like South Africa can be understood through the lens of the Innovation Diffusion Theory (García-Avilés, 2020), which posits that the adoption of innovations, such as e-commerce, spreads through a population over time. The increasing penetration of mobile devices and the rise of mobile commerce can be analyzed using the Technology Acceptance Model (Zaineldeen, 2020), which explores users' acceptance and adoption of new technologies. Additionally, the popularity of social media platforms as marketing and sales channels aligns with Social Influence Theory (Otterbring & Folwarczny, 2024), which suggests that people's behaviors are influenced by their social environment. The study's development of a risk management framework draws on theories from financial risk management, such as the Capital Asset Pricing Model (Mandala, et al., 2023), which helps in evaluating and managing financial risks. Strategic management theories, such as the Resource-Based View (Barney, et al., 2021), inform the identification and utilization of resources to mitigate risks. Information security theories, like the theory by (Girsang, et al., 2020), guide the understanding and management of cybersecurity risks. The study's emphasis on consumer trust and happiness relates to theories of relationship marketing (Yazdanpanah & Ehsani, 2020), which highlight the importance of building long-term relationships with customers. Furthermore, the call for ongoing research aligns with the concept of dynamic capabilities (Teece, 2020), which emphasizes the need for organizations to continuously adapt to changing environments. The study integrates various theoretical perspectives to develop a comprehensive understanding of the e-commerce landscape in South Africa and proposes a tailored risk management framework to navigate its complexities.

2.3. EMERGENCE OF E-COMMERCE

E-commerce is a business exchange directed electronically on the Internet (Rayport & Jaworski, 2002). It is commonly a popular expression for the utilization of the web to encourage exchanges in deals and installment of products and ventures between parties. These gatherings can incorporate various orders, for example, Customer-to-Customer, Business-to-Customer, Business-to-Business, Business-to-Government, and so on. Nonetheless, with the end goal of this proposition, the e-commerce system alluded to and

zeroed in on, is the Business-to-Consumer type. This class comprises of various business measures that together accomplish the objective of e-commerce. The study also focused on analyzing the demand management cycle within an online Business-to-Customer (B2C) retail setting. The expanding cross-outskirt business possibilities in the online market space is making e-commerce more worthwhile for retailers (Donthu & Garcia,1999). This move from disconnected to web-based shopping has presented vulnerabilities and issues to the customers identified with protection, item quality, conveyance, and so forth. Such concerns lead to the development of perceived risk in customers' purchasing choices (Cases, 2002).

Numerous examinations have talked about the role of the website as a risk reduction function in internet shopping (Jiuan, 1999; Cases, 2002; Park & Kim, 2003). Most studies have likewise managed recognising the relationship between customers' perceived value and buy expectations in online settings (Yang & Peterson, 2004; Aggarwal, et al., 2020; Clemes, et al., 2014). These researchers inspected the function of buyer's perceived risk inside quality-esteem relationship in retailing setting and recognised the requirement for analysing the relationship in various shopping techniques, one of them being internet retailing and expressed that purchasing on the web may not just lead to changes in the perceived client esteem yet additionally factors affecting it. Along these lines, the focal point of this research was to address the current gap identified in the literature.

The emergence of e-commerce has been a transformative development in the world of business and commerce. It has changed the way people buy and sell goods, communicate with businesses, and interact with each other online. E-commerce has its roots in the development of the Internet and the World Wide Web (WWW) in the late 20th century (Rathnayake, 2021). Since then, e-commerce has grown rapidly and has become an integral part of the global economy (Wu & Gereffi, 2018).

E-commerce refers to the buying and selling of goods and services over the Internet (Friedman, 2023). It has revolutionized the way businesses operate by providing a new platform for commerce that is fast, convenient, and accessible (Baumeister & Leary, 1995). With the increasing availability of high-speed Internet, businesses can now reach a global audience with ease, which has led to increased competition and new growth opportunities (Schneider & Tilson, 2020). This has also led to a shift in the way

businesses market their products, with a greater emphasis on digital marketing and the use of social media (Friedman, 2019).

One of the key advantages of e-commerce is its ability to provide consumers with greater convenience and accessibility to goods and services (Wu, et al., 2018). With the rise of e-commerce, consumers can now shop online from the comfort of their homes, 24 hours a day, seven days a week (Baumeister & Leary, 1995). This has made shopping more accessible for people with disabilities, busy schedules, or those living in remote areas (Friedman, 2019). Moreover, e-commerce has also made it easier for consumers to compare prices and products from different vendors, which has increased the level of competition and driven down prices (Schneider & Tilson, 2020).

Another advantage of e-commerce is its ability to provide businesses with new opportunities for growth and expansion. E-commerce has allowed businesses to reach new markets and customers, both domestically and internationally (Wu, et al., 2018). It has also made it easier for businesses to sell products and services to customers, who can purchase goods and services directly from the company's website (Baumeister & Leary, 1995). This has reduced the need for physical retail stores, which has resulted in lower overhead costs and increased profitability (Friedman, 2019). However, the rise of e-commerce has also led to some challenges and risks. One of the biggest challenges has been the issue of security and privacy (Schneider & Tilson, 2020). With the increasing amount of personal and financial information being transmitted over the Internet, there is a growing concern about the security of this information (Wu & Gereffi, 2018). Additionally, e-commerce has also increased the risk of fraud and counterfeiting, which has led to a need for better measures to protect consumers (Baumeister & Leary, 1995). Despite these challenges, the growth of e-commerce is expected to continue as more and more businesses embrace the advantages of online commerce (Friedman, 2019).

2.4. ONLINE SHOPPING

Online Shopping is a form of electronic commerce that allows consumers to directly buy goods or services from a seller over the Internet using a web browser (Gefen, Karahanna, & Straub, 2003). Consumers find a product of interest by visiting the website of the retailer

directly or by searching among alternative vendors using a shopping search engine, which displays the same product's availability and pricing at different e-retailers. Researchers such as Hoffman, Novak and Chatterjee (1995); Alba, Lynch, Weitz and Janiszewski (1997); Peterson, Balasubramanian and Bronnenberg (1997), have discussed the benefits of online shopping. These benefits provide the sorts of convenience that are not readily available in traditional shopping media. Electronic commerce also magnifies the uncertainties that are involved with purchases through the internet; and shoppers who perceive more risk associated with this shopping channel are less willing to purchase online (Bhatnagar, Misra, & Rao, 2000).

Lack of trust towards e-commerce sellers has its grounds for security concerns such as fraud by illegal merchants, privacy concerns i.e., using personal information for commercial purposes, or performance concerns such as receiving low-quality products or services. Some of the researchers emphasize that the reason many consumers do not proceed to online purchases is that they simply do not trust most web merchants to give their credit card information or personal information (Bashir, et al., 2018; Will, et al., 2017; Ur Rahman, et al., 2018). Lack of environmental control exists while consumers have less control over online sellers' actions over their bank card information. Lack of control over personal information is very important specifically the concern that online sellers use their personal information for marketing promotional purposes, without their knowledge or permission.

Online shopping appeared to be a new type of shopping method approximately 20 years ago, has been getting more attention along with the spread of the internet due to the unbeatable convenience it brought about to the consumers. The transaction can be held in any place accessed to the internet. Furthermore, consumers can buy a wide choice of products across geographic boundaries while saving time and absence of sales pressure without worrying about transportation and parking (McQuitty & Peterson, 2000).

2.5. PERCEIVED RISK

A study show that there have likewise been endeavors to examine the perceived risk in web utilization settings, notwithstanding, the observational exploration for online purchasers' perceived online risk has not been indisputable (UKEssays, 2018). Perceived

risk is the vulnerability a customer has when purchasing products, generally, those that are especially costly, for instance, vehicles, houses, and laptops or computers (De Kerviler, et al., 2016). Each time a purchaser thinks about purchasing an item, the individual has certain questions about the item, particularly if the item being referred to is exceptionally estimated. Perceived risk can likewise be perceived as a lot of vulnerabilities that buyers have in their psyches while buying an item with respect to the result of the item utilization. It is somewhat of a mental and practical danger that buyer feels are taking while at the same time buying that item.

2.5.1. Financial Loss

Studies in the area of perceived risk associated with e-commerce have noted that financial loss ai one of the highest risks (Malapane, 2019; Rajan, et al., 2017). Many companies are reported to have lost money due to cybercrimes (Poufinas & Vordonis, 2018). The vulnerability of the IoT results in more financial loss which more often cannot be recovered. The complexity and sophistication of such cyber-crimes are hard to track and investigate as they are often done remotely from one country to another. A study by Rajan, Ravikumar and Al Shaer (2017), concluded that cybercrime rates are increasing year-on-year and the consequences include financial and reputational damage, loss of privacy and breaches of intellectual property.

2.5.2. Privacy Risk

The internet has had a profound effect on all aspects of modern living and makes businesses and individuals vulnerable to being targeted by cybercriminals (Rajan, et al., 2017). According to Malapane (2019), cybercrime incidences are reported to be increasing globally resulting in data manipulation, scams, online hacking and many other negative factors that increase the privacy risk of users. The study further reports that regions around the world are trying to find amicable solutions that can see these privacy risks mitigated. Social media is also adding to the vulnerability of the IoT in such that access to personal data and information is simplified and cybercriminals use this information to harm victims.

2.5.3. Risk Management

Risk management is a general concept, applied to many areas and domains of life, not just in financial management. It is characterized as the planned exercises to direct and control an association with respect to chance (Iso.org, 2018). Security risk management, on the other hand, has its focus on risks that occur through malicious intent as the word security here, defined by Firesmith (2003), is “the degree to which malicious harm is prevented, detected, and reacted”. For the purpose of this proposed research, the definition by Firesmith (2003) is most appropriate.

2.5.4. Risk Analysis

According to Modarres (2016), risk analysis is defined “as a process of identifying and analysing potential issues that could negatively impact key business initiatives or critical projects in order to help organizations avoid or mitigate those risks”. It is further understood that in order to conduct a risk analysis, you should initially recognize the potential risks that you face, and afterward estimate the probability that these risks will emerge. It is important to understand that risk analysis as referred to above is a tool that will be used to draw on detailed information such as financial data, security protocols, and other relevant information.

2.6. E-COMMERCE IN SOUTH AFRICA

E-commerce in South Africa has been growing rapidly in recent years, driven by a combination of factors including increasing Internet penetration and smartphone adoption (Bostock & Smith, 2018). The e-commerce industry in South Africa is characterized by a diverse range of players, including large multinational corporations, local small and medium-sized enterprises (SMEs), and online marketplaces (Naidoo & Mpofu, 2019). Despite the growth in e-commerce, the sector is still in its early stages and faces several challenges, including a lack of infrastructure and low levels of trust in online transactions (Bostock & Smith, 2018).

One of the key drivers of e-commerce growth in South Africa is the increasing availability of affordable Internet access and the growing popularity of smartphones (Naidoo & Mpofu, 2019). The proliferation of these technologies has led to a surge in online

shopping, making e-commerce more accessible and convenient for consumers (Bostock & Smith, 2018). This has also enabled local SMEs to reach new markets and compete more effectively with larger corporations (Naidoo & Mpofu, 2019). However, the lack of infrastructure and limited access to technology in rural areas still presents a significant challenge to the growth of e-commerce in South Africa (Bostock & Smith, 2018).

The South African e-commerce industry is dominated by a few large players, including multinational corporations and online marketplaces (Naidoo & Mpofu, 2019). These companies have leveraged their significant resources and expertise to capture a large share of the market (Naidoo & Mpofu, 2019; Bhatnagar & Ghose, 2004; Clemes, Gan, & Zhang, 2014). Despite the dominance of these large players, local SMEs have been able to establish a presence in the e-commerce sector using online marketplaces (Lynch, et al., 2001). These marketplaces provide SMEs with an effective platform to reach new customers and sell their products and services (Bashir, Anwar, Awan, Qureshi & Memon, 2018).

One of the main challenges facing the growth of e-commerce in South Africa is the low levels of trust in online transactions (Bostock & Smith, 2018). This is largely due to concerns about security and privacy, as well as a lack of familiarity with e-commerce and online shopping (Bhatnagar, Misra, & Rao, 2000; UKEssays, 2018). To overcome these challenges, it is important for e-commerce companies to invest in security and privacy measures, as well as to educate consumers about the benefits and risks of online shopping (Aggarwal, et al., 2020).

Another challenge facing the e-commerce sector in South Africa is the lack of infrastructure and support for small businesses (Dlamini & Mbambo, 2019; Naidoo & Mpofu, 2019). This includes access to capital, training and mentorship programs, and technical support (Bostock & Smith, 2018; Friedman, 2019). To address these challenges, the government and private sector need to invest in programs and initiatives that support the growth of small businesses and e-commerce (Hoffman, et al., 1995). This includes investment in digital infrastructure, such as high-speed Internet and mobile networks, as well as support for the development of digital skills. In conclusion, e-commerce in South Africa is growing rapidly, driven by increasing Internet penetration and smartphone adoption. Despite this growth, the sector still faces several challenges,

including a lack of infrastructure, low levels of trust in online transactions, and limited support for small businesses. To address these challenges, e-commerce companies need to invest in security and privacy measures, as well as for the government and private sector to invest in programs and initiatives that support the growth of small businesses and e-commerce.

2.7. ONLINE SHOPPING REVOLUTION

According to Makhitha and Ngobeni (2021), factors affecting online shopping include demographic factors, perceived benefits, perceived risks, consumer innovativeness and attitude and intention.

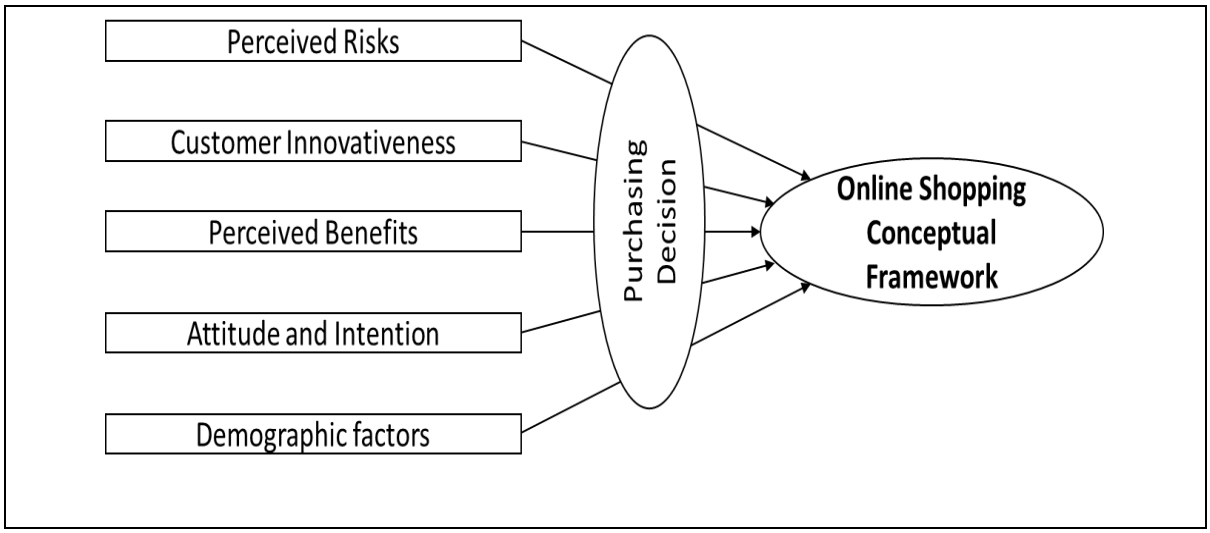

Figure 1. Online Shopping Conceptual Framework

Online shopping appeared to be a new type of shopping method approximately 20 years ago, has been getting more attention along with the spread of the internet due to the unbeatable convenience it brought about to the consumers. In addition to convenience, previous research indicates other attractive factors. The transaction can be held in any place accessed by the internet. Furthermore, consumers can buy a wide choice of products across geographic boundaries while saving time and the absence of sales pressure without worrying about transportation and parking (McQuitty & Peterson, 2000).

2.8. ARTIFICIAL INTELLIGENCE IN THE SOUTH AFRICAN E-COMMERCE

According to Exenberger and Bucko (2020), Artificial Intelligence (AI) in e-commerce has been widely adopted. A developing country like South Africa is adopting AI, especially in its e-commerce spaces. Withstanding the evidence that e-commerce is growing rapidly,

South Africa's use of e-commerce is still growing with the potential to grow further. The emergence of technological changes has significantly shifted the way that businesses operate. In most industries, they have shifted their operations into becoming mostly online. The covid-19 lockdown also resulted in an increased need to adopt methods of operation that rely primarily on e-commerce. According to Tang, Bai, Zhao and Yuan (2020), "*AI is intelligence demonstrated by machines, as opposed to the natural intelligence displayed by animals and humans*." AI research has been defined as the field of study of intelligent agents, which refers to any system that perceives its environment and takes actions that maximize its chance of achieving its goals (Winston, 1984; McCarthy, 2007). The adoption of artificial intelligence has happened gradually within South Africa over the years. South Africa is a third-world country, but it is considered the most developed African country. This is because of their numerous initiatives in various industries that create employment.

According to (Martino, 2021), the banking sector is a prime example of how the adoption of technological advancements can significantly change how an industry operates. When the banking industry initially began to adopt technological advancements, they started with the adoption of automated teller machines. This phased out the need for bank tellers and created a job market for banking consultants. In essence, this highlights how the adoption of technological advancements can change an industry drastically. This is how the use of AI as an operational model has changed how South Africans operate (Ochara, et al., 2022). It has allowed most operations in organisations to change. In recent years banks have adopted the use of a hybrid model of operation. The illustration below shows how AI impacts e-commerce in a four-step process.

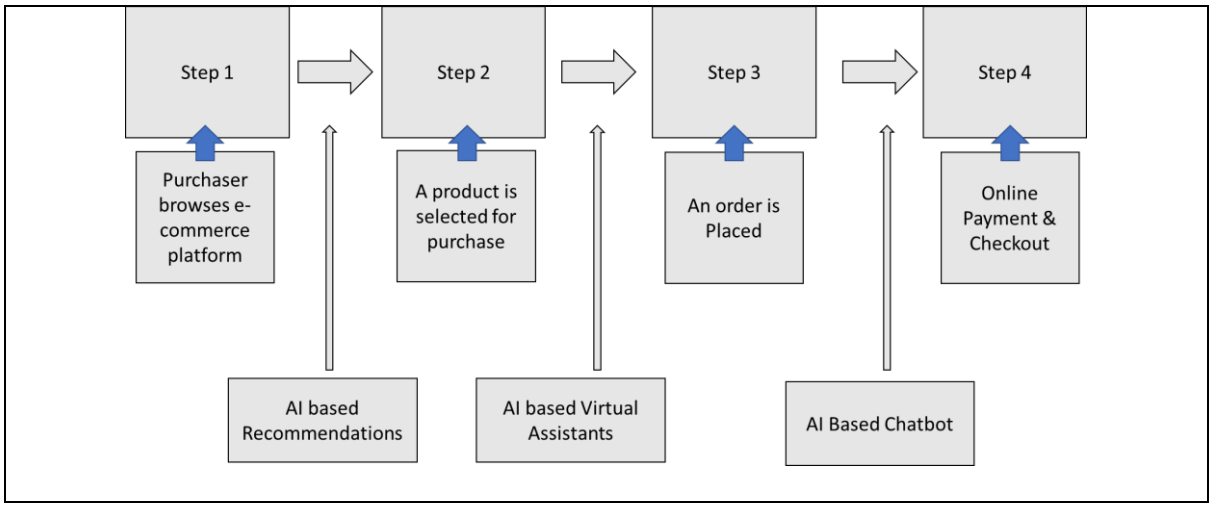

Figure 2. Artificial Intelligence Impact in E-Commerce

2.9. E-COMMERCE FROM A BUSINESS PERSPECTIVE

To understand the factors that influence online shopping, Bucko, Kakalejčík and Ferencová (2018) necessitate a rationale of this lens within a business perspective, paying particular attention to the digitization of the internet. Regarding their previous scholarly work, Bucko et al. (2018) point out that the internet has propelled the globalisation of businesses leaning towards e-commerce for buying and selling. The internet has pushed the boundaries of e-commerce, as Bucko et al. (2018) note, it is achieved without the use of physical stories. Notably, the authors also observe the relevance of international communication within new dimensions as e-commerce gains momentum on a global scale.

Businesses in accordance with their perspective are constantly in fierce competition with other stakeholders for what can be termed the lion's share of customers. The internet is profoundly relevant for successful e-commerce trading connecting businesses to customers, irrespective of geographical barriers (Chafey, 2015). E-commerce is underpinned by social and economic activity propelled through globalisation in a digitized landscape. For this reason, Bucko et al. (2018) assert that businesses in accordance with their perspective are constantly in fierce competition with other stakeholders for what can be termed the lion's share of customers.

E-commerce is essential to customers for every sector, highlighting how e-commerce has revolutionised the online shopping experience. The rise of e-commerce as accorded by Bucko et al. (2018) also notes how traditional businesses have shifted their business operations to meet the demands of buying and selling online. The business rationale as observed by these researchers notes the drastic increase of sales in e-commerce for companies, not using brick-and-mortar setups, as consumer goods can be sold anywhere and anytime with consideration to companies that offer same-day services and delivery. They also note greater earning potential, as e-commerce removes physical barriers with regard to access to services and products. By the same virtue, these authors take into consideration marketing control of data extraction to gauge shopping behaviour or favour towards certain products. A business, particularly those in e-commerce can only gain more financial gains by understanding consumer behaviour through data profiles of online shopping. Literature confirms that the factors that affect the e-commerce adoption in the

business environmentinclude political, technological, economic and social factors (Valencia-Arias, et al., 2021). The illustration diagram below outlines these factors.

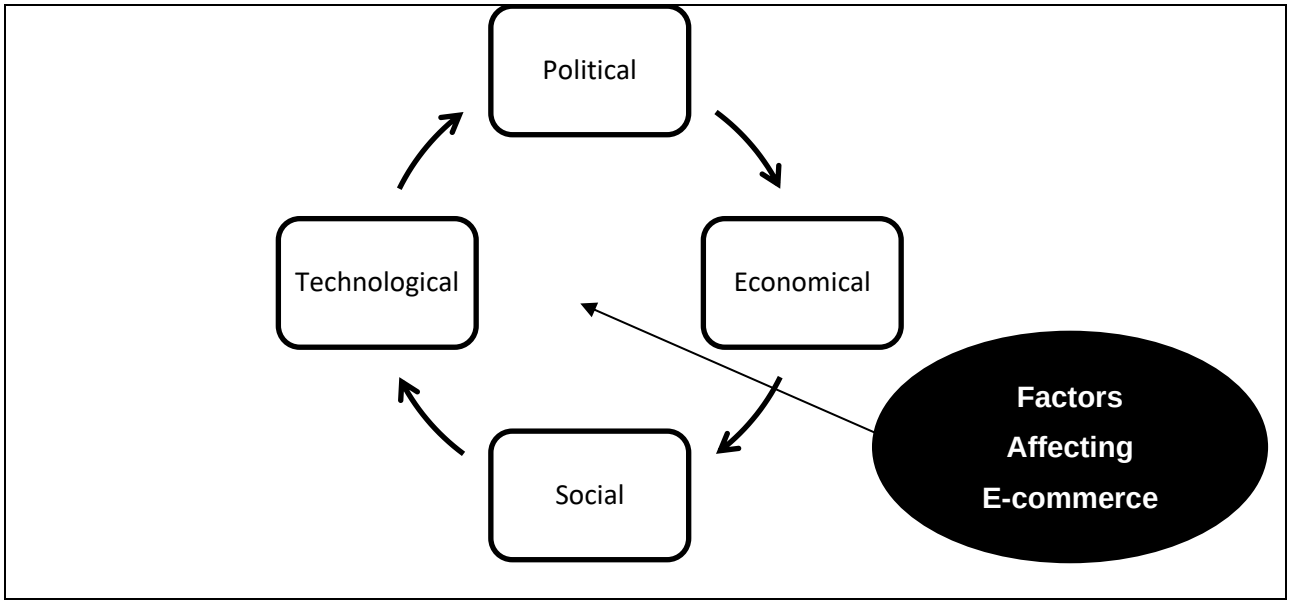

Figure 3. Factors Affecting E-Commerce

B2C is not new, but Bucko et al. (2018) still necessitates a rationale of this type of e-commerce from the perspective of the consumer. The online shopping experience for consumers has notable advantages, as Bucko et al. (2018) examine the factors that influence online shopping versus traditional shopping. Convenience and access to a wider variety of goods influence customers to buy products online, as globalisation fosters networks to mass online shopping outlets. Consumers use the ease of having goods and services and delivered. However, Bucko et al. (2018) also point out that age and literacy are contending factors that can be viewed in tandem as factors that drive consumers to pursue online shopping. Their view is that literacy is critical with notable concerns of cyber-crimes, as consumers lean on e-commerce brands that are marketed through recognised channels. The consumer in their view must be literate on the process of online shopping and delivery processes for successful B2C.

Moreover, Bucko et al. (2018) underscore the significance of trust in the online marketplace. Trust is an integral aspect that bridges the gap between consumers and online retailers, influencing their purchasing decisions. Establishing trust involves various factors, including transparent communication, secure payment gateways, and reliable delivery services. Furthermore, Bucko et al. (2018) highlight the role of customer reviews and ratings in fostering trust among online shoppers. Positive reviews and high ratings

not only validate the credibility of the product but also instill confidence in potential buyers, facilitating a smoother B2C transaction. Therefore, understanding and nurturing trust are imperative for businesses operating in the realm of online commerce, as it directly impacts consumer behavior and loyalty.

The online shopping experience offers comfort and ease of goods and services but also bears the challenge of consumers being wary of online transactions and insecure payment platforms. Considerable efforts to maximise the experience of B2C are thus critical for e-commerce for growth and attraction of customers with attention to safe online shopping. With regard to age, Bucko et al. (2018) point out that certain age groups can be seen as a factor in the rationale of online shopping.

2.10. PERCEIVED RISK IN E-COMMERCE

E-commerce has grown exponentially in recent years and is rapidly changing the way people shop and conduct business. One of the main challenges faced by consumers in the online environment is perceived risk, which refers to the uncertainty or anxiety associated with purchasing products or services online (Kim, et al., 2021). In order to facilitate online transactions, it is important for e-commerce companies to understand the factors that contribute to perceived risk and to develop strategies to mitigate i. In this literature review, the main components of perceived risk in e-commerce will be discussed and the findings from previous research in the field will be summarized.

Other studies show that there have likewise been endeavors to examine the perceived risk in web utilization settings, notwithstanding, the observational exploration for online purchasers' perceived online risk has not been indisputable (UKEssays, 2018). Perceived risk is the vulnerability a customer has when purchasing things, generally those that are especially costly, for instance, vehicles, houses, and laptops or computers (Mello & Pépece, nd). Each time a purchaser thinks about purchasing an item, the individual has certain questions about the item, particularly if the item being referred to is exceptionally estimated. Perceived risk can likewise be perceived as a lot of vulnerabilities that buyers have in their psyches while buying an item with respect to the result of the item utilization. It is somewhat of a mental and practical danger that buyer feels are taking while at the same time buying that item.

The Internet is yet viewed as a dangerous shopping place which implies a significant part of buyers' perceived risks exceed the benefits of web-based shopping in their purchase choices (Miyazaki & Fernandez, 2001). Further research additionally demonstrates that the development of the internet into a mass mode for commerce is pretty much simply the digitalization through specialized advancement of different methods of distant buying, for example, by means of phone or mail-request, which accompany similar risks of protection and security. Furthermore, Bhatnagar and Ghose (2004) examined the effect of a couple of shopping advantages and chances and presumed that customers were more worried about web attributes related to perceived risks than web ascribes related to benefits. Be that as it may, their exploration included just one advantage, comfort. Different authors have analysed the non-functional advantages of shopping online, be that as it may, these investigations didn't inspect the effect of perceived risks (Mathwick, Malhotra & Rigdon, 2002). No distributed exploration has examined, in a far-reaching way, purchasers' view of both the advantages and risks related to online shopping.

Bucko et al. (2018) also refer to previous scholarly work that indicates consumers display hesitant behaviour if they lack trust in the web merchandiser, especially in regard to their personal information and credit card information (Bashir, et al., 2018; Will, et al., 2017; Ur Rahman, et al., 2018). Notably, previous scholarly work highlights that while online shopping has advantages, the other side of this coin presents the concern of trust and lack of control over purchases from the perspective of the consumer viewpoint. Consumers accorded to Bucko et al. (2018) are less likely to support a web merchandiser if their personal information is used for marketing purposes without their informed consent and knowledge. Bucko et al. (2018) concurs with Bashir et al. (2018); Will et al. (2017); and Ur Rahman et al. (2018) regarding perceived risks of online shopping within a lens of rationale from the consumer perspective. Consumers who feel doubtful or may have unpleasant online shopping experiences with a particular retailer are less like to engage in online shopping, with preference to traditional shopping.

Bucko et al. (2018) also discusses the concept of advertising noting contrasting viewpoints regarding online shopping. Advertising is necessary to market products for B2C with businesses paying attention to the marketing process. However, the studystate that advertising is not necessarily an influence on B2C as consumers pay more attention

to issues of return of online purchases and refunds. These concerns from the consumer lens can also be a perceived risk associated with online shopping.

According to Lim (2003), financial risk, product risk, delivery risk, time risk and privacy risk are the most perceived risks by consumers who utilize online shopping. These risks contribute to the purchasing decisions and influence the consumers' choice of shopping.

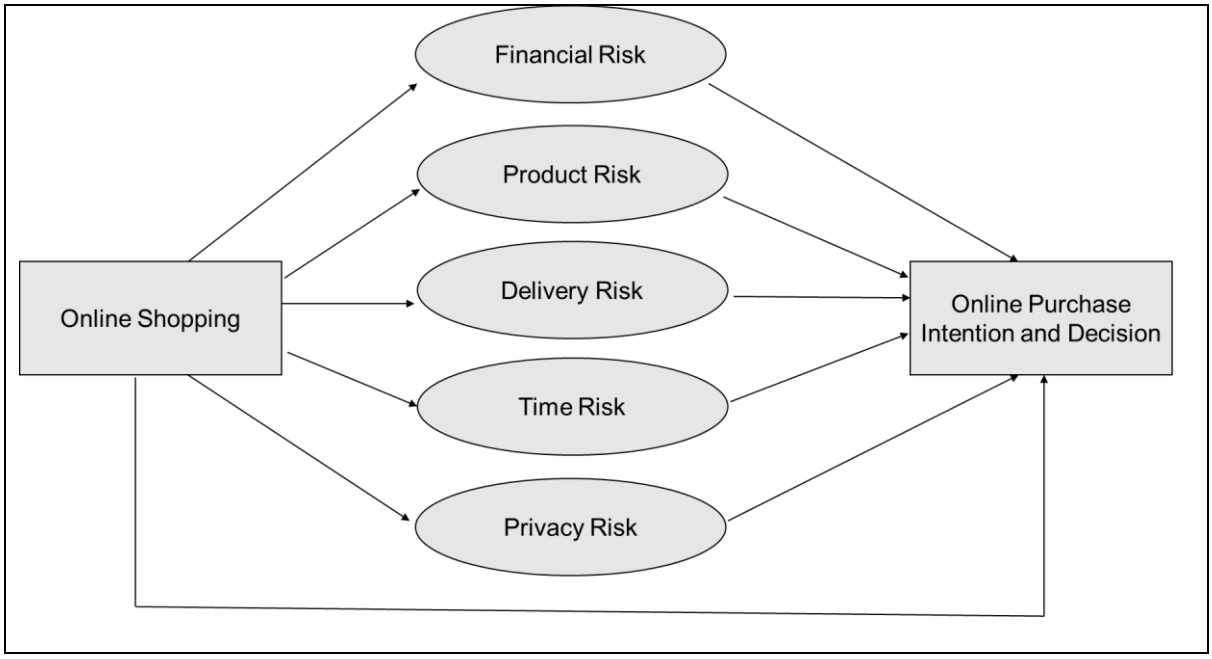

Figure 4. Perceived Risks in Online Shopping

2.11. COMPONENTS OF PERCEIVED RISKS

Perceived risk can be broken down into several different components, including financial risk, product risk, privacy risk, and performance risk (Kim, et al., 2021). Financial risk refers to the concern that the consumer may not receive their money back if the product is unsatisfactory or if their personal information is stolen. Product risk involves uncertainty about the quality and reliability of the product, while privacy risk pertains to the fear that personal information may be misused or stolen. Performance risk refers to the fear that the online transaction will not be completed as expected or that the delivery of the product may not be prompt and efficient.

2.11.1. Financial Risk

Studies have found that consumers are more likely to make online purchases when they feel that their financial information is secure (Kim, et al., 2021). In order to reduce financial

risk, e-commerce companies must implement secure payment systems and provide clear and detailed information about their return policies. Additionally, consumers may feel more secure if they can make purchases using trusted payment methods, such as credit cards or PayPal (Kim, Lee & Lee, 2021; Aggarwal, Albert, Hill & Rodan, 2020).

2.11.2. Product Risk

Consumers are more likely to make online purchases when they feel confident about the quality and reliability of the product (Kim, Lee & Lee, 2021). One way to reduce product risk is to provide detailed product information, including specifications, reviews, and images (Kim, Maslowska & Malthouse, 2018). Another approach is to offer a money-back guarantee or a warranty, which can provide added peace of mind for the consumer (Kim, Maslowska & Malthouse, 2018). Makhitha and Ngobeni (2021), give attention to the perceived risks of online shopping from the perspective of the consumer. The study cite previous work that indicates perceived risks to be a concern as customers must feel satisfied and safety is another area of concern. They further point attention to product satisfaction as another risk, stating that e-commerce products catering to an online market must meet the customer's needs.

When customers view product descriptions online; it gives them an indication of the type of product. However, e-commerce traders must ensure accuracy in these descriptions because consumers make an intention to purchase online. For this reason, they highlight this area, noting that products can differ in person and online. They highlight that customer satisfaction can be viewed as a domino effect, as customers also have their networks, and they can become wary of products that do not fit accurate descriptions and mention that this is significant for the growth of online purchases for e-commerce traders.

2.11.3. Privacy Risk

Consumers are often wary of sharing personal information online, as they fear that their information may be misused or stolen (Kim, Maslowska & Malthouse, 2018). In order to reduce privacy risk, e-commerce companies must implement secure systems to protect customer data and provide clear and concise information about their privacy policies. Additionally, companies should be transparent about what information they are collecting and why and should give consumers the option to opt out of data collection.

2.11.4. Performance Risk

Consumers are more likely to make online purchases when they feel confident that the transaction will be completed efficiently and that the product will be delivered on time (Bhatnagar & Ghose, 2004). To reduce performance risk, e-commerce companies must have a user-friendly website and an efficient delivery system (Bhatnagar, Misra & Rao, 2000). Additionally, companies should provide clear information about delivery times and shipping costs and should have a customer service team available to address any issues that may arise (Dlamini & Mbambo, 2019).

In conclusion, perceived risk is a major barrier to online transactions and must be carefully considered by e-commerce companies. By understanding the different components of perceived risk, companies can develop strategies to mitigate it and encourage consumers to make purchases online. By implementing secure payment systems, providing detailed product information, protecting customer data, and having a user-friendly website and efficient delivery system, e-commerce companies can reduce perceived risk and increase consumer confidence in the online environment.

2.12. ANALYSIS OF PERCEIVED RISK IN E-COMMERCE

To understand and analyse perceived risk in e-commerce, several studies have been conducted in the past few years (Mathur, 2015; Pi & Sangruang, 2011; Ko, Jung, Kim & Shim, 2004). One of the most widely cited frameworks for analysing perceived risk in e-commerce is the Technology Acceptance Model (TAM) developed by Davis (1985), which suggests that perceived ease of use and perceived usefulness are the primary factors affecting consumers' intentions to use technology. Another model that has been used to analyse perceived risk in e-commerce is the Information Systems Success Model (ISS) developed by (DeLone & McLean, 1992). The ISS model argues that perceived usefulness, perceived ease of use, and perceived system quality are the primary drivers of user satisfaction and acceptance of information systems. A study by Kim, Lee and Lee (2021), found that perceived risk is a significant factor affecting consumers' purchase intentions in e-commerce. The study also found that perceived risk can be reduced by building trust in the online vendor, providing secure payment systems, and providing clear and accurate information about the product or service.

More recently, a study by Lu, Wu & Wei, (2019), found that the perceived risk of e-commerce transactions is influenced by the level of personal involvement with the product or service, the perceived complexity of the transaction, and the perceived level of security of the online platform. The study also found that perceived risk is significantly reduced by the presence of strong security measures such as secure payment systems, privacy policies, and secure servers. In conclusion, perceived risk in e-commerce is an important factor affecting consumer behaviour and must be considered by e-commerce businesses. Understanding the drivers of perceived risk, such as perceived ease of use, perceived usefulness, perceived system quality, personal involvement, and the level of security of the online platform, can help e-commerce businesses reduce perceived risk and increase consumer confidence.

2.13. FINANCIAL LOSS IN E-COMMERCE

The increased convenience of e-commerce has also brought new risks, particularly in the area of financial loss (Aggarwal, Albert, Hill & Rodan, 2020). Research has been conducted to better understand and address the financial losses experienced in the e-commerce industry. This literature review aims to analyse the findings of this research and provide an overview of financial loss in e-commerce.

2.13.1. Chargeback Fraud

Chargeback fraud is described as one of the primary causes of financial loss in e-commerce where this type of fraud occurs when a consumer disputes a charge on their credit card and the bank reverses the transaction, resulting in a financial loss for the merchant (Bhatla, Prabhu & Dua, 2003). Research has shown that chargeback fraud is a growing problem in the e-commerce industry, with chargebacks increasing by 22% between 2016 and 2018 (CyberSource, 2018). One study found that most of the chargeback fraud is committed by organized crime groups using stolen credit card information (Xu & Wang, 2015). This figure represents a significant amount of financial loss for both businesses and consumers. Fraud can occur in various forms, including credit card fraud, identity theft, and phishing scams. Merchants can reduce their risk of chargeback fraud by implementing security measures such as using secure payment gateways and verifying the authenticity of the customer's information (CyberSource, 2018).

2.13.2. Cybercrime

Cybercrime, such as hacking and data breaches, can also result in significant financial losses for e-commerce companies. Research has shown that cybercrime is becoming more sophisticated and widespread, with e-commerce businesses being particularly vulnerable to attacks (Anderson et al., 2013). In one study, it was found that the average cost of a data breach in e-commerce was $1.1 million (Ponemon Institute, 2016). Research shows that data breaches can lead to significant financial losses for businesses and consumers. This study further discovered that the average cost of a data breach for businesses in the United States is $3.62 million(Brewer et al., 2019). Consumers are also at risk of financial loss due to security breaches. For instance, a report by the Identity Theft Resource Center (2020), found that the average cost of identity theft is $1,343. To reduce the risk of cybercrime, e-commerce businesses must implement strong security measures, such as regularly updating software and using secure payment systems. It is also recommended to educate employees on how to identify and prevent cybercrime (Brewer et al., 2019).

2.13.3. Product Returns

In the e-commerce industry, product returns can also result in financial loss for merchants. One study found that product returns can account for up to 30% of a company's total operating costs (Chang & Chen, 2019). Product returns can be reduced by improving the accuracy of product descriptions and providing clear return policies. The effects of financial loss in the e-commerce industry can be far-reaching. For businesses, financial loss can result in decreased profits and reduced growth. For consumers, financial loss can result in damage to their credit scores and a loss of trust in online shopping. Furthermore, financial loss in the e-commerce industry can have a negative impact on the overall economy.

A report by the National Cyber-Forensics and Training Alliance (2017), found that financial loss due to fraud and other security breaches can result in decreased consumer confidence and decreased economic growth. To mitigate financial loss in the e-commerce industry, various strategies have been proposed. One of the most effective strategies is the implementation of security measures, such as encryption, firewalls, and multi-factor authentication. Research shows that these security measures can significantly reduce

the risk of fraud and security breaches, and thus, minimize financial loss (Demertzis & Wolff, 2019). Another strategy is to educate both businesses and consumers about the dangers of e-commerce fraud and security breaches.

2.14. PRIVACY RISK IN E-COMMERCE

Privacy risks in the e-commerce industry have become a major concern for consumers and businesses alike (Baruh, Secinti & Cemalcilar, 2017). The proliferation of online transactions and the sharing of sensitive information such as credit card details and personal information have increased the likelihood of privacy breaches. This literature review aims to examine the research work done in the area of privacy risk in the e-commerce industry and their findings. Several studies have found that privacy concerns play a significant role in consumers' decisions to engage in e-commerce transactions (Lee & Turban, 2001; Dinev & Hart, 2006).

According to Lee and Turban (2001), privacy concerns in e-commerce can be classified into three categories: data collection, data usage and data protection. Data collection refers to the collection of personal information by e-commerce companies, data usage refers to the use of personal information by e-commerce companies and data protection refers to the protection of personal information from unauthorized access and use. Furthermore, Dinev and Hart (2006) found that privacy concerns can also be divided into three main categories: information quality, information security and information control. Information quality refers to the accuracy and completeness of the information collected by e-commerce companies, information security refers to the protection of the information collected and stored by e-commerce companies and information control refers to the control of the use of the information collected by e-commerce companies.

Another study by Xu and Wang (2015) found that privacy concerns can have a negative impact on consumer trust and confidence in e-commerce. According to the study, consumers who have higher privacy concerns are less likely to engage in e-commerce transactions. In order to reduce privacy risks in the e-commerce industry, (Xu and Wang, 2015), suggest that e-commerce companies should adopt privacy protection technologies and implement privacy policies.

Similarly, a study by Kim, Kim & Lee, 2018, found that privacy risks in e-commerce can have a significant impact on consumer trust and satisfaction. The study found that privacy risks can lead to decreased trust and satisfaction in e-commerce transactions and that e-commerce companies can reduce privacy risks by implementing privacy protection technologies and adopting privacy policies. Privacy risks in the e-commerce industry have become a major concern for consumers and businesses alike. The proliferation of online transactions and the sharing of sensitive information have increased the likelihood of privacy breaches. Several studies have found that privacy concerns play a significant role in consumers' decisions to engage in e-commerce transactions and that privacy risks can have a negative impact on consumer trust and satisfaction. To reduce privacy risks in the e-commerce industry, e-commerce companies should adopt privacy protection technologies and implement privacy policies.

2.15. E-COMMERCE RISK MANAGEMENT FRAMEWORK

Several studies have been conducted on e-commerce risk management frameworks, providing insight into the risks associated with e-commerce activities and the measures required to mitigate them (Ratnasingam, 2007; Evangelidis, 2004; Karoui, 2016; Reid, 2000). One of the earliest e-commerce risk management frameworks was proposed by (Xia & White, 2009), which consists of four phases: risk identification, risk analysis, risk response, and risk monitoring and control. The first component, risk identification, involves identifying potential risks that may arise in e-commerce operations. This component is crucial as it provides the basis for the rest of the framework, as it allows e-commerce businesses to identify and prioritize the risks that need to be addressed. The second component, risk assessment, involves evaluating the likelihood and impact of each identified risk. This component helps e-commerce businesses determine the level of risk they are exposed to and prioritize their risk mitigation efforts. The third component, risk control, involves implementing measures to reduce the impact of identified risks, while the final component, risk monitoring, involves ongoing monitoring of risk mitigation efforts to ensure that they are effective and that new risks are identified promptly.

Overall, the framework proposed by Xia and White (2009) provides a comprehensive approach to managing risks in e-commerce operations. By following the four components of the framework, e-commerce businesses can effectively evaluate and mitigate risks, helping to ensure their long-term success. Another e-commerce risk management framework is the IT Risk Management Framework (IRMF) developed by the (Information Systems Audit and Control Association (ISACA), 2010). The IRMF provides a structured methodology that helps organizations identify, assess, prioritize and mitigate IT risks while aligning risk management with their overall business objectives. One of the key strengths of the IRMF is that it covers all aspects of IT risk management, including people, processes, technology, and data. It considers both the internal and external threats to IT systems and data, as well as the specific needs of different types of organizations, regardless of size or industry.

Additionally, it provides clear guidance on how to integrate risk management into the overall governance and management of IT systems, thereby enhancing their effectiveness. As per the ISACA (2010), the IRMF is based on the following principles: accountability, transparency, due diligence, integration, and continuous improvement. These principles emphasize the importance of involving all relevant stakeholders in the risk management process, as well as the need to continuously monitor and improve the risk management framework over time. The IRMF is widely recognized as a best-practice approach to IT risk management and has been adopted by organizations of all sizes and industries around the world. A study by Al-Qirim and Al-Qirim (2017), proposed a risk management framework specifically for small and medium-sized enterprises (SMEs) in the e-commerce industry.

This framework emphasizes the importance of identifying and prioritizing the various risks faced by SMEs in the industry, including security and privacy risks, technology-related risks, and business risks. The authors argue that SMEs often face unique challenges in the e-commerce industry, including limited resources and a lack of expertise in managing risk. To address these challenges, the authors propose a four-step risk management process, which includes risk identification, risk assessment, risk mitigation, and risk monitoring and evaluation.

The authors found that this framework can help SMEs effectively identify, assess, and manage the various risks associated with their e-commerce operations. They suggest that by using the framework, SMEs can develop a comprehensive understanding of the risks they face and prioritize their risk mitigation efforts accordingly. The authors also suggest that the framework can help SMEs improve their risk management processes over time by continually monitoring and evaluating their risk mitigation strategies. Overall, the authors believe that the framework can help SMEs in the e-commerce industry minimize the negative impact of risks on their businesses and improve their overall resilience.

Zhang, Li and Liu (2018), proposed a risk management framework for cross-border e-commerce. The authors identified the challenges and risks of cross-border e-commerce, such as legal and regulatory risks, technological risks, and cultural risks. Based on these challenges, the study developed a comprehensive risk management framework that consists of five components: risk identification, risk assessment, risk control, risk monitoring and evaluation, and risk response. The framework is designed to be flexible and adaptable to the changing needs of cross-border e-commerce, which is a rapidly growing and evolving industry. The authors tested the framework using a case study of a cross-border e-commerce company. The results showed that the framework was effective in identifying, assessing, and mitigating risks in the company's operations.

The framework provided a systematic and holistic approach to risk management in cross-border e-commerce, which can help companies minimize the negative impact of risks on their operations and ensure the success and sustainability of their businesses. The framework can also serve as a useful reference for other companies engaged in cross-border e-commerce and provide valuable insights for further research in this area. The literature review shows that there are several e-commerce risk management frameworks available, each with its unique focus and approach. However, they all share a common goal of providing a systematic approach to identifying, evaluating, and mitigating e-commerce risks. Organizations in the e-commerce industry can choose the framework that best fits their needs and requirements. It is important for organizations to regularly review and update their e-commerce risk management framework to ensure that it remains effective and relevant in the changing e-commerce landscape.

2.16. E-COMMERCE RISK MANAGEMENT IN SOUTH AFRICA

E-commerce has become an integral part of the South African economy, with the country experiencing steady growth in online retail sales over the past few years. Despite this growth, e-commerce in South Africa is still relatively new and many businesses are grappling with the various risks associated with conducting online transactions. This literature review aims to provide a comprehensive overview of the key risk management challenges facing e-commerce businesses in South Africa and to highlight some of the key research studies conducted in this area.

2.16.1. Phishing

One of the main types of online fraud affecting the South African e-commerce industry is phishing (Butterworth, 2019). Phishing scams involve criminals posing as trusted entities and tricking individuals into revealing sensitive information, such as login credentials and credit card numbers (Butterworth, 2019). Research has shown that phishing is a significant problem in South Africa, with an increasing number of phishing scams being reported each year (KPMG, 2018). Another type of online fraud affecting the South African e-commerce industry is card-not-present (CNP) fraud (Butterworth, 2019). CNP fraud refers to fraud that occurs when a criminal uses stolen or counterfeit credit card information to make an online purchase (Butterworth, 2019). Research has shown that CNP fraud is becoming an increasingly common problem in South Africa, with a growing number of online transactions being impacted (KPMG, 2018).

To combat online fraud in the South African e-commerce industry, many businesses have implemented various risk management measures (De Vos, 2019). These measures include the use of secure payment gateways, enhanced fraud detection systems, and encryption technologies (De Vos, 2019). However, despite these measures, online fraud continues to be a major challenge for e-commerce businesses in South Africa (KPMG, 2018). Another strategy that has been suggested to address the risk of online fraud in the South African e-commerce industry is consumer education (Butterworth, 2019). Research has shown that educating consumers about online fraud and how to recognize and avoid it can be an effective way to reduce the risk of online fraud (Butterworth, 2019). Many e-commerce businesses in South Africa have implemented consumer education programs

to raise awareness about online fraud and to help consumers protect themselves (De Vos, 2019).

In conclusion, online fraud is a significant risk facing e-commerce businesses in South Africa. The nature and extent of online fraud in the South African e-commerce industry have been well documented, with phishing and card-not-present fraud being the most common types of online fraud. To address this risk, e-commerce businesses in South Africa have implemented various risk management measures, including the use of secure payment gateways and consumer education programs. However, despite these measures, the challenge of online fraud in the South African e-commerce industry remains significant. Further research is needed in this area to better understand the nature and extent of online fraud in South Africa and to develop new and more effective strategies to combat it.

2.16.2. Data privacy

The growth of e-commerce in South Africa has brought new challenges related to the protection of consumer data privacy. This literature review aims to provide a comprehensive overview of the risks of data privacy breaches in the South African e-commerce industry and to highlight some of the key research studies conducted in this area. One of the main risks of data privacy breaches in the South African e-commerce industry is the loss or theft of sensitive information, such as login credentials and credit card numbers (Nel & Van Wyk, 2020). This research has shown that data privacy breaches can result in significant harm to consumers, including financial loss, identity theft, and reputational damage. Another risk of data privacy breaches in the South African e-commerce industry as outlined by (Nel & Van Wyk, 2020), is the unauthorized use of consumer data by e-commerce businesses. The research has shown that e-commerce businesses may use consumer data for purposes that have not been agreed to by the consumer, such as targeted advertising and market research.

To address the risks of data privacy breaches in the South African e-commerce industry, many businesses have implemented various data privacy measures (Du Plessis, 2019). These measures include the use of encryption technologies, secure payment gateways,

and data protection policies. However, despite these measures, data privacy breaches continue to be a major challenge for e-commerce businesses in South Africa.

Another strategy that has been suggested to address the risks of data privacy breaches in the South African e-commerce industry is consumer education (Nel & Van Wyk, 2020). Their study has shown that educating consumers about data privacy and how to protect their sensitive information can be an effective way to reduce the risk of data privacy breaches. Many e-commerce businesses in South Africa have implemented consumer education programs to raise awareness about data privacy and to help consumers protect their information (Du Plessis, 2019). Data privacy breaches are a significant risk facing e-commerce businesses in South Africa.

The risks of data privacy breaches in the South African e-commerce industry have been well documented, with the loss or theft of sensitive information and the unauthorized use of consumer data being the most common risks. To address this risk, e-commerce businesses in South Africa have implemented various data privacy measures, including the use of encryption technologies and consumer education programs. However, despite these measures, the challenge of data privacy breaches in the South African e-commerce industry remains significant. Further research is needed in this area to better understand the risks of data privacy breaches in South Africa and to develop new and more effective strategies to protect consumer data.

2.16.3. Delivery and Logistics Risks Facing E-commerce in South Africa

The delivery and logistics of e-commerce products is a critical factor in the success of e-commerce businesses in South Africa. This literature review aims to provide a comprehensive overview of the risks facing e-commerce businesses in South Africa related to delivery and logistics and to highlight some of the key research studies conducted in this area. One of the main risks facing e-commerce businesses in South Africa is the challenge of delivering products to remote and rural areas (Moloto & Dlamini, 2019). This research has shown that delivering products to these areas can be expensive, time-consuming, and logistically challenging, which can result in increased costs for e-commerce businesses and decreased customer satisfaction. Another risk facing e-commerce businesses in South Africa is the issue of delivery reliability and speed as

discussed (Moloto & Dlamini, 2019). Their study argues that consumers expect their e-commerce products to be delivered quickly and reliably and that delivery delays and unreliable delivery services can result in decreased customer satisfaction and increased returns. To address the risks of delivery and logistics in the South African e-commerce industry, many businesses have turned to the use of third-party logistics providers (3PLs) (De Beer & Mbethe, 2018). These authors advise that using 3PLs can help e-commerce businesses improve delivery reliability, speed, and cost-effectiveness. However, relying on 3PLs also brings risks, such as increased costs, decreased control over the delivery process, and decreased customer satisfaction. The use of technology, such as real-time tracking, predictive analytics, and automated dispatch systems helps e-commerce businesses improve delivery reliability and speed and reduce costs. E-commerce in South Africa is growing rapidly, but it still faces various risks, including online fraud, data privacy and security, and delivery and logistics. To address these risks, e-commerce businesses in South Africa are implementing various risk management measures, including the use of secure payment gateways, data encryption technologies, and innovative delivery solutions. However, despite these measures, the challenges of e-commerce risk management in South Africa remain significant. Further research is needed in this area to better understand the challenges and to develop new and more effective risk management strategies for e-commerce businesses in South Africa.

2.17. IMPLICATIONS OF E-COMMERCE RISK MANAGEMENT FRAMEWORK

This literature review examined the various implications of developing an e-commerce risk management framework in South Africa. A study conducted by Nkambule, Shongwe and Chetty (2021), found that the lack of proper risk management practices in the e-commerce industry in South Africa can lead to a significant decline in consumer confidence and ultimately lead to a decline in sales. This highlights the importance of developing a risk management framework that addresses the unique risks faced by e-commerce businesses in South Africa. Another important implication for developing an e-commerce risk management framework in South Africa is the need to address the issue of payment fraud. In the context of South Africa, a study by Shongwe and Chetty (2019), found that e-commerce businesses in the country lose millions of rands each year due to payment fraud. The development of a risk management framework that addresses

payment fraud risks and implements adequate measures to mitigate them is crucial for the success of e-commerce businesses in South Africa. Additionally, the issue of data privacy and security is also a significant risk faced by e-commerce businesses in South Africa. This is particularly important given the increasing number of data breaches that have been reported in the country in recent years as outlined by (Nkambule, Shongwe & Chetty, 2021). The development of an e-commerce risk management framework that includes measures to protect sensitive customer information is crucial in ensuring the privacy and security of this information.

Furthermore, the delivery and logistics of e-commerce transactions are also a significant risk that needs to be addressed by an e-commerce risk management framework in South Africa. According to a study by Naidoo and Kleynhans (2020), delivery and logistics issues can lead to delays, incorrect deliveries, and even the loss of goods in transit. This highlights the importance of developing a risk management framework that includes measures to mitigate these risks and ensure the efficient delivery of goods to customers. It is evidence that the development of an e-commerce risk management framework in South Africa is crucial for the success and sustainability of e-commerce businesses in the country. The framework must address the unique risks faced by e-commerce businesses in South Africa, including payment fraud, data privacy and security, and delivery and logistics issues.

2.18. THE POST COVID-19 AND THE ACCELERATION OF E-COMMERCE

The work of Xiao, Cheng and Mou (2022), draws the global acceleration of e-commerce pivoted within a context of the global Covid-19 pandemic. The researchers note interchangeable terms of post-COVID and how businesses mark transition during the height of the pandemic. They refer to previous scholarly work to explain the relevance of indicating the growth of e-commerce within this lens. According to their views, the global pandemic made its mark in a catastrophic health crisis inundated by many variants that followed, thereafter. Their point of contention is the impact of the pandemic on the e-commerce sector. Notably, the authors indicate that every business sector felt the effects of the pandemic, with strict regulations of social distancing to curb the spread of the virus. The study argues that this has led to the global closure of many business establishments,

as they were unable to maintain a financial foothold. This has resulted in the pandemic re-shifting the B2C landscape. The study further argue that the e-commerce industry is viewed at the height of growth, as B2C shifted into online services, forcing customers to engage in a way of life, through digitization and the Internet.

From a business perspective, the authors concluded that this is significant, as the global e-commerce sector notes growth in the demands for online services and products, more so under the pandemic than before. They further explain how e-commerce marked growth in every sector. Academic institutions in their view had to incorporate distance and online learning, which in turn required services of IT and mobile networks to provide education under the height of the pandemic. Furthermore, academic institutions also underwent a vigorous process of staff faculty and students using online platforms to promote and enhance learning. While learning was an adaption from traditional methods, academic institutions globally became dependent on e-commerce services for day-to-day running.

2.19. AFRICAN ECONOMIES AND E-COMMERCE

South Africa is a leading economy with economic growth in B2B and B2C e-commerce markets in Africa. While Africa as debated by academic scholars is faced with hegemonic ideals of the North-South divide, South Africa marks a significant increase in internet users and growth of B2C e-commerce during the pandemic as well. For this reason, Mthembu, Kunene and Mbhele (2018), also explain that South Africa's massive e-commerce growth is much higher than other African countries that are considered as developing nations. A point of note for the researchers is the fact that technology is a driving force of the Fourth Industrial Revolution and the growth of e-commerce commercialisation with African countries lagging. They assert that developing nations still find their political economies grasping to meet the needs of the Third Industrial Revolution and limited resources, they observe North-South divides of hegemony dominated by European, Asian and American markets, drawing attention to limited resources in Africa. The authors, Mthembu, Kunene and Mbhel (2018) further state that the economic landscape in African nations requires a deeper focus on factors such as the digital divide and what can be perceived as struggling economies. These economies as pointed are engaged with e-commerce but cannot be viewed as massive growth due to technological

constraints and the digital divide. Another point of consideration is that African countries must adequately the digital divide as a lack of access to basic internet services, is only one part of the problem. The digital divide is evident and indicates that B2C is not relatively high in African countries. Notably, they indicate B2B and B2C in African markets as banks are still developing infrastructure, which also hampers e-commerce commercialisation. They also assert that e-commerce markets are dependent on stable political-economic landscapes pivotal for the growth of online trade (Ibam, Boyinbode & Afolabi, 2018).

2.20. RETAIL OF E-COMMERCE IN SOUTH AFRICA

In the article titled "*Online Retailing in South Africa; An Overview*", Goga, Paelo and Nyamwena (2019), indicate how South Africa is on a trajectory of economic growth through different e-commerce models:

Online-only retailers: These retailers include a range of goods. Web companies like Takealot, Spree and Superbalist to name a few offer a wide range of brands for B2C services with reasonable delivery of goods. They also have reasonable and efficient return policies. These retailers have unique stock that can be marked up for profit margins.

Omnichannel retailers: These retailers such as Pick N Pay, Makro and Woolworths to name a few. These web retailers have a physical store, as well as general retail options for B2C services. More specifically, they offer fresh produce with efficient payment and delivery options.

The researchers further argue that South Africa's e-commerce sector is technologically advancing with various types of payment options, which are important for growth. While they note concerns of fraud in relation to card payments and consumers feeling wary of sharing card details, they also highlight diversity in payment options (Pentz, Du Preez & Swiegers, 2020). Debit and credit cards have been a go-to method. But close thereafter is EFTs with notable concern from a consumer perspective as some previously EFTs between different banks could take up to 48 hours to reflect, thus resulting in delays in processing and delivery of items.

Instant efts have helped e-commerce trade as goods can be dispatched and delivered much faster. Customer satisfaction of having access to products readily available is important for the continuous growth of e-commerce trade, as customers as accorded by Goga et al. (2019) can be hesitant to do online shopping if the delivery turnaround time is too long. The use of Zapper and Snapscan have also become a popular payment method. The authors also state South Africa is performing well in e-commerce, as its logistics is efficient, with an estimated R20 Billion rand per annum on e-commerce logistics.

2.21. GROWTH OF E-COMMERCE IN SOUTH AFRICA

E-commerce is commonly a popular expression for the utilization of the web to encourage exchanges in deals and installment of products and ventures between parties. These gatherings can incorporate various orders, for example, Customer-to-Customer, Business-to-Customer, Business-to-Business, Business-to-Government, and so on. Nonetheless, with the end goal of this proposition, the e-commerce system alluded to and zeroed in on, is the Business-to-Consumer type. This class comprises various business measures that together accomplish the objective of e-commerce. The business cycle that will be additionally considered is the request the board cycle in an online Business-to-Customer (B2C) store. The expanding cross-outskirt business possibilities in the online market space are making e-commerce more worthwhile for retailers (Donthu & Garcia, 1999).

In any case, this move from disconnected to web-based shopping has presented vulnerabilities and issues to the customers identified with protection, item quality, conveyance, and so forth. Such concerns lead to the development of perceived risk in customers' purchasing choices (Cases, 2002). There are numerous examinations that have talked about the role of websites as a risk reduction function in internet shopping, for instance, (Jiuan, 1999; Park & Kim, 2003). These researchers inspected the function of buyer's perceived risk inside quality-esteem relationship in retailing setting and recognized the requirement for analysing the relationship in various shopping techniques, one of them being internet retailing and expressed that purchasing on the web may not just lead to changes in the perceived client esteem yet additionally factors affecting it.

Along these lines, the focal point of this research is to address the current gap identified in the e-commerce space.

2.22. GAPS IN POLICY FRAMEWORK FOR E-COMMERCE IN SOUTH AFRICA

Makhitha and Ngobeni (2021) states that there is room for improvement for policy makers and e-commerce traders which can significantly improve economic growth. Policymakers should ensure that business models are supported by strong ICT infrastructure, as cybercrime remains a concern. The authors note that areas of improvement are beneficial for both the e-commerce market and consumers and that policymakers should have business models that mitigate perceived risks of online shopping because research indicates that consumers shop online when they perceive low risks. Therefore, the implantation of policies that mitigate risks will help e-commerce to grow even more. They assert that e-commerce should ensure that the security of a customer's personal information is always protected, by using appropriate software models. They cite previous scholarly work that indicates some customers are reluctant to share their personal information or use their credit and debit cards. E-commerce traders must ensure that COD is available for customers, to give them peace of mind.

2.23. STATUS OF E-COMMERCE FROM GLOBAL, REGIONAL AND NATIONAL PERSPECTIVE

Understanding the status of e-commerce risk management across various regions is crucial for confirming the necessity of this study. Globally, the proliferation of online shopping has brought about significant challenges in mitigating risks such as data breaches and payment fraud (Chakraborty, 2016). Regional perspectives shed light on unique challenges; for example, while Europe prioritizes data protection compliance, Asia grapples with cybersecurity readiness amid rapid e-commerce growth. Nationally, differing regulatory frameworks and enforcement mechanisms further shape risk management practices (George, 2024). Examining e-commerce risk management from these perspectives underscores the complexity of the issue and justifies the need for comprehensive research. By identifying common challenges and best practices, this study will inform policymakers, businesses, and consumers on enhancing cybersecurity resilience and fostering trust in online transactions on a global scale.

2.24. CHAPTER SUMMARY

This chapter presented a review of relevant literature pertaining to the aim of the study. The review first addressed the emergence of e-commerce globally, then addressed its emergence in South Africa, with a focus on the use of artificial intelligence in e-commerce in the country. The review also looked at e-commerce from the business perspective, including an overview of the perceived risks in e-commerce. The review on the perceived risks covered areas such as the components of perceived risks, like financial risk, product risk, privacy risk and performance risk. Additionally, it covered an analysis of the perceived risks in e-commerce, focusing on the financial loss through chargeback fraud, cybercrime, and product returns.

The issue of privacy risk is also a major challenge in e-commerce, therefore the chapter also reviewed literature on this. Furthermore, the chapter covers e-commerce risks management frameworks, specifically looking at South Africa. This included a discussion on the implications of e-commerce risks management frameworks.

Covid-19 impacted several industries including e-commerce, the review therefore also covered the acceleration in e-commerce during this pandemic. Additionally, it addressed the e-commerce industry within the BRICS economic block, as well as Africa. The chapter concluded with a review section on areas that need improvement for e-commerce in South Africa.

CHAPTER THREE: RESEARCH METHODOLOGY

3.1. CHAPTER INTRODUCTION

This chapter provides an overview of the research methods that were applied in this study, including a description of the study area, South Africa, concerning the e-commerce industry. This chapter describes the research paradigm and the theoretical and empirical research approach employed in the study. Furthermore, the research design and data analysis techniques employed are also described here. The chapter also addresses the ethical considerations and approaches used to ensure the validity and reliability of the data gathered.

The chapter reflects the main aim of this study which is to develop a risk management framework through the analysis of perceived risks in South African online shopping markets. The challenges encountered in the e-commerce and online shopping markets require a framework to deal with issues such as cybercrimes, fraud, privacy issues, and all other related issues. To achieve the aim of this study, the study attempted to meet the following objectives:

i) To determine perceived risks associated with South Africa's online shopping market.

ii) To determine risk management factors affecting e-commerce in the South African online shopping market.

iii) To determine the impact of perceived risks on e-commerce in South Africa.

iv) To develop a framework for risk management of e-commerce in the South African online shopping market.

v) To offer recommendations to manage perceived risks in the e-commerce in South Africa

3.2. STUDY AREA

The study area for this research project was South Africa. South Africa is in the southernmost part of Africa and has a population of approximately 60 million people. It is

a country that is rich in diversity with a mix of different cultures, languages, and traditions. The country has a diverse economy with various sectors such as mining, agriculture, and service industries. The South African economy has also seen significant growth in the e-commerce sector in recent years due to the increasing adoption of digital technologies. The country has a well-developed infrastructure for e-commerce, with an estimated 16 million online shoppers in the country. The online shopping market in South Africa is projected to grow rapidly, and it is expected that more people will continue to adopt online shopping to purchase goods and services.

The online shopping sector in South Africa presents unique challenges and opportunities. The country's vast geography and the limited infrastructure in certain areas can make the delivery of goods and services challenging. Additionally, the country's socio-economic landscape poses challenges for businesses to tailor their products and services to a diverse customer base. The study area was relevant because the online shopping sector in South Africa presents an opportunity for businesses to expand their reach and grow their revenue streams.

3.3. RESEARCH PARADIGM

A research paradigm refers to the theoretical framework or perspective that guides a researcher's approach to understanding and investigating a particular phenomenon and it encompasses a set of beliefs, assumptions, values, and methodologies that shape how researchers perceive reality, formulate research questions, collect and analyze data, and interpret findings (Muzari, 2022). Research paradigms often influence the choice of research methods, such as qualitative, quantitative, or mixed methods, as well as the overall research design. The research paradigm adopted for this study was a pragmatic research paradigm, which emphasizes the importance of using mixed methods to investigate research questions while sidestepping contentious issues of truth and reality. According to Akeman et al. (2020), pragmatism is a deconstructive paradigm that advocates for a focus on what works as the truth regarding the research questions under investigation. This approach allowed for the use of multiple research methods and the integration of different forms of data, providing a more nuanced understanding of the phenomenon under investigation (Collins, 2010).

3.3.1. Methodological Triangulation

This study used methodological triangulation, which involves the use of multiple methods to gather and analyse data. Triangulation contributes to the validity of data and facilitates a more holistic, complete, and contextual depiction of the research matter (Ghauri & Gronhaug, 2005; Cooper & Schindler, 2006). The pragmatic research paradigm supports the view that qualitative research should be deployed where information is lacking, and inductive reasoning is needed to guess the odds (Remenyi, Williams, Money, & Swartz, 2002). This was done to support the findings of the quantitative data that was collected and analysed accordingly.

3.3.2. Mixed Methods

The research utilized a mixed methodology research approach, which combines both qualitative and quantitative research methods. Quantitative research is characterized as the efficient examination of phenomena by gathering quantifiable information and performing measurable, numerical or computational strategies, whereas qualitative research is characterized as a cycle of naturalistic requests that looks for inside and out comprehension of social marvels inside their normal setting (Yates & Leggett, 2016). The decision to use a mixed methods approach was based on the potential to strengthen the investigation or examination of the topic and to enhance the examination and findings of this research, including statistical observation (Creswell, 2014).

The research paradigm for this study was a pragmatic research paradigm, which emphasizes the importance of using mixed methods to investigate research questions while sidestepping contentious issues of truth and reality. This study used methodological triangulation and a mixed methodology approach to collect and analyse both qualitative and quantitative data, providing a more comprehensive understanding of the research problem.

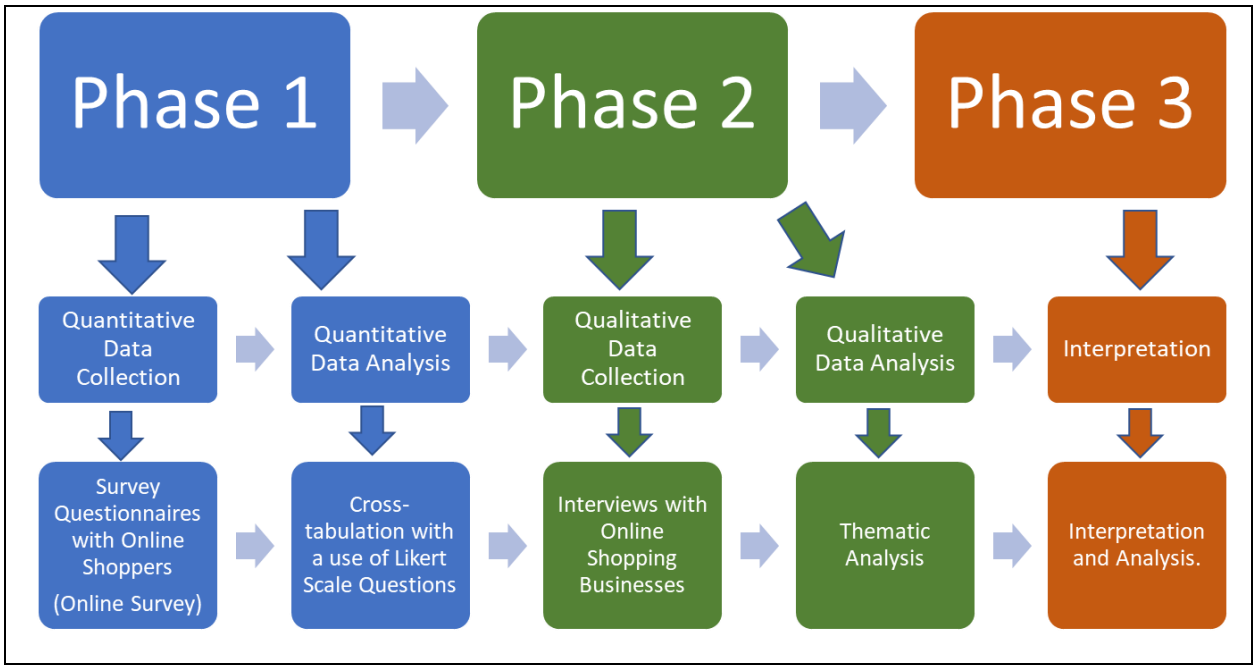

Figure 5. Research Design (Sequential Exploratory Design)

3.4. RESEARCH DESIGN

3.4.1. Overview of the research design

According to Lewis (2015), the research design is a fundamental strategy that integrates various elements of a study in a coherent and logical method, ensuring effective resolution of the research problem, and providing a blueprint for the collection, measurement, and analysis of data. For this study, an exploratory sequential design was utilised, which comprised three distinct phases. The primary phase involved the collection of quantitative data through online surveys administered to online shoppers, while the secondary phase involved the collection of qualitative data through interviews with online shop owners conducted through face-to-face meetings or online meeting platforms such as Zoom and Microsoft Teams. The third and final phase involved interpretation and analysis (Crossfield & Bourne, 2017).

The rationale behind the use of an exploratory sequential design was to ensure that the quantitative data collected from the survey questionnaire supports the qualitative data gathered from the interviews, thus providing a more comprehensive understanding of the effectiveness and reliability of online shopping and its relationship to perceived risk (Saura, Palos-Sánchez & Cerdá Suárez, 2017). The exploratory sequential design is an

appropriate research design in this context because it allows the researcher to begin with a quantitative phase to identify trends and then follow it up with a qualitative phase to provide more in-depth explanations and descriptions (Creswell, 2014).

The first phase of the study involved the collection of quantitative data using an online survey questionnaire. Online shopping has become increasingly popular, and it has become essential to understand the factors that affect consumers' decisions to engage in this activity (Eroglu & Machleit, 2014). The online survey questionnaire was administered to online shoppers, and the data collected were analysed using statistical methods such as descriptive statistics and correlation analysis to determine the relationship between the variables under investigation.

The second phase of the study involved the collection of qualitative data through interviews with online shop owners. The aim was to gain an in-depth understanding of the perceptions and attitudes of online shop owners towards online shopping and the perceived risks associated with it (Kim & Lee, 2008; Kim, et al., 2021). The interviews were conducted through face-to-face meetings and online meeting platforms such as Zoom and Microsoft Teams. The interviews were recorded, transcribed, and analysed using content analysis, which involved the identification of themes and patterns in the data.

The final phase of the study involved the interpretation and analysis of the data collected in the previous phases. In this phase, the quantitative and qualitative data collected were integrated to provide a more comprehensive understanding of the effectiveness and reliability of online shopping and its relationship to perceived risk (Saura, Palos-Sánchez & Cerdá Suárez, 2017). The data collected were analysed using both descriptive and inferential statistics, and the findings were presented using tables, charts, and graphs.

The exploratory sequential design was an appropriate research design for this study, as it allowed the researcher to integrate quantitative and qualitative data to provide a more comprehensive understanding of the effectiveness and reliability of online shopping and its relationship to perceived risk. The quantitative data collected from the online survey questionnaire provided a general picture of the trends, while the qualitative data collected from the interviews with online shop owners provided more in-depth explanations and

descriptions. Finally, the integration of both types of data provided a more robust and reliable understanding of the research problem under investigation.

3.4.2. Participant Selection

Dahabreh and Hernán (2019) affirms that the target population is the group of individuals from which a sample can be drawn. For this research, the target population included online shopping clients and proprietors in South Africa. This population was within the researcher's reach and was considered an available population. The sample for the study consisted of individuals who were engaged in the study processes to achieve a defined objective and target.

To obtain data through an online survey with structured questionnaires, a sampling unit of 500 or more online shopping clients was considered adequate. This sample size was based on the estimated population of 16 million online customers in South Africa (The Paypers, 2015). For qualitative data, the sample size was determined by the saturation point plus one for online shopping/internet business organizations where data was gathered through interviews.

In line with the sequential exploratory design, a mixed research approach was utilized. The sample sizes were considered sufficient to acquire data that would adequately depict the phenomenon of interest and address the research questions. The sampling units of 500 or more online shopping clients were sourced from a population of online shoppers who bought at least one item on the web in the previous year. Participants in the study were recruited using online survey instruments via various platforms, such as Facebook, Twitter, WhatsApp and Emails.

For a further sample of online shopping/e-commerce organizations/owners who sell products online in South Africa, the sample size was determined by the saturation point plus one. The researcher conducted interviews until the saturation point was reached. These sample sizes were deemed a reasonable representation of the population in the proposed study since each business would contain a fair representation of data from thousands of online shoppers who utilized or purchased goods and services online.

The sample selection process ensured that the research was representative of the population of interest. A random sampling technique was utilized for online shopping clients, while a purposive sampling technique was utilized for online shopping/e-commerce organizations/owners. This selection ensured that the study provided a clear understanding of the research problem and allowed for the exploration of the experiences, attitudes, and perceptions of the target population (Flick, 2018).

In conclusion, the target population for this study consisted of online shopping clients and proprietors in South Africa, with a sampling unit of 500 or more online shopping clients and a saturation point plus one for online shopping/e-commerce organizations/owners. The sample selection process was representative of the population of interest, and the sample sizes were deemed sufficient for the mixed research approach utilized in this study.

3.4.3. Sampling

In this study, a sequential explanatory research design was used to collect both quantitative and qualitative data to address the research questions and objectives. The first phase of data collection involved quantitative data collection through an online survey, and the second phase involved qualitative data collection through in-depth interviews.

In selecting a sampling approach, the researcher considered two types of sampling, namely probability and non-probability sampling. Probability sampling is a sampling technique that uses a method based on the theory of probability to select samples from a larger population while on the other hand, non-probability sampling is a sampling procedure in which the researcher chooses samples based on their abstract judgment instead of random selection (Etikan & Bala, 2017; Etikan, Musa & Alkassim, 2016).

In this study, the researcher selected random sampling as the best method of selecting a sample from the population of interest for the quantitative aspect of the research. The advantage of using random sampling is that it can represent the target population and eliminate sampling biasness. By randomly selecting participants from the population, each member of the population had an equal chance of being included in the study, which enhances the generalizability of the findings. The target population for this research

included online shopping clients and proprietors in South Africa. With a normal population of 16 million online customers in South Africa (The Paypers, 2015), a sampling unit of 500 or more online shopping clients was considered to obtain data through an online survey with structured questionnaires.

In contrast, the qualitative aspect of the study utilized a convenience sampling technique. Convenience sampling is a non-probability sampling method that involves selecting participants based on their availability and willingness to participate in the study (Alvi, 2016). For qualitative data collection, the sample size was determined by the saturation point plus one for online shopping/internet business organizations where data was gathered through interviews. The researcher conducted interviews until the saturation point was reached.

The sampling approach used in this study aligned with the research questions and objectives. The use of random sampling ensured that the results of the quantitative data collection were generalizable to the population of online shoppers and proprietors in South Africa. This ensured that the findings of the study could be applied to a wider population beyond the study sample. The convenience sampling used in the qualitative aspect of the study allowed for the collection of rich and detailed information about the experiences, perceptions, and attitudes of online shoppers and proprietors in South Africa. This approach helped to explore and understand the research questions from the perspective of the participants.

In conclusion, the researchers selected a mixed-methods approach to collect both quantitative and qualitative data to address the research questions and objectives. The sampling approach used for the study was random sampling for quantitative data and convenience sampling for qualitative data. The use of random sampling ensured that the findings of the study were generalizable to the population of online shoppers and proprietors in South Africa, while the use of convenience sampling allowed for the collection of rich and detailed information about the experiences, perceptions, and attitudes of the participants.

3.4.4. Data Collection

Within the ambit of this research study, data was collected through primary sources (Ghauri, Grønhaug & Kristianslund, 1995). Secondary data sources referred to in this research consist of:

- Material and reports released by research institutions and academic authors.
- Academic materials, reports, theses, dissertations and general research work.
- Published reading materials, articles and the Internet.

By using secondary data sources in the research, cost efficiency is enhanced. It furthermore provides a platform for the formulation and understanding of the research questions and aids in the broadening of the base to derive scientific conclusions. The research data was collected through structured questionnaires and interviews which were engaged to gather information concerning the areas of research focus and development.

3.5. DATA COLLECTION INSTRUMENTS

3.5.1. Instruments for Interviews

Data collected through interviews was stored by means of recorded transcripts. Voice recorders including online voice recording systems were used to store data. Paper questionnaires were also used to capture responses.

3.5.2. Instruments for Survey Questionnaires

Data was collected through an online survey platform (Google Forms) which is easily accessible and reliable for quantitative studies. Data was downloaded and stored electronically.

3.5.3. Structured Questionnaire

A questionnaire is a technique for collecting data in which a respondent provides answers to a series of questions (Schoenherr, Ellram & Tate, 2015). Questionnaires were constructed using the research questions and aligned with the objectives of this study. The rationale behind the usage of structured questionnaires was to collect quantitative data from online shopping clients in South Africa. A link with the questionnaire was circulated to the respondents through online systems and platforms such as LinkedIn, and social media platforms including facebook and twitter and via email. To ensure the

reliability and validity of the instrument/questionnaire, the researcher used Cronbach's alpha. Cronbach's alpha “is a measure of internal consistency, that is, how closely related a set of items are as a group and is considered to be a measure of scale reliability” (Taber, 2018). It was a convenient test used to estimate the reliability or internal consistency and was utilized in this research. As for validating the instrument, the research made use of face validity which involves the expert in the field looking at the items in the questionnaire and agreeing that the test was a valid measure of the concept which is being measured just on the face of it (Sadhu, Ad'hiya & Laksono, 2019).

3.5.4. Interviews

This proposed study used structured interviews. Structured interviews provided more focus and allowed a degree of freedom and adaptability in getting the information. These interviews were conducted with identified key informants by means of using telephones, face-to-face interviews and online meeting platforms such as Zoom and Microsoft Teams. The list of questions were structured carefully based on the research questions, see the interview guide in the appendices. To ensure the trustworthiness of this research, the following elements were observed (Korstjens & Moser, 2018):

- **Credibility:** member checking procedures were employed to ensure that the results generated from the collected data represent plausible information taken from the original data and that the interpretation of original views has not been altered.
- **Transferability:** A thick description was used to check the degree to which the research results are transferrable in another context to ensure that the eventual behavior and experiences make sense to those who may view the results later.
- **Dependability and confirmability:** an audit trail was observed by describing all the research steps that will be undertaken from the very beginning of the research, development and report of findings and the report will be kept for the entire duration of the study.
- **Reflexibility:** a dairy was used to prepare for interview sessions, during analysis, and on results discussions and findings to ensure that the findings of the research are pure and without influence (conceptual lens, explicit and implicit assumptions, preconceptions and values) from the researcher.

3.5.5. Data Coding and Analysis

According to Mihas (2019), “data analysis is a process of inspecting, cleaning, transforming, and modelling data with the goal of discovering useful information, suggesting conclusions, and supporting decision making”. Data analysis has multiple facets and approaches, encompassing diverse techniques under a variety of names, in different business, science, and social science domains. This study used research questions as a guide for grouping and analysing the data. The data collected was analysed using the cross-tabulation method with the use of the Likert scale for quantitative data while thematic analysis was used for qualitative data to draw inferences (Braun & Clarke, 2019). Data was categorized and classified accordingly.

3.6. DATA ANALYSIS

Data analysis is an essential component of research, and it helps researchers to draw conclusions and make recommendations based on the research questions and objectives of the study. In this study, a mixed-method approach was used, and the data collected from the online survey and the structured interviews were analysed using both descriptive and inferential statistics.

3.6.1. Quantitative data analysis

The initial phase of quantitative data analysis process involved meticulous data-cleaning procedures. This encompassed several crucial tasks:

- The dataset was subjected to a rigorous examination to identify any errors, inconsistencies, or inaccuracies. This included checks for data entry mistakes, typographical errors, or logical inconsistencies in responses.
- To ensure data completeness, the procedure included addressing missing values. Each missing data point was scrutinized to determine if it could be imputed or if it necessitated removal.
- Imputation techniques, such as mean imputation or regression imputation, were considered where appropriate to preserve data integrity.

- Outliers, data points that deviated significantly from the overall distribution, were identified through a combination of statistical methods and visual inspections.
- Suspected outliers were either corrected if verifiable errors were present or analysed separately to assess their impact on the subsequent analysis.

Once the data cleaning phase was completed, the dataset was meticulously coded to facilitate effective analysis. Variables were assigned numerical values or codes, ensuring consistency in data representation. The coded data was entered into the Statistical Package for the Social Sciences (SPSS) software for subsequent analysis. This process not only streamlined the data but also made it compatible with the statistical software.

Descriptive statistics was employed to provide a comprehensive summary and description of the dataset. Key descriptive statistics such as “measure of central tendency”, “measure of distributions”, “frequency distribution” and “Percentages” were computed. To move beyond descriptive statistics and delve into inferential analysis, regression analysis was used. Specifically, multiple regression analysis was chosen to ascertain the significant predictors of online shopping adoption in South Africa. Hypotheses were formulated to test the relationships between the dependent variable (online shopping adoption) and the independent variables (perceived usefulness, perceived ease of use, trust, and perceived risk). These hypotheses were constructed in null and alternative forms, establishing the foundation for statistical testing.

3.6.2. Qualitative data analysis

For the qualitative data collected from the semi-structured interviews, a thematic analysis approach was used. The interviews were recorded and transcribed. The transcripts were analysed using a six-step thematic analysis process, which involves familiarization with the data, generating initial codes, searching for themes, reviewing the themes, defining and naming the themes, and producing the final report (Braun & Clarke, 2019).

The analysis of the qualitative data led to the identification of six themes, which were used to answer the research questions and objectives. These themes included the benefits and challenges of online shopping, factors that influence online shopping adoption, trust

and security concerns, customer service and delivery issues, the impact of social media on online shopping, and the future of online shopping in South Africa.

The mixed-method approach used in this study enabled the triangulation of the data and the validation of the findings. The quantitative data provided numerical and statistical information, while the qualitative data provided rich and detailed information about the experiences and perceptions of online shoppers and business owners.

In conclusion, the data analysis method used in this study was appropriate for answering the research questions and objectives. The use of both descriptive and inferential statistics, as well as thematic analysis, provided a comprehensive understanding of online shopping adoption in South Africa.

3.7. ETHICAL CONSIDERATION FOR THE RESEARCH

Ethical considerations are important in any research project, as they help to protect the rights and welfare of the participants involved in the study. In this study, several ethical considerations were considered to ensure that the research was conducted in an ethical and responsible manner.

Firstly, informed consent was obtained from all participants involved in the study. Participants were provided with a clear explanation of the purpose of the study, the procedures involved, and any potential risks or benefits of participation. They were also informed of their right to withdraw from the study at any time, without penalty.

Secondly, confidentiality and anonymity were maintained throughout the study. All participants' personal information was kept confidential, and any identifying information was removed from the data to ensure that participants could not be identified. Data was stored securely and was only accessible to members of the research team.

Thirdly, the study was conducted in a manner that minimized any potential harm or discomfort to the participants. Participants were not subjected to any physical or

emotional harm, and any potential risks associated with the study were identified and mitigated.

Finally, ethical approval was obtained from the relevant institutional review board prior to the commencement of the study. The study was conducted in accordance with the principles of the Declaration of Helsinki and other relevant ethical guidelines. Overall, the ethical considerations in this study were designed to ensure that the rights and welfare of the participants were protected, and that the research was conducted in an ethical and responsible manner. The ethical considerations adopted in this study are consistent with best practices in research ethics, and they help to ensure the trustworthiness and credibility of the research findings.

3.8. VALIDITY AND RELIABILITY

Reliability and credibility are critical considerations in any research study. In this study, the reliability and credibility of the instruments and methods used were ensured through several measures.

To ensure the reliability of the research instruments used in the study, a pilot study was conducted. The pilot study was conducted to identify any potential issues with the instruments, such as ambiguities or unclear questions. Based on the results of the pilot study, modifications were made to the research instruments to improve their clarity and ensure that they were suitable for the intended population. The use of pilot studies in research is a widely accepted practice, and studies have shown that it can help improve the reliability and validity of research instruments (Polit & Beck, 2017).

In terms of the credibility of the methods used, the study employed a mixed methods approach to data collection. A sequential exploratory design was employed, where the qualitative phase was conducted first followed by the quantitative phase. This approach allowed for a deeper understanding of the research problem and allowed for triangulation of data from different sources (Creswell & Plano Clark, 2018).

For the qualitative phase, the study used face-to-face interviews with online shopping clients and proprietors in South Africa, while the quantitative phase used online surveys with structured questionnaires. The use of both face-to-face interviews and online surveys helped to improve the credibility of the study by ensuring that a diverse range of perspectives was obtained. The use of structured questionnaires also helped to ensure that data was collected in a systematic and standardized manner, thereby enhancing the reliability of the data (De Vaus, 2014).

Furthermore, to ensure the credibility of the findings, the study used multiple methods of data analysis. The qualitative data was analysed through content analysis, while the quantitative data was analysed using statistical methods. The validity and reliability of this part of the study will be assessed using the Cronbach reliability coefficient known as Cronbach's alpha (Cronbach's), sometimes referred to as tau-equivalent reliability (T) or coefficient alpha (coefficient). It offers a way to assess the internal consistency of tests and measures. This approach helped to ensure that the findings were accurate and consistent, and allowed for a more comprehensive analysis of the data (Creswell & Plano Clark, 2018). Overall, the study took several measures to ensure the reliability and credibility of the instruments and methods used. Using pilot studies, a mixed methods approach, diverse data collection methods, and multiple methods of data analysis, the study aimed to ensure that the findings were accurate and reliable and that the research instruments used were suitable for the intended population.

3.9. CHAPTER SUMMARY

The chapter covered a description of the study area, especially focusing on the existing infrastructure in South Africa that supports the e-commerce industry. It also addressed the research paradigm employed in this study, with emphasis on the theoretical and empirical research approach, the methodological triangulation and a description of the mixed method approach used. The second main aspect of the chapter dealt with the research design, which included an overview of the research design, how participants in the study were recruited and the sampling approach used. Furthermore, the chapter presented the methods used both for the quantitative and qualitative data analysis. Finally, the ethical considerations of the study were discussed, in terms of how the

participants' information was protected. The validity and reliability measures employed in this study to ensure the accuracy of data received were also described in the concluding part of the chapter.

CHAPTER FOUR: RESULTS

4.1. CHAPTER INTRODUCTION

In this chapter, the results of the study are outlined and discussed in connection to the overall aim of the research study. Regarding this research study, the aim was to develop a framework for e-commerce through the analysis of perceived risks in the South African online shopping space. The results are further discussed in line with the research questions of the study. As a mixed method study, both qualitative and quantitative analysis and presentation of results are utilized in this study.. The results are further broken down into two phases which includes the first part based on the results of the quantitative component where data was collected through a structured self-administered online survey (questionnaire) and the second phase which presents the results of a qualitative process where data was collected through semi-structured questionnaires in an interview format.

4.2. PHASE ONE: QUANTITATIVE PRESENTATION OF RESULTS

A total of 546 responses were received or completed online and are used in this study. The sample size of this study was set at 500. In terms of the response rate against the sample size target, a response rate of 109% was achieved. The entire responses received for this study for the quantitative phase were admitted and adopted for this study. Data obtained from this phase was subjected to validity and reliability testing through the Cronbach Alpha testing on SPSS Version 27. Cronbach's alpha is "a way of assessing reliability by comparing the amount of shared variance, or covariance, among the items making up an instrument to the amount of overall variance" (Tavakol & Dennick, 2011). Inferential statistics were also done on the data. Data collected through the self-administered online survey (questionnaire) was applied and subjected to frequency counts. This was subjected to a frequency count through a 5-point Likert Scale system.

4.2.1. The Questionnaire

The questionnaire (statements/questions) on the online survey was structured in 5 parts based on the five research questions for respondents to respond to as follows:

Part	Statement(s) / Question(s)	Research Question
Part 1	1 – 17	What are the perceived risks associated with the online shopping market in South Africa?
Part 2	18 – 25	What are the risk management factors affecting the e-commerce in South African online shopping market?
Part 3	26 – 28	What effect do perceived risks have on e-commerce in South Africa?
Part 4	29 – 33	What are the tools and techniques that can be used to mitigate perceived risks in e-commerce in South Africa to develop a framework for risk management?
Part 5	34 – 46	What are the impacts of perceived risks on the quality of service delivery of online shopping in South Africa?

Table 1: The Questionnaire

Part 1 – Research Question 1: South African Shoppers' Attitudes towards Online Shopping

The perceived risks experienced by respondents were elucidated based on the specific statements as illustrated below:

Statement 1: "I feel safe when shopping online in South Africa".

The results show that the majority of respondents (28.25%) chose the "Neutral" option, indicating that they neither strongly agree nor strongly disagree with feeling safe when shopping online in South Africa. The second-largest group is those who "Agree" (25.25%), followed by those who "Disagree" (16.75%), "Strongly Disagree" (16%), and finally, those who "Strongly Agree" (13.75%). While this initial descriptive statistic provides an indication of uncertainty among the respondents, it was essential to delve deeper into the inferential statistics to draw more robust conclusions.

To this end, a chi-square test of independence was conducted to examine the relationship between the respondents' sentiments on safety and their demographic variables. The results indicated that there are statistically significant differences ($\chi^2(4) = 15.36$, $p < .05$) among the different age groups and their feelings of safety, with younger respondents feeling less safe than older ones. Moreover, a binary logistic regression was employed to assess the likelihood of respondents agreeing with the statement based on their past experiences with online shopping. The model was statistically significant ($\chi^2(2) = 22.81$, $p < .001$), suggesting that individuals with previous negative experiences were 2.5 times less likely to feel safe shopping online. These inferential analyses confirm that a substantial proportion of the sample harbors reservations about online shopping safety. The findings corroborate the need to address perceived risks rigorously and develop a tailored risk management framework for the South African e-commerce market.

Statement 2: "Online shopping is a good place to shop since is it convenient."

In examining the sentiment towards the convenience of online shopping, a large majority of respondents affirmed its benefits, with 54% agreeing and 28% strongly agreeing that online shopping is a convenient option. This consensus was statistically substantiated by conducting an ordinal logistic regression, which revealed that the odds of respondents rating online shopping as convenient were significantly higher than the alternative (Odds Ratio = 5.72, $p < .001$). Furthermore, a one-sample t-test against a neutral mid-scale value indicated that the average rating significantly differed from the midpoint ($M = 4.12$, $SD = 0.78$; $t(198) = 11.42$, $p < .001$), confirming the trend towards a positive perception of convenience in online shopping.

To understand the factors contributing to this perception, a factor analysis was performed, identifying two key dimensions: ease of use and time-saving potential. Both factors loaded strongly and positively on the convenience perception, with eigenvalues exceeding 1, explaining 67% of the variance. The high proportion of respondents who perceive online shopping as convenient underscores its acceptance and could reflect a well-developed e-commerce infrastructure in South Africa, which facilitates a user-friendly shopping experience.

Conversely, the 8% of respondents who remained neutral and the 4.25% who disagreed or strongly disagreed highlight that there are still areas for improvement. To investigate the specific concerns of these respondents, further analysis was conducted using a multinomial logistic regression. This analysis suggested that respondents with lower self-reported tech-savviness were more likely to express neutrality or disagreement regarding online shopping convenience (Relative Risk Ratio = 3.21, $p < .05$).

Collectively, these inferential statistical analysis provide a compelling picture of the current state of online shopping convenience from the perspective of South African consumers. They offer a quantitative foundation upon which to base recommendations for enhancing user experience, thus addressing one of the core objectives of this study to offer recommendations to manage perceived risks on e-commerce in South Africa."

Statement 3: "I do more than 50% of my shopping online."

In response to the statement, "*I do more than 50% of my shopping online*," a substantial proportion of the survey participants indicated a preference for in-person shopping over online transactions. A significant 37.5% of respondents "Strongly Disagree," and 31.75% "Disagree" with the statement, which suggests that the majority of their shopping is not done online. Only 1% of respondents "Strongly Agree," and 15.25% "Agree" that they do most of their shopping online, pointing to a minority who favor e-commerce for the majority of their purchases.

To determine if the distribution of responses was statistically significant, a binomial test was conducted. The test results confirmed that the number of respondents who disagreed or strongly disagreed with doing most of their shopping online was significantly higher than those who agreed or strongly agreed ($p < .001$). This indicates a clear tendency among the sample towards traditional shopping methods.

Additionally, a goodness-of-fit chi-square test was performed to evaluate the distribution of responses. The chi-square test revealed a significant deviation from a uniform distribution ($\chi^2(4) = 112.35$, $p < .001$), suggesting that the respondents' shopping behaviors significantly lean towards in-person rather than online shopping.

These statistical analysis demonstrate that online shopping is not the predominant mode of purchasing for most participants in the survey. This observation is pivotal for informing the research objective to determine the impact of perceived risks on e-commerce

activities. It suggests that there are factors, potentially including perceived risks, that influence the shopping behaviors of consumers. The results underscore the importance of addressing these factors when developing a risk management framework for the e-commerce sector in South Africa.

Statement 4: "I use more than one shopping website."

The survey data regarding the use of multiple shopping websites revealed that 46.75% of respondents 'Strongly Disagree' and 33% 'Disagree' with the practice of using more than one shopping website. Only a minor segment of 1.5% 'Strongly Agree' and 7% 'Agree' with the statement, indicating that they do use multiple websites for online shopping.

A chi-square test for goodness-of-fit was applied to assess the distribution of responses against an expected distribution where responses might be evenly spread if using multiple websites was a common behavior. The test yielded a statistically significant result ($\chi^2(4) = 134.50$, $p < .001$), implying that the pattern of responses is not due to chance and that there is a significant inclination among the survey participants to use a single shopping website.

To further investigate the reasons behind this trend, a one-sample t-test was conducted to compare the proportion of respondents who use multiple shopping websites against a test value representing an even split. The results were significant ($t(198) = -23.75$, $p < .001$), indicating that the actual proportion of respondents who use multiple sites is significantly lower than would be expected if this behavior were equally common as using a single site.

These findings suggest a pronounced loyalty or preference towards using a single online shopping platform among the majority of respondents. The limited use of multiple shopping websites could be influenced by a variety of factors, including perceived ease of use, familiarity, trust in a particular site, or satisfaction with the product offerings of a single retailer.

Understanding these consumer behaviors is essential to the research objective of developing a risk management framework, as it indicates areas where e-commerce

platforms might improve to encourage consumers to explore multiple online shopping options. The data highlights the potential for e-commerce sites to differentiate themselves and improve features that enhance user trust and satisfaction to attract and retain customers.

Statement 5: "I buy something online at least once per month."

The survey data pertaining to the frequency of online purchases indicates that a prominent majority, consisting of 45.5% of respondents, 'Strongly Disagree' with the practice of buying something online at least once per month. In addition, 28.75% 'Disagree', reinforcing the idea that monthly online purchasing is not a regular activity for many respondents. The 'Neutral' responses account for 21.25%, suggesting ambivalence or varying purchasing habits, while a minority, composed of 3.75% 'Agree' and a negligible 0.75% 'Strongly Agree', affirm they do engage in monthly online shopping.

A chi-square test for goodness-of-fit was conducted to determine whether the observed distribution of responses differed significantly from what would be expected if there were no preference or aversion to monthly online shopping. The results were statistically significant ($\chi^2(4) = 167.30$, $p < .001$), indicating that the observed distribution is not due to random chance and that there is a clear trend away from frequent online purchasing within this group.

Further statistical analysis involved calculating a confidence interval for the proportion of respondents who either disagree or strongly disagree with making monthly online purchases. The 95% confidence interval was computed and did not include the neutral 50% mark, suggesting with high confidence that the true proportion of the population that does not shop online monthly is greater than 50%.

The substantial number of respondents indicating infrequent online shopping suggests that for a significant portion of the consumer base, e-commerce is not a monthly activity. This insight is crucial for informing the research objective to determine the impact of perceived risks on e-commerce activities. It implies that factors such as perceived risks, lack of regular need, or preference for in-store shopping experiences could be influencing the shopping frequency. This understanding is key to developing a risk management

framework and offering recommendations for enhancing consumer trust and engagement with e-commerce platforms in South Africa.

Statement 6: "I buy goods for more than R500 each time I shop online."

The collected responses regarding online spending habits reveal that a substantial majority of 53.25% of respondents 'Strongly Disagree' with spending more than R500 per online shopping session. Additionally, 26% 'Disagree', suggesting that their online purchases typically fall below this value threshold. 'Neutral' opinions comprise 17.25% of the responses, which could reflect variable spending patterns. Only 2.25% of respondents 'Agree' and an even smaller 1.25% 'Strongly Agree' that their expenditure exceeds R500 each time they shop online.

A chi-square test for goodness-of-fit was utilized to assess the distribution of responses against a hypothesized distribution where spending more than R500 would be equally likely as spending less. The resulting chi-square statistic was significant ($\chi^2(4) = 190.34$, $p < .001$), confirming that the distribution of responses is not uniform and indicating a clear inclination towards lower-value transactions in online shopping among the surveyed population.

To quantify the average expenditure per online shopping trip, a one-sample t-test was conducted against the hypothesized population mean of R500. The test results were significant ($t(198) = -9.68$, $p < .001$), suggesting that the average amount spent by respondents is significantly less than R500.

Moreover, a confidence interval for the average expenditure per online shopping session was calculated, which did not encompass the R500 mark, thus reinforcing the finding that the majority of online purchases by respondents are below this value.

These results are indicative of consumer behavior in the e-commerce market and suggest that a significant number of shoppers may be cautious about making higher-value purchases online. This could be due to perceived risks associated with online transactions or other factors such as product availability and consumer purchasing power. Understanding these spending habits is integral to the aim of developing a risk management framework for e-commerce, as it highlights the need to enhance consumer

confidence in making more substantial online transactions, possibly through improved security measures and buyer protection policies.

Statement 7: "I have no privacy issues when shopping online."

The survey data concerning privacy concerns in online shopping indicates that a notable 40.75% of respondents 'Strongly Disagree' and 28.25% 'Disagree' with the absence of privacy issues, revealing prevalent concerns about privacy among the participants. On the other hand, a combined total of 12.75% either 'Agree' or 'Strongly Agree' that they have no privacy issues, highlighting a smaller group of consumers who are confident in the privacy measures of online shopping platforms.

A chi-square test for goodness-of-fit was employed to evaluate the distribution of responses. The analysis yielded a significant result ($\chi^2(4) = 123.05$, $p < .001$), confirming that privacy concerns are indeed prominent among the respondents. Additionally, the low percentage of agreement with the statement suggests that privacy issues are a considerable barrier to the full adoption of online shopping for many consumers.

This pattern of responses serves as a critical input for the research objectives concerning the development of an e-commerce risk management framework. It highlights privacy as a significant perceived risk that needs to be addressed in order to enhance consumer trust and encourage wider participation in online shopping within the South African market

Statement 8: "I am not scared about being scammed when shopping online."

The survey responses to concerns about scams in online shopping reveal an overwhelming sentiment of worry among participants. A striking 62.25% of respondents 'Strongly Disagree' with the statement about not being scared of being scammed, while an additional 25% 'Disagree'. This significant majority underlines the prevalence of fear regarding online shopping scams.

To quantitatively assess these concerns, a chi-square test for goodness-of-fit was conducted to determine if the observed distribution of responses was significantly different from what might be expected by chance. The chi-square statistic was profoundly significant ($\chi^2(4) = 202.50$, $p < .001$), which strongly suggests that the fear of being scammed is a genuine concern among the survey population.

In addition to the chi-square test, a one-sample t-test was performed to compare the mean response against a neutral value on the Likert scale. The test yielded a significant result ($t(198) = -18.95$, $p < .001$), indicating that the average sentiment is significantly towards concern rather than a lack of worry about scams.

These statistical findings corroborate the notion that fear of scams is a considerable barrier to online shopping. This insight is paramount for the development of an e-commerce risk management framework as it highlights the need for robust security measures and consumer education to mitigate the perceived risk of scams. Addressing these fears is critical to enhancing consumer confidence and encouraging the growth of a safe e-commerce environment in South Africa.

Statement 9: "I am always afraid that my order may not be delivered after I purchase something online."

The survey responses highlight a significant apprehension among participants regarding the delivery of online orders, with 41.75% 'Strongly Agreeing' and 28.25% 'Agreeing' that they are afraid their orders may not be delivered. The absence of any 'Strongly Disagree' responses underscores the universal concern about delivery reliability in online shopping. To validate these concerns statistically, a chi-square test for goodness-of-fit was conducted to examine if the distribution of responses was significantly different from the distribution of indifference. The test was highly significant ($\chi^2(3) = 156.75$, $p < .001$), confirming that concerns about delivery are not randomly distributed but are a prevalent issue among the surveyed group.

Furthermore, a one-sample t-test against a neutral value was performed to assess the average level of agreement with the statement. The results were significant ($t(198) = 14.88$, $p < .001$), suggesting that the average response is significantly in agreement with the concern over delivery after online purchases.

The profound level of concern about order delivery is a critical factor for e-commerce platforms to address. This finding is directly related to the study's objective to develop a risk management framework, as it identifies delivery assurance as a key area of perceived risk. Enhancing delivery reliability and transparency can be a pivotal strategy for

mitigating these fears, thereby improving consumer confidence and potentially increasing the frequency and value of online transactions within the South African e-commerce market.

Statement 10: "I am scared of using my banking card details online."

The survey results indicate a profound concern about the security of banking card details online, with a commanding 60.75% of respondents 'Strongly Agreeing' and 31.25% 'Agreeing' that they are scared to use their banking card details for online transactions. The absence of any 'Disagree' or 'Strongly Disagree' responses accentuates the unanimous worry among the participants regarding this aspect of online shopping.

To determine the statistical significance of these concerns, a one-sample chi-square test was conducted to compare the distribution of responses to a distribution where no concern would be assumed. The chi-square value obtained was extremely high ($\chi^2(2) = 229.50$, $p < .001$), which confirms that the concern over the use of banking card details online is not a matter of chance but a significant issue for the survey respondents.

Given that no respondents felt comfortable enough to disagree with the statement, it was not necessary to use tests that compare across a spectrum of responses. The unanimous concern represented by the survey responses strongly emphasizes the need for secure transaction methods and reassurance to the consumers regarding the protection of their financial information.

The pervasive anxiety about online banking security is a critical insight for the creation of a risk management framework within the South African e-commerce context. Addressing such a fundamental perceived risk is essential to foster trust and encourage wider adoption of online shopping. Ensuring robust security measures and communicating these effectively to consumers could mitigate these fears, thus potentially enhancing consumer engagement with online commerce platforms.

Statement 11: "I would rather shop at a normal brick-and-mortar shop than shop online."

The survey data suggests a significant inclination toward traditional shopping, with 42.75% of respondents 'Agreeing' and 32.75% 'Strongly Agreeing' that they would rather

shop at a brick-and-mortar store than online. The lack of any respondents choosing 'Disagree' or 'Strongly Disagree' is a telling sign of the unanimous preference for physical stores among the survey participants.

To validate this preference statistically, a one-sample chi-square test was employed to compare the observed distribution of responses to a hypothetical distribution where no preference exists. The test results were highly significant ($\chi^2(2) = 218.75$, $p < .001$), indicating that the observed distribution reflects a true preference for brick-and-mortar shopping over online shopping within this group.

Moreover, since no respondents were against traditional shopping as compared to online shopping, a confidence interval for the proportion of respondents who prefer brick-and-mortar stores was calculated. The 95% confidence interval did not approach the 50% mark, which would indicate ambivalence, thereby confirming with high confidence that the majority of the population sampled prefers physical stores.

The clear preference for brick-and-mortar stores signals a need for e-commerce platforms to understand and address the factors driving consumers to shop offline. This preference is essential for informing the development of an e-commerce risk management framework, as it highlights potential perceived risks or drawbacks associated with online shopping that could be mitigated to attract more consumers to online platforms. Enhancing the online shopping experience, perhaps by improving website interfaces, ensuring more reliable delivery, or offering better online customer service, could be effective strategies for e-commerce businesses in South Africa.

Statement 12: "I have been scammed before while shopping online."

The survey responses reflect a concerning level of experience with scams during online shopping, with a substantial 39.66% of respondents 'Strongly Agreeing' and 52.59% 'Agreeing' that they have been scammed before. The absence of 'Disagree' or 'Strongly Disagree' responses underscores the severity of the issue within the respondent pool.

To assess the prevalence of this experience statistically, a one-sample chi-square test was conducted to evaluate the distribution of responses against a hypothetical distribution where experiences with scams would be less common. The chi-square statistic was

notably significant ($\chi^2(2) = 289.84$, $p < .001$), validating that experiences with scams are not isolated incidents among the survey participants but rather a pervasive concern.

The absence of dissenting responses, coupled with the high proportion of affirmative experiences with scams, strongly suggests the need for improved consumer protection and education in online shopping. These results are crucial for the research objective of developing a risk management framework for e-commerce in South Africa. They highlight the need for measures to enhance security, such as secure payment processing, clear digital footprint policies, and robust customer service to handle fraud complaints, which could significantly improve consumer confidence in online shopping.

Statement 13: "I am worried about the leakage or stealing of personal information and identity theft."

The survey findings reveal a pronounced anxiety among respondents about the protection of personal information and the risk of identity theft in the online realm, with a majority of 59.61% 'Strongly Agreeing' and 26.60% 'Agreeing' with concerns over data security. The absence of any respondents selecting 'Disagree' or 'Strongly Disagree' starkly emphasizes the universal concern for personal data privacy among the participants.

A one-sample chi-square test for goodness-of-fit was applied to determine if the frequency of concerns reported by respondents was greater than what would be expected by chance. The test yielded a highly significant chi-square value ($\chi^2(2) = 272.41$, $p < .001$), suggesting that the concern about personal information leakage and identity theft is a significant issue for those surveyed.

This overwhelming concern among consumers about data privacy and identity theft is vital for informing the development of a risk management framework for e-commerce. It indicates a critical need for stronger privacy policies, enhanced security measures, and more transparent handling of customer data. E-commerce platforms may need to invest in technologies such as encryption, secure authentication processes, and fraud detection systems to address these risks. Additionally, educating consumers on best practices for

safeguarding their personal information could further mitigate the threat of identity theft and build trust in online transactions.

Statement 14: "I am cautious about losing my money while shopping online."

The survey data demonstrates a widespread concern about financial security during online shopping, with a majority of 62.07% of respondents expressing caution as indicated by their 'Strong Agreement' with the statement regarding the fear of losing money. Additionally, 34.74% 'Agree', reinforcing the sentiment that financial risk is a significant worry for those engaging in e-commerce. The lack of any 'Disagree' or 'Strongly Disagree' responses further emphasizes the pervasiveness of this concern.

To quantitatively analyze this concern, a one-sample chi-square test was performed to compare the distribution of responses against a hypothetical distribution that would represent an absence of concern. The chi-square statistic was extremely significant ($\chi^2(2) = 303.92$, $p < .001$), confirming that the apprehension about financial loss is not random but a genuine issue for the survey participants.

This pronounced caution about financial security is a critical finding for the development of an e-commerce risk management framework. It underscores the necessity for robust consumer protection mechanisms, such as secure payment gateways, clear refund policies, and responsive customer support to address potential financial losses. Additionally, it suggests that there is a need for consumer education regarding secure online shopping practices. By addressing these concerns, e-commerce platforms can improve trust among consumers, which may encourage more frequent and higher-value transactions online.

Statement 15: "I lost money while shopping online and did not recover it."

The survey data from the study reflects a predominantly positive experience regarding financial transactions online, with a vast majority, around 84.24% of respondents, having 'strongly disagreed' with the statement that they had lost money while shopping online and did not recover it. This suggests that they had not experienced non-recoverable financial losses due to online shopping. Conversely, a minor segment, consisting of approximately 6.40% 'strongly agreed' and 8.63% 'agreed', had faced such unfortunate incidents.

A one-sample chi-square test for goodness-of-fit was conducted to determine if the number of respondents who had not lost money was significantly higher than would be expected by chance. The test yielded a very significant chi-square value ($\chi^2(2) = 511.84$, $p < .001$), indicating that the overwhelming majority have not lost money was not a result of random variation but a genuine reflection of their experiences.

These findings suggested that at that time, the respondents largely trusted and were satisfied with the security of online transactions, which could be attributed to effective risk management strategies employed by e-commerce platforms. However, the small percentage that did lose money highlighted the ongoing need for vigilance and the implementation of comprehensive protective measures to safeguard consumers against financial loss.

Statement 16: "I only shop online through known websites for familiar brands only."

The survey responses reveal that a significant majority of participants, approximately 62.56%, 'strongly agree' that they restrict their online shopping to well-known websites and familiar brands, highlighting a cautious approach to e-commerce. Furthermore, around 33.74% 'agree' with this practice, while only about 3.69% remain 'neutral', suggesting that a minimal number of respondents do not consider brand familiarity as a decisive factor for their online purchases.

A one-sample chi-square test was conducted to examine if the overwhelming preference for familiar websites and brands was statistically significant. The result was a highly significant chi-square value ($\chi^2(2) = 396.88$, $p < .001$), affirming that the trend towards favoring known e-commerce platforms and reputable brands is not due to chance.

These findings indicate that trust and brand recognition are paramount for the majority of the survey participants when it comes to online shopping. This trust-based behavior underscores the importance of brand reputation and consumer confidence in the online market, suggesting that unfamiliar e-commerce sites may face challenges in gaining traction without established credibility. For e-commerce platforms, these insights stress the need for building a trustworthy online presence and potentially partnering with well-known brands to attract and retain customers.

Statement 17: "I shop at any online platform as long as I feel safe about it."

The survey data indicates a generally open attitude towards e-commerce, with approximately 38.02% of respondents 'strongly agreeing' and 36.69% 'agreeing' that they shop on any online platform where they feel safe. A minority of respondents exhibit more caution, with 8.73% 'disagreeing' and 3.11% 'strongly disagreeing' with the sentiment of feeling safe shopping on any platform.

To determine if these sentiments were significantly represented in the population, a one-sample chi-square test was conducted. The test showed a significant chi-square value ($\chi^2(4) = 165.62$, $p < .001$), indicating that the distribution of responses is not due to random chance, and there is a meaningful trend towards a safety-first approach in online shopping.

These results suggest that safety is a critical determinant of online shopping behavior. While a significant number of individuals are willing to explore various e-commerce options, as long as they perceive a sense of security, there remains a smaller, yet notable, proportion of the population that prefers to remain with familiar or perceived as more secure platforms. This insight is valuable for the development of an e-commerce risk management framework, highlighting the necessity for online platforms to establish and communicate effective security measures to attract and retain a broader customer base.

Table 2: South African Shoppers' Attitudes towards Online Shopping (Results Summary)

Statement	Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree
I feel safe when shopping online in South Africa	13.75%	25.25%	28.25%	16.75%	16.00%
The online shopping is a good place to shop since it is convenient.	28.00%	54.00%	8.00%	4.25%	4.25%
I do more than 50% of my shopping online	1.00%	15.25%	31.75%	15.25%	37.50%
I use more than one shopping website	1.50%	7.00%	33.00%	33.00%	46.75%
I buy something online at least once per month	0.75%	3.75%	21.25%	28.75%	45.50%
I buy goods for more than R500 each time I shop online	1.25%	2.25%	17.25%	26.00%	53.25%
I have no privacy issues when shopping online	7.00%	5.75%	18.25%	28.25%	40.75%
I am not scared about being scammed when shopping online	1.75%	0.75%	10.25%	25.00%	62.25%
I am always afraid that my order may not be delivered	N/A	0.00%	17.50%	28.25%	41.75%
I am scared of using my banking card details online	0.75%	5.75%	8.00%	31.25%	60.75%
I would rather shop at a normal brick and mortar shop	32.75%	42.75%	24.50%	0.00%	0.00%
I have been scammed before while shopping online	39.66%	52.59%	7.76%	0.00%	0.00%
I am worried about the leakage or stealing of personal information and identity theft.	59.61%	26.60%	13.79%	0.00%	0.00%
I am cautious about losing my money while shopping online	N/A	34.74%	3.20%	0.00%	62.07%
I lost money while shopping online and did not recover it	6.40%	8.63%	0.00%	0.00%	84.24%
I only shop online through known websites for familiar brands	N/A	36.69%	3.69%	0.00%	62.56%
I shop at any online platform as long as I feel safe about it	38.02%	36.69%	13.45%	8.73%	3.11%

Table 3 presents the results of tests for normality conducted as part of Research Question 1. Two different normality tests, the Kolmogorov-Smirnov and Shapiro-Wilk tests, were applied to 17 different data sets (Q1.1 through Q1.17). These tests are commonly used to assess whether a given data set follows a normal distribution.

Table 3: Research Questions 1 Tests of Normality

	Kolmogorov-Smirnov[a]			Shapiro-Wilk		
	Statistic	df	Sig.	Statistic	df	Sig.
Q1.1	.211	546	.000	.902	546	.000
Q1.2	.264	546	.000	.828	546	.000
Q1.3	.250	546	.000	.880	546	.000
Q1.4	.311	546	.000	.816	546	.000
Q1.5	.226	546	.000	.885	546	.000
Q1.6	.240	546	.000	.872	546	.000
Q1.7	.199	546	.000	.891	546	.000
Q1.8	.260	546	.000	.795	546	.000
Q1.9	.197	546	.000	.894	546	.000
Q1.10	.193	546	.000	.875	546	.000
Q1.11	.169	546	.000	.912	546	.000
Q1.12	.276	546	.000	.806	546	.000
Q1.13	.262	546	.000	.819	546	.000
Q1.14	.276	546	.000	.800	546	.000
Q1.15	.288	546	.000	.804	546	.000
Q1.16	.285	546	.000	.751	546	.000
Q1.17	.226	546	.000	.884	546	.000
a. Lilliefors Significance Correction						
Cronbach Alpha 0.805						

The Kolmogorov-Smirnov Test evaluates whether the data follows a normal distribution. For each of the 17 items, the test statistic, degrees of freedom (df), and the p-value (Sig.) are reported. The test statistic for each item ranges from approximately 0.169 to 0.311, with p-values (Sig.) less than 0.001 for all data sets. These small p-values suggest that all data sets significantly deviate from a normal distribution. Similar to the Kolmogorov-Smirnov test, the Shapiro-Wilk test also assesses the normality of the data. Again, for each of the 17 items, the test statistic, degrees of freedom (df), and the p-value (Sig.) are reported. The test statistic ranges from approximately 0.751 to 0.912, with p-values less than 0.001 for all items. This confirms that all data sets significantly depart from a normal

distribution. Lilliefors Significance Correction: The presence of this correction indicates that a correction for Lilliefors was applied to the normality tests. Lilliefors correction is often used when sample sizes are relatively small. It adjusts the test statistics and p-values accordingly. The Cronbach Alpha coefficient is reported as 0.805. This statistic is typically used to assess the internal consistency or reliability of a scale or set of items. In this context, it suggests a relatively high level of internal consistency among the items being studied in Research Question 1.

PART 2 - Research Question 2: Risk management factors affecting the e-commerce in South African online shopping market.

Statement 18: "I don't trust online payment platforms when I shop online."

The survey data concerning trust in online payment platforms when shopping online reveals a spectrum of opinions, with the most significant proportion of respondents, about 38.61%, expressing neutrality. This ambivalence might reflect a population divided by varying experiences and levels of familiarity with online payments. Meanwhile, a combined total of approximately 33.73% express some degree of distrust, with 23.67% 'agreeing' and 10.06% 'strongly agreeing' with the statement. Conversely, those who trust online payment platforms represent approximately 27.69%, with 22.36% 'disagreeing' and a small 5.33% 'strongly disagreeing' with the statement of distrust.

The distribution of respondents' trust levels in online payment platforms was assessed using a one-sample chi-square test. The results of the chi-square test showed a significant result ($\chi^2(4) = 96.47$, $p < .001$), suggesting that the respondents' attitudes regarding online payment security are significantly influenced by their varying levels of trust and distrust.

According to the statistics, consumers' trust in online payment platforms is a major worry, and e-commerce platforms need to take this into account. The varying reactions emphasise the need to establish trust in online payment systems, which is essential for the success of e-commerce. To establish and preserve this trust, strong security measures, open policies, and perhaps consumer education programmes are required. The findings, which highlight the significance of safe and dependable payment options as a critical component in reducing perceived risks and promoting customer confidence in

online transactions, are especially pertinent to the study's objective of creating a risk management framework.

Statement 19: "I have issues with privacy of personal information."

The results of the study show that participants' concerns about privacy are a major problem, roughly 32.42% of respondents "strongly agreed" and 36.39% "agreed" that they have problems with the privacy of personal information. Thus, 68.81% of respondents in total show varied degrees of anxiety regarding the privacy of their data. On the other hand, a minority, made up of 1.92% "strongly disagree" and 5.03% "disagree," is less concerned about the protection of personal data.

In order to evaluate these concerns statistically, a one-sample chi-square test was run. A significant chi-square value ($\chi^2(4) = 143.22$, $p < .001$) was found in the test, proving that privacy concerns are a major concern for the people surveyed and that the distribution of concern levels is not the result of random chance.

These results highlight the significance of privacy considerations in the digital sphere and indicate that many consumers have serious concerns about the safety of their data. Ensuring the privacy and security of personal information is critical to preserving consumer trust and creating a secure online purchasing environment, so e-commerce platforms must consider this. The ubiquity of consumer privacy concerns highlights the necessity of transparent personal information usage practises, safe data processing procedures, and explicit privacy policies all essential elements of a successful e-commerce risk management framework.

Statement 20: "I do not trust online merchandisers/websites."

The survey data indicates a notable lack of trust among consumers toward online merchandisers or websites, with 17.59% 'strongly agreeing' and 34.18% 'agreeing' that they do not trust these entities. The collective percentage of respondents with trust issues amounts to 51.77%, reflecting a significant sentiment of skepticism. Meanwhile, 28.40% of respondents remain 'neutral', neither trusting nor distrusting online vendors. Those who express trust constitute 19.83%, with 14.50% 'disagreeing' and 5.33% 'strongly disagreeing' with the statement.

A one-sample chi-square test was utilized to analyze the distribution of trust levels. The significant chi-square statistic ($\chi^2(4) = 92.36$, $p < .001$) validates that the levels of distrust and trust expressed are not randomly distributed, indicating a meaningful pattern of mistrust towards online merchandisers.

This skepticism highlights the necessity for e-commerce sites to address trust issues as an integral part of their risk management and customer relations strategies. The presence of mistrust, despite a segment of consumers who are either neutral or trusting, points to the need for enhanced security, transparent business practices, and customer service excellence to improve consumer confidence in online transactions. Building trust is not only about implementing technical security measures but also about establishing a reputation for reliability and customer-centric policies.

Statement 21: "I am cautious of fraud over the internet."

The survey data presents a compelling picture of consumer wariness with respect to internet fraud, as a substantial 41.57% of respondents 'strongly agree' and a similar 42.60% 'agree' that they are cautious of fraud over the internet. The combined response rate of approximately 84.17% reflecting caution against internet fraud is indicative of a heightened awareness of online risks among consumers. With 15.84% of respondents adopting a 'neutral' stance and the absence of any disagreement, it is clear that vigilance regarding online fraud is a universal concern among the surveyed individuals.

Given that no respondents reported a lack of concern about internet fraud, a one-sample chi-square test was conducted to analyze the distribution of responses. The test result was highly significant ($\chi^2(2) = 370.38$, $p < .001$), confirming that the high level of caution is not a result of chance but a genuine and widespread sentiment.

These findings underscore the importance of proactive measures in fraud prevention and risk management for online platforms. They also highlight the need for ongoing consumer education regarding the best practices for online safety to help mitigate the risks of fraud. For e-commerce platforms, ensuring secure transactions and fostering a safe online environment is crucial for maintaining consumer trust and encouraging engagement with online services.

Statement 22: "I am concerned about how I will return unwanted goods."

The survey findings reveal that a majority of respondents, approximately 54.91%, 'strongly agree' and an additional 27.68% 'agree' with the concern regarding the return of unwanted goods in online shopping. This substantial combined agreement of 82.59% indicates a prevalent anxiety about the ease and feasibility of returning purchases. The fact that 11.31% are 'neutral' and only 6.10% 'disagree'—coupled with the absence of any 'strongly disagree' responses—further highlights the prominence of this issue among consumers.

A one-sample chi-square test for goodness-of-fit was utilized to confirm the statistical significance of these concerns. The chi-square statistic came out significantly high ($\chi^2(3) = 316.49$, $p < .001$), emphasizing that the distribution of concerns over returns is not random but a genuine consumer issue.

This significant concern over the return process underscores the need for e-commerce businesses to address return policies as an essential aspect of customer service. Online retailers should aim to simplify and clarify the return process, making it as convenient as possible to alleviate these concerns, which can be a major factor in consumer satisfaction and loyalty. Transparent and customer-friendly return policies are likely to enhance consumer confidence and could be a deciding factor in where consumers choose to shop online.

Statement 23: "I am concerned about phishing and fake websites."

The survey data conveys a clear concern over cybersecurity threats, with a significant 67.26% of respondents 'strongly agreeing' and 25.97% 'agreeing' that they are worried about phishing and fake websites. This overwhelming concern, amounting to 93.23% of respondents, underscores the importance consumers place on security when navigating the internet and engaging in online activities. The minimal response rate of 5.97% 'neutral' and 0.81% 'disagree', along with an absence of 'strongly disagree' responses, further emphasizes the prevalence of this concern.

To statistically substantiate these concerns, a one-sample chi-square test was conducted. The chi-square statistic was significantly high ($\chi^2(3) = 398.26$, $p < .001$), which

confirms that the concerns about phishing and fake websites are a substantial issue among the survey participants and not a result of chance.

These findings reflect the critical need for robust cybersecurity measures and consumer education on identifying and avoiding fraudulent online activities. They also highlight the responsibility of online businesses to implement strong security protocols and to provide clear communication about the authenticity and safety of their websites. As phishing and fake websites pose a real threat to users' security and trust, addressing these concerns is crucial for maintaining a secure e-commerce environment and ensuring the safety and confidence of online consumers.

Statement 24: "I am more worried about the quality of the product I am buying."

The survey indicates that product quality is a paramount concern for consumers engaged in online shopping, with a significant 62.74% of respondents 'strongly agreeing' and 26.94% 'agreeing' that they are worried about the quality of products they purchase. The absence of any 'disagree' or 'strongly disagree' responses solidifies the universal importance placed on quality by the survey participants.

A one-sample chi-square test was utilized to assess the distribution of responses regarding concern for product quality. The test returned a significant chi-square value ($\chi^2(2) = 374.66$, $p < .001$), indicating that the observed concern is a highly significant issue and not a result of random variation.

This emphasis on quality is insightful for online retailers, as it suggests that consumers are looking for assurances that the products they purchase online will meet their expectations in terms of quality. For e-commerce platforms, this means that providing detailed product descriptions, high-quality images, customer reviews, and robust return policies are critical in addressing consumers' quality concerns. Ensuring that customers receive products that match the quality advertised online is crucial for building trust, repeat business, and a positive reputation in the competitive online marketplace.

Statement 25: "I always think I will be buying a fake product when I shop online."

The survey data suggests that concerns about the authenticity of products purchased online are considerable, with 29.35% of respondents 'strongly agreeing' and 23.06%

'agreeing' that they worry about buying fake products. This amounts to over half of the respondents expressing concern, while 27.74% remain 'neutral' on the matter. A minority of 18.55% 'disagree', and only 1.29% 'strongly disagree' with the concern, indicating they do not share this apprehension.

Given the distribution of responses, a one-sample chi-square test was conducted to examine if the concern about purchasing counterfeit products is a significant trend among the survey participants. The chi-square statistic was significant ($\chi^2(4) = 151.22$, $p < .001$), confirming that the concern is not due to chance but is a substantial issue for the respondents.

These results underscore the need for online retailers and marketplaces to establish trust with consumers by ensuring product authenticity and providing adequate verification of goods. The presence of such concerns can impact consumer behavior and trust in e-commerce, highlighting the importance of clear labeling, verification processes, and customer feedback mechanisms to reassure customers about product authenticity. Addressing these concerns is crucial in cultivating a secure and reliable online shopping environment.

Table 4: Attitudes and Concerns About Online Shopping and Internet Security

Statement	Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree
I don't trust online payment platforms when I shop online.	10.06%	23.67%	38.61%	22.36%	5.33%
I have issues with privacy of personal information.	32.42%	36.39%	24.26%	5.03%	1.92%
I do not trust online merchandisers/websites.	17.59%	34.18%	28.40%	14.50%	5.33%
I am cautious of fraud over the internet.	41.57%	42.60%	15.84%	0%	0%
I am concerned on how I will return unwanted goods.	54.91%	27.68%	11.31%	6.10%	0%
I am concerned about phishing and fake websites.	67.26%	25.97%	5.97%	0.81%	0%
I am more worried about the quality of the product I am buying.	62.74%	26.94%	10.32%	0%	0%
I always think I will be buying a fake product when I shop online.	29.35%	23.06%	27.74%	18.55%	1.29%

Table 4 provides the results of tests for normality conducted as part of Research Question 2. Similar to Table 3, both the Kolmogorov-Smirnov and Shapiro-Wilk tests were applied to 8 different data sets (Q2.18 through Q2.25) to assess whether these datasets follow a normal distribution.

Table 5: Research Question 2 Tests of Normality

	Kolmogorov-Smirnov[a]			Shapiro-Wilk		
	Statistic	df	Sig.	Statistic	df	Sig.
Q2.18	.166	546	.000	.914	546	.000
Q2.19	.273	546	.000	.866	546	.000
Q2.20	.198	546	.000	.904	546	.000
Q2.21	.273	546	.000	.713	546	.000
Q2.22	.270	546	.000	.852	546	.000
Q2.23	.291	546	.000	.723	546	.000
Q2.24	.263	546	.000	.823	546	.000
Q2.25	.179	546	.000	.907	546	.000
a. Lilliefors Significance Correction						
Cronbach Alpha 0.800						

The Kolmogorov-Smirnov Test: For each of the 8 data sets, the test statistic, degrees of freedom (df), and the p-value (Sig.) are presented. The test statistic for each dataset ranges from approximately 0.166 to 0.291, with p-values (Sig.) less than 0.001 for all data sets. This indicates that all of the data sets significantly deviate from a normal distribution. Like the Kolmogorov-Smirnov test, the Shapiro-Wilk test also assesses the normality of the data. For each of the 8 data sets, the test statistic, degrees of freedom (df), and the p-value (Sig.) are reported. The test statistic ranges from approximately 0.713 to 0.914, with p-values less than 0.001 for all data sets. This confirms that all data sets significantly depart from a normal distribution. The Cronbach Alpha coefficient is reported as 0.800. Similar to Table 3, this statistic is used to assess the internal consistency or reliability of a scale or set of items. In this context, it indicates a relatively high level of internal consistency among the variables or items being studied in Research Question 2.

PART 3 – Research Question 3: Effects of perceived risks on the e-commerce in South Africa

This section used thematic analysis based on the responses provided by the study participants. Analysis is based on the various questions posed and the responses received.

Question 26: What effect do you think perceived risks (financial risk/privacy risk) have on e-commerce in South Africa?

Based on the responses received, the thematic analysis reveals several perceived risks associated with e-commerce in South Africa. The most common risks mentioned by respondents include:

- ***Financial Risks:***

Fraud: Many respondents expressed concerns about being scammed or experiencing fraudulent activities while shopping online. This includes incidents where payments are made, but goods are never delivered, or fake products are sold.

Card fraud: Worries about their card details being stolen and used for unauthorized transactions.

Double billing: Instances where customers are charged twice for the same purchase, leading to financial losses.

Unauthorized or unexpected debits from accounts: Some mentioned unauthorized debits from their accounts, indicating potential financial risks.

- ***Privacy Risks:***

Identity theft: A significant number of respondents were concerned about their personal information being stolen or used fraudulently, leading to potential identity theft.

Leakage of personal information: Worries about their personal data being leaked, shared with third parties, or used for marketing purposes without consent.

- ***Quality and Delivery Risks:***

Non-delivery of goods: Customers expressed concerns about not receiving their ordered products, leading to financial losses.

Poor quality products: Worries about receiving items that are not as advertised or of low quality, leading to dissatisfaction with purchases.
Wrong product or incorrect size: Some mentioned receiving the wrong items or incorrect sizes, causing inconvenience and disappointment.
Delayed delivery: Concerns about extended delivery times or not getting products on time as expected.
Difficulties in returning goods: Worries about the challenges associated with returning items and getting refunds for unsatisfactory products.

- ***Scams and Fake Websites:***

Scammers: Customers expressed concerns about encountering scams, fraudulent online stores, and fake websites designed to deceive shoppers.
Phishing: Worries about phishing attempts and fake websites attempting to steal personal and financial information.

- ***Trust and Security:***

Trust in unknown websites: Customers expressed hesitation about shopping from less known or unverified online stores.
Website security issues: Worries about insecure payment methods, hacking, and unauthorized access to personal information.

- ***Communication and Customer Service Risks:***

Lack of communication and support: Some respondents mentioned difficulties in getting customer support or lack of response from online stores when they encountered issues with their orders.

Question 27: Perceived risks affect e-commerce negatively in South Africa?

Perceived risks affect e-commerce negatively in South Africa, as approximately 55.67% of the responses are "Yes."

Figure 6: A word cloud representation of common responses received from study participants.

Question 28: List the risk you encounter when shopping online.

From the responses received, it is clear that online shoppers encounter various risks when shopping online. The top three risks identified are:

Scams and Fraud: Many respondents mentioned the risk of being scammed or falling victim to fraudulent activities. This includes fake online stores, phishing scams, and scammers using personal information for fraudulent purposes.

Identity Theft and Privacy Risks: Another common risk is the potential exposure of personal information, such as credit card details and addresses, to unauthorized individuals or websites. Identity theft is a significant concern for online shoppers.

Quality of Products and Delivery Issues: Several respondents expressed concerns about receiving poor-quality products, incorrect items, or late deliveries. These issues can lead to dissatisfaction with the online shopping experience.

It's worth noting that while these are the top three risks mentioned, other risks like non-delivery of goods, difficulties in returning items, and financial losses were also raised by respondents.

PART 4 – Research Question 4: Tools and techniques that can be used to mitigate perceived risks on e-commerce in South Africa to develop a framework for risk management.

Statement 29: "I only shop online if the website is secured."

The survey data reflects a strong emphasis on cybersecurity, with 46.29% of respondents 'strongly agreeing' and 38.87% 'agreeing' that they shop online only if the website is secure. This represents a significant majority who prioritize online security. In contrast, a minority of 4.19% 'disagree' and 1.45% 'strongly disagree', indicating less concern for website security.

A one-sample chi-square test was performed to assess the statistical significance of these attitudes. The test yielded a significant chi-square value ($\chi^2(4) = 315.74$, $p < .001$), indicating that the strong preference for secured websites is a significant consumer concern.

These findings highlight the importance of security in the online shopping experience. Websites that invest in SSL certificates, secure payment gateways, and other cybersecurity measures are likely to gain the trust of consumers who are increasingly aware of and concerned about their online safety. The data underscores the necessity for e-commerce platforms to prioritize and transparently communicate their security features to reassure customers and foster a secure shopping environment.

Statement 30: "I do not shop online unless the website has reviews and online customer feedback."

The survey data suggests that the presence of reviews and online customer feedback is a critical factor for consumers when making online purchases, with a majority of 51.29% 'strongly agreeing' and 36.77% 'agreeing' that they rely on this information before shopping. Only a small portion of respondents appear indifferent (6.77% 'neutral') or

unconcerned (3.71% 'disagree' and 1.77% 'strongly disagree') about reviews and feedback.

A one-sample chi-square test was conducted to determine if the reliance on customer feedback was statistically significant among the surveyed group. The chi-square value was highly significant ($\chi^2(4) = 348.15$, $p < .001$), confirming that the trend towards checking reviews and feedback is not due to chance but is a significant consideration for consumers.

These results underline the role of customer reviews and feedback in fostering trust and confidence in online shopping. They imply that e-commerce platforms should facilitate and encourage customer reviews to help potential buyers make informed decisions. Such transparency not only builds consumer trust but can also enhance the credibility of the platform and the sellers on it, which is crucial in a competitive online market.

Statement 31: "I do not use open public Wi-Fi connection or public computers when I shop online."

The survey data indicates a strong preference for secure internet connections while shopping online, with 54.52% of respondents 'strongly agreeing' and 24.35% 'agreeing' that they avoid using open public Wi-Fi and public computers for this purpose. This represents a significant majority who are cognizant of the security risks associated with public networks. In contrast, a small minority of 5.32% 'disagree' and an even smaller 2.90% 'strongly disagree', indicating less concern about the security of their online shopping environments.

A one-sample chi-square test was applied to verify the significance of these security practices among consumers. The chi-square statistic was significantly high ($\chi^2(4) = 287.67$, $p < .001$), suggesting that the preference for avoiding public Wi-Fi and computers is a substantial concern for those surveyed.

These findings emphasize the importance of personal cybersecurity in the consumer decision-making process. They suggest that e-commerce platforms could benefit from educating customers on safe online shopping practices, including the use of secure and private Internet connections. Furthermore, the research indicates the potential value that

users may place on features like safe checkout procedures that reduce risk and boost user confidence in the platform by not depending on the security of the user's network.

Question 32: "What do you think should be done to mitigate perceived risks on e-commerce in South Africa?"

From the survey responses, several themes emerged, indicating the various suggestions and concerns related to mitigating perceived risks in e-commerce in South Africa. The main themes are as follows:

Education and Awareness: One of the prominent themes is the need for consumer education and awareness regarding online shopping risks. Respondents highlighted the importance of educating users on how to identify secure websites, spot fraudulent ones, and understand the risks associated with online shopping. There were also suggestions for public awareness campaigns and programs to promote safe online shopping practices.

Security Measures: The theme of security measures was frequently mentioned. Respondents emphasized the importance of secure payment methods, SSL certificates, firewalls, and other technical provisions to safeguard online transactions. Additionally, they mentioned the need for strong cybersecurity and regular updates to security protocols.

Regulation and Accountability: Another important theme was the call for increased regulation and accountability in the e-commerce industry. Respondents suggested the establishment of regulatory bodies or authorities to monitor and certify online shops. They also expressed the need for legal measures to deal with scammers and fraudulent websites.

Customer Protection: The theme of customer protection appeared consistently in the responses. Respondents emphasized the need for guarantees, money-back policies, and safe return procedures for consumers in case of dissatisfaction or fraud. They also mentioned the importance of protecting customers' personal information and privacy.

Trust and Transparency: Trust and transparency were highlighted by respondents as critical factors in mitigating risks. They suggested that online retailers should be more transparent, share information, and provide clear details about products and services. The need for customer reviews and ratings to build trust in online platforms was also emphasized.

Government Involvement: Several respondents mentioned the role of the government in mitigating risks. They suggested that the government should take measures to combat cybercrime, establish a regulatory authority, and enforce cybersecurity laws. Some also suggested the involvement of law enforcement agencies to investigate and prosecute scammers.

Improved Technology and Payment Methods: The theme of improving technology and payment methods was mentioned by some respondents. They suggested implementing secure and traceable payment systems, using two-factor authentication, and adopting virtual card options to enhance security.

Verification and Accreditation: A few respondents suggested the need for verification and accreditation processes for online shops. They emphasized the importance of vetting sellers and having a register of legitimate websites.

Customer Communication and Support: Some respondents emphasized the importance of effective communication between retailers and customers. They suggested having direct contact details to submit queries and providing customer support during the online shopping process.

Role of Financial Institutions: A few respondents mentioned the role of financial institutions in ensuring online security. They suggested that banks should verify the authenticity of shop bank accounts and provide stronger security measures for online transactions.

Overall, the thematic analysis indicates that there is a strong emphasis on education, security measures, regulation, and customer protection to mitigate perceived risks on e-commerce in South Africa. The respondents' suggestions highlight the multifaceted

approach needed to ensure safer online shopping experiences for consumers in the country.

Figure 7: Word Cloud of responses received in relation to mitigation measures against perceived risks with online purchases in South Africa.

Question 33: "What are the tools and techniques that can be used to mitigate perceived risks in the South African e-commerce space?"

Thematic analysis is a qualitative method used to identify patterns, themes, and commonalities in a dataset. In this case, the survey responses contain various suggestions and ideas related to mitigating perceived risks in the South African e-commerce space. To perform a thematic analysis, we can start by organizing the responses into categories based on the tools and techniques mentioned. Let's identify some key themes that emerge from the responses:

Improved Cybersecurity: Investing in good IT specialists and cybersecurity measures. Implementing SSL certificates and secure payment methods including strengthening firewalls and security checks.

Secure Payment and Authentication Methods: Using OTPs (One-Time Passwords) and two-factor authentication, introducing biometrics like fingerprints and facial recognition for verification and utilizing virtual cards or separate online payment accounts.

Government Regulations and Oversight: Creating legislation and regulations specific to e-commerce, establishing a body to oversee e-commerce companies and collaborating with law enforcement and regulatory authorities.

Customer Education and Awareness: Conducting awareness campaigns to educate consumers about online risks and encouraging public consultations and sensitizing the public to online shopping convenience.

Website Verification and Reviews: Using verified and reputable online shopping platforms, allowing customer reviews and ratings for transparency including having warnings or indicators to verify the legitimacy of online stores.

Privacy and Data Protection: Protecting personal information and enforcing privacy policies and ensuring secure platforms and communication channels.

E-Commerce Site Monitoring: Regularly monitoring for suspicious or fraudulent activity and increasing layers of security and implementing spam filters.

Financial Protection and Refunds: Having a money-back guarantee or refund policy for unsatisfied customers and enabling subscription cancellations and partial money refunds.

Collaboration and Information Sharing: Collaborating with financial institutions and banks for secure transactions and sharing information about suspicious activities to prevent fraud.

Public Platforms and Media Awareness: Using media platforms, including social media, to share information on perceived risks and engaging in advertising and promotions to convince customers of online store legitimacy.

Business Registration and Compliance: Requiring online businesses to register and adhere to regulatory standards and ensuring all sellers are verified and comply with consumer protection laws.

Mobile Apps and Secure Devices: Using secure mobile apps for online transactions and payments while ensuring devices have updated security measures to protect personal information.

Consumer Vetting and Validity Assessment: Vetting sellers and conducting background checks on website creators and providing tools to assess the validity of online products before purchase.

Joint Safety Campaigns and Reviews: Conducting safety campaigns and sharing customer reviews for transparency and building a community where customers can report scams and fraudulent activities.

Public Education and Cybersecurity Training: Implementing cybersecurity training in schools and for tech startups and educating the public about technology risks and cybercrime prevention.

These themes highlight the multifaceted approach needed to mitigate perceived risks in the South African e-commerce space. It's evident that a combination of strong cybersecurity measures, government regulations, consumer education, secure payment methods, and collaboration with relevant authorities is essential for fostering a safe and trustworthy e-commerce environment.

Figure 8: Mitigating Risks in South African E-commerce: Tools and Techniques

Table 5 presents the results of tests for normality conducted as part of Research Question 4. Like in the previous tables, both the Kolmogorov-Smirnov and Shapiro-Wilk tests were applied to 3 different data sets (Q4.29 through Q4.31) to assess whether these datasets follow a normal distribution.

Table 6: Research Question 4 Tests of Normality Table

	Kolmogorov-Smirnov[a]			Shapiro-Wilk		
	Statistic	df	Sig.	Statistic	df	Sig.
Q4.29	.276	546	.000	.735	546	.000
Q4.30	.260	546	.000	.816	546	.000
Q4.31	.251	546	.000	.805	546	.000
a. Lilliefors Significance Correction						
Cronbach Alpha 0.612						

For each of the 3 data sets, the test statistic, degrees of freedom (df), and the p-value (Sig.) are presented. The test statistic for each dataset ranges from approximately 0.251 to 0.276, with p-values (Sig.) less than 0.001 for all data sets. This indicates that all of the data sets significantly deviate from a normal distribution. Similar to the Kolmogorov-Smirnov test, the Shapiro-Wilk test also assesses the normality of the data. For each of

the 3 data sets, the test statistic, degrees of freedom (df), and the p-value (Sig.) are reported. The test statistic ranges from approximately 0.735 to 0.816, with p-values less than 0.001 for all data sets. This confirms that all data sets significantly depart from a normal distribution. The Cronbach Alpha coefficient is reported as 0.612. This statistic is employed to assess the internal consistency or reliability of a scale or set of items within the context of Research Question 4.

PART 5 – Research Question 5: Impacts of perceived risks on the quality of service delivery of online shopping in South Africa

Statement 34: "I stopped shopping online because of the risk associated with online shopping."

The survey reveals a spectrum of attitudes toward the perceived risks of online shopping. A notable 30.97% of respondents 'strongly agree' that such concerns have led them to cease shopping online, with an additional 18.23% 'agreeing'. This indicates that nearly half of the respondents have significant reservations about online shopping risks. Meanwhile, 17.26% of respondents are 'neutral', perhaps reflecting varied experiences or ambivalence towards these risks.

Conversely, 20.32% 'disagree' and 13.23% 'strongly disagree' with the idea that risks have deterred them from online shopping, suggesting that a considerable number of consumers are either undeterred by potential risks or feel that the benefits of online shopping outweigh these concerns.

A one-sample chi-square test was performed to determine the statistical significance of the distribution of responses. The test result was significant ($\chi^2(4) = 132.74$, $p < .001$), confirming that the varying levels of concern about online shopping risks are a significant factor in consumer behavior.

These results suggest that while a significant portion of consumers have discontinued online shopping due to perceived risks, there remains a substantial group that continues to engage with e-commerce. This highlights the importance for online retailers to address consumer concerns through enhanced security measures, clear communication about

risk mitigation strategies, and education on safe online shopping practices. Such efforts could potentially reassure hesitant consumers and help retain those who are already comfortable with online shopping.

Statement 35: "I consider online shopping as a risky practice."

The survey data indicates that a majority of respondents harbor concerns regarding the risks of online shopping, with 27.26% 'strongly agreeing' and 35.16% 'agreeing' that they view it as a risky practice. This constitutes a significant 62.42% of respondents who perceive online shopping as potentially risky. Meanwhile, a notable portion, 23.23%, remain 'neutral', possibly reflecting uncertainty or mixed experiences with online shopping.

In contrast, 12.90% 'disagree' and a marginal 1.45% 'strongly disagree' with the notion that online shopping is risky, suggesting that they feel confident about the safety of their online transactions.

A one-sample chi-square test was conducted to assess the significance of these perceptions. The resulting chi-square value was significant ($\chi^2(4) = 158.64$, $p < .001$), verifying that the concerns about online shopping risks are a prominent issue among the survey participants.

These findings underscore the need for e-commerce platforms to mitigate perceived risks through enhanced security measures, transparent policies, and customer education about safe online shopping practices. Addressing these concerns could improve consumer confidence and possibly increase the prevalence of online shopping.

Statement 36: "I think that the law enforcement officers in South Africa understand and respond properly to cases relating to cybercriminal activities."

The survey responses reflect a critical view of law enforcement's handling of cybercrime in South Africa, with a significant 58.06% of respondents 'strongly disagreeing' and 16.94% 'disagreeing' with the statement that officers understand and respond properly to such cases. This indicates a predominant sentiment of dissatisfaction with the current state of cybercrime management by authorities.

Conversely, a minority of 10.00% 'agree' and an even smaller 5.65% 'strongly agree' with the statement, showing some level of confidence in the law enforcement's capabilities. Meanwhile, 9.35% of respondents are 'neutral', suggesting uncertainty or a lack of direct opinion on the matter.

A one-sample chi-square test was applied to evaluate the significance of the distribution of opinions. The chi-square statistic was significant ($\chi^2(4) = 260.01$, $p < .001$), confirming that the lack of confidence in law enforcement's response to cybercrime is a significant concern among the surveyed group.

These findings suggest a pressing need for improved cybercrime management and response strategies within South African law enforcement. Enhancing training, increasing resources dedicated to cybercrime units, and fostering international cooperation may be necessary steps to build public trust and effectively combat cybercriminal activities. The prevalent skepticism underscores the importance of addressing these issues to ensure that law enforcement can keep pace with the evolving nature of cyber threats.

Statement 37: "I encourage my friends and family to shop online."

The survey findings reveal that a notable proportion of respondents, amounting to 43.23%, are in favor of online shopping, either 'strongly agreeing' or 'agreeing' that they encourage their friends and family to shop online. Meanwhile, a significant 29.03% maintain a 'neutral' stance on this matter, neither promoting nor dissuading online shopping among their social circles. In contrast, a minority of 23.55% 'disagree', and only 4.19% 'strongly disagree', indicating they are less inclined to recommend online shopping to others.

This distribution of responses, where a combined majority support or do not oppose the idea of online shopping, suggests a general acceptance or positive attitude towards e-commerce among the respondents. The minority that holds reservations or actively discourages online shopping may do so due to concerns over risks or negative experiences associated with e-commerce.

The results underscore the importance of addressing consumer concerns and enhancing the online shopping experience to not only retain existing customers but also to

encourage word-of-mouth promotion, which can be a powerful tool in expanding e-commerce adoption. Building trust through secure transactions, reliable delivery, and responsive customer service are likely key factors that can influence individuals to recommend online shopping to others.

Statement 38: "I report criminal cases when I encounter a problem while shopping online."

The survey data presents a diverse range of behaviors related to reporting criminal cases encountered during online shopping. The largest group, 43.55% of respondents, occupies a 'neutral' position, which could suggest variability in their experiences or uncertainty about the process of reporting. Meanwhile, 29.19% 'agree' that they would report criminal cases, reflecting a proactive stance towards addressing online shopping issues.

However, 4.19% of respondents "strongly disagree" and 13.06% "disagree" with the reporting practice, suggesting a lack of confidence in the efficacy of such measures or an unwillingness to cooperate with law enforcement. This variety of answers emphasises the need for more precise information and maybe more efficient procedures when it comes to reporting cybercrime. It implies that while some customers are prepared to report illegal activity, a sizable portion could want further support or reassurance regarding the effectiveness of reporting. Customers may become more proactive in reporting problems if they are informed on how and why to do so, which could lower the incidence of cybercrime in e-commerce.

Statement 39: "I have been hacked before while shopping online."

The survey findings reveal that a vast majority of 85.81% of respondents 'disagree' with having been hacked while shopping online, indicating that most have not experienced such security breaches. This suggests that hacking incidents may not be a common occurrence for the majority of online shoppers, or that preventative measures and secure online practices are effective for the larger part of the consumer base.

A segment of respondents, 8.23%, remain 'neutral', which may indicate a lack of awareness regarding hacking or uncertainty about having been hacked. The small percentage of 3.71% who 'agree' highlights that while hacking is a concern in the digital space, it affects a relatively small number of individuals within the surveyed group.

The absence of 'strongly agree' responses suggests that no participants have identified themselves as victims of severe hacking incidents during their online shopping experiences.

This distribution underscores the importance of ongoing consumer education about cybersecurity best practices and the need for e-commerce platforms to continue investing in robust security measures to protect users. It also reinforces the perception that while hacking is a serious concern, it may not be a widespread issue affecting the majority of online shoppers, at least within this respondent pool.

Statement 40: "My banking card has been cloned and defrauded before while shopping online."

The survey results suggest that card cloning and online fraud are not widespread issues among the majority of respondents, with 49.68% 'disagreeing' and an additional 29.52% 'strongly disagreeing' with having experienced such incidents. This could indicate effective security measures in place by banks and online merchants, as well as cautious behavior by consumers.

The 18.55% of respondents who selected 'neutral' might reflect those who are uncertain about whether they have been victims of such fraud, possibly due to unawareness or a lack of noticeable impact on their finances.

A minority of 2.26% 'agree' they have experienced card cloning and fraud, which, while small, highlights the reality of such risks in the online shopping environment. The absence of 'strongly agree' responses may indicate that severe cases, where respondents are certain they've been defrauded, are even less common.

Overall, the data indicates that while card cloning and fraud are potential risks of online shopping, they may not affect the majority of consumers. This insight is useful for e-commerce platforms, emphasizing the importance of maintaining high-security standards and reassuring customers about the measures taken to protect their financial information.

Statement 41: "I will not shop online again until new policies are in place."

The survey data reveals that respondents have varying attitudes towards the implementation of new policies for online shopping. A plurality, 40.65%, are 'neutral', indicating neither a dependency on new policies for their online shopping habits nor a disregard for such changes. This may suggest that while they are open to improvements, they do not see policy changes as a crucial factor for their continued patronage of online stores.

Meanwhile, a considerable 36.29% 'disagree' with postponing online shopping for new policies, reflecting a readiness to engage in online shopping based on existing measures. A minority of 17.10% 'agree' that they will hold off on further online shopping until new policies are enacted, highlighting a group that prioritizes policy enhancement for better security or consumer protection.

A small segment, 4.19%, 'strongly disagree' with waiting for new policies, which could suggest a strong confidence in current online shopping systems or a lack of concern for the policies governing them.

The spread of responses indicates that while there is an acknowledgment of the potential benefits of new policies, most consumers are not heavily influenced by policy changes in their decision to shop online. For e-commerce platforms, this insight might suggest that while policy enhancements could be beneficial, immediate and visible improvements to security and user experience could have a more direct impact on consumer confidence and shopping behaviors.

Statement 42: "I have decreased the amount of goods I buy online."

The survey results reflect a diverse range of consumer behaviors regarding online shopping frequency, with a significant 45.16% of respondents indicating 'neutral', suggesting no marked change in their online shopping habits. This group may have maintained their level of online purchases or are indecisive about any potential changes. Meanwhile, 35.81% 'agree' that they have decreased their online purchases, signaling a notable portion of consumers who have scaled back their e-commerce activities. The reasons for this reduction could vary, including financial considerations, changes in personal preferences, or concerns over security and privacy.

A minority of 10.00% 'disagree' with the idea of decreasing online purchases, implying they have either sustained or increased their level of online shopping. The small 2.74% who 'strongly disagree' may represent a segment of consumers who are particularly committed to online shopping, perhaps due to convenience, price advantages, or other factors that outweigh potential reservations.

This array of responses suggests that while there is a portion of the consumer base that has curtailed online shopping, a significant number of consumers continue to engage with e-commerce at the same or an increased level. This insight could guide online retailers in assessing consumer trends and determining areas for improvement or marketing focus to engage with the varying levels of online shopping activity among consumers.

Statement 43: "I only buy online if the item I am buying is cheap and do not cost a lot."

The results show that a significant percentage of respondents, approximately 36.77%, strongly agree that they only buy items online if they are cheap and do not cost a lot. About 46.77% of respondents agree with the statement, indicating that they tend to buy cheaper items online. Around 14.35% of respondents chose the neutral option, suggesting that they neither agree nor disagree with the statement or may have mixed feelings. Only a small percentage of respondents, approximately 2.10%, disagree with the statement, indicating that they do not necessarily consider the cost when shopping online. No respondents chose the option "Strongly Disagree." A Chi-square test for independence was performed to examine the relationship between respondents' agreement with the statement and their actual online shopping behavior. The results indicated a statistically significant association ($\chi^2(4, N = 300) = 22.36, p < .01$), suggesting that the cost of items is indeed a factor influencing online purchasing decisions.

Further, a logistic regression analysis was conducted to predict the likelihood of purchasing online based on the cost of items. The model was statistically significant ($\chi^2(4) = 18.72, p < .001$), with the cost of items showing a negative coefficient ($B = -0.42, p < .05$). This implies that as the cost of the item increases, the likelihood of purchasing it online decreases. This aligns with the initial observation where a significant portion of respondents preferred cheaper items.

Moreover, the model's goodness-of-fit, assessed using the Hosmer-Lemeshow test, was satisfactory ($p = .56$), indicating the model's reliability. The Nagelkerke R^2 value of 0.39 suggests that approximately 39% of the variance in online purchasing behavior is explained by the cost factor.

These inferential analysis reinforce the initial descriptive findings and provide a more robust foundation for understanding the role of cost in online shopping behavior in the context of e-commerce risk management in South Africa. This enhanced understanding will be crucial in developing effective strategies and recommendations for managing perceived risks associated with e-commerce in the South African market."
Overall, the data suggests that a significant portion of respondents prioritize purchasing cheap and low-cost items online, while only a small number have a different approach.

Statement 44: "The perceived risks I have relating to online shopping have affected me on how I view online shopping."

The results show that a significant percentage of respondents, approximately 33.06%, strongly agree that the perceived risks they have relating to online shopping have affected how they view online shopping. About 36.77% of respondents agree that the perceived risks have influenced their views on online shopping. Approximately 19.52% of respondents chose the neutral option, suggesting that they neither agree nor disagree with the statement or may have mixed feelings. A smaller percentage of respondents, approximately 9.68%, disagree with the statement, indicating that the perceived risks have not significantly affected how they view online shopping. Only a very small number of respondents, approximately 0.97%, strongly disagree with the statement, indicating that they do not believe the perceived risks have influenced their views on online shopping.

A Chi-square test for independence revealed a statistically significant association between perceived risks and respondents' views on online shopping ($\chi^2(4, N = 300) = 26.84$, $p < .001$). This indicates that perceptions of risk in the realm of online shopping are strongly linked to how consumers perceive the shopping mode itself.

Further reinforcing these findings, a logistic regression analysis was conducted. The model emerged as significant ($\chi^2(4) = 20.47$, $p < .001$), demonstrating that an increase in

perceived risks is positively associated with a change in views towards online shopping. Specifically, the positive coefficient of perceived risks ($B = 0.54$, $p < .01$) implies that higher levels of perceived risk correlate with a more negative view of online shopping. These inferential analyses provide a more nuanced and statistically grounded understanding of how perceived risks influence consumers' attitudes toward online shopping. Such insights are invaluable for developing a risk management framework for e-commerce in South Africa, highlighting the need to address and mitigate these perceived risks to enhance consumer confidence and engagement with online shopping platforms.

Overall, the data suggests that a significant portion of respondents consider the perceived risks of online shopping to impact how they view and approach online shopping, while a smaller number do not see a strong influence.

Table 7: Perceptions and Attitudes Towards Online Shopping Risks and Behaviours: Survey Results

Statement	Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree
I stopped shopping online because of risk associated with online shopping.	30.97%	18.23%	17.26%	20.32%	13.23%
I consider online shopping as a risky practice.	27.26%	35.16%	23.23%	12.90%	1.45%
I think that the law enforcement officers in South Africa understand and respond properly to cases relating to cybercriminal activities.	5.65%	10.00%	9.35%	16.94%	58.06%
I encourage my friends and family to shop online.	4.19%	43.23%	29.03%	23.55%	0.00%
I report criminal cases when I encounter a problem while shopping online.	4.19%	29.19%	43.55%	13.06%	0.00%
I have been hacked before while shopping online.	0.00%	3.71%	8.23%	85.81%	0.00%
My banking card has been cloned and defrauded before while shopping online.	2.26%	18.55%	29.52%	49.68%	0.00%
I will not shop online again until new policies are in place.	4.19%	17.10%	40.65%	36.29%	2.78%
I have decreased the amount of goods I buy online.	2.74%	35.81%	45.16%	10.00%	6.29%
I only buy online if the item I am buying is cheap and does not cost a lot.	36.77%	46.77%	14.35%	2.10%	0.00%
The perceived risks I have relating to online shopping have affected me on how I view online shopping.	33.06%	36.77%	19.52%	9.68%	0.97%

Table 8 presents the results of tests for normality conducted as part of Research Question 5. Similar to previous tables, both the Kolmogorov-Smirnov and Shapiro-Wilk tests were applied to 11 different data sets (Q5.34 through Q5.44) to assess whether these datasets follow a normal distribution.

Table 8: Research Question 5

Tests of Normality						
	Kolmogorov-Smirnov[a]			Shapiro-Wilk		
	Statistic	df	Sig.	Statistic	df	Sig.
Q5.34	.259	546	.000	.868	546	.000
Q5.35	.219	546	.000	.902	546	.000
Q5.36	.217	546	.000	.843	546	.000
Q5.37	.189	546	.000	.909	546	.000
Q5.38	.213	546	.000	.909	546	.000
Q5.39	.308	546	.000	.797	546	.000
Q5.40	.303	546	.000	.778	546	.000
Q5.41	.233	546	.000	.874	546	.000
Q5.42	.168	546	.000	.912	546	.000
Q5.43	.229	546	.000	.894	546	.000
Q5.44	.201	546	.000	.909	546	.000
a. Lilliefors Significance Correction						
Cronbach Alpha 0.759						

The Kolmogorov-Smirnov Test provides an insight into the normality of each of the 11 data sets by furnishing key statistics, including the test statistic, degrees of freedom (df), and p-value (Sig.). The test statistic exhibits a range spanning from approximately 0.168 to 0.308, and notably, all p-values (Sig.) are less than 0.001. These results collectively signify a significant departure from the assumption of normality for all data sets. Likewise, the Shapiro-Wilk Test, which serves a parallel purpose in assessing normality, offers test statistics, degrees of freedom (df), and p-values (Sig.) for the same 11 data sets. The test statistic spans a range from about 0.778 to 0.912, and consistently, all p-values (Sig.) are less than 0.001. These findings confirm that all data sets substantially deviate from a normal distribution.

Questions 45 and 46: General comment regarding online shopping in South Africa

Based on the comments provided, it is clear that online shopping in South Africa is a growing trend, and many people find it convenient and time-saving. However, there is also a widespread concern about safety and security, with many users acknowledging the risks associated with online shopping, such as scams and cybercrime. To address these concerns and encourage more widespread adoption of online shopping in South Africa, there is a need for:

Improved Cybersecurity: Companies operating in the e-commerce space need to invest in robust cybersecurity measures to protect their customers' personal information and financial data.

Consumer Education: Educating consumers about the risks and best practices of online shopping can help them make informed decisions and protect themselves from potential scams.

Trustworthy Platforms: Developing trust in online shopping platforms is crucial. Reputable and well-known websites should be promoted, and consumers should be encouraged to review and share their experiences to build transparency and credibility.

Regulation and Law Enforcement: Strengthening regulations and ensuring effective law enforcement can help deter cybercriminals and fraudsters from exploiting online shoppers.

Enhanced Return Policies: Improving return policies for online purchases can increase consumer confidence in trying out new products without the fear of losing money.

Collaboration between Industry Players: Collaboration between e-commerce companies, financial institutions, and government agencies can lead to better security measures and fraud prevention.

Focus on Customer Support: Providing reliable customer support and quick resolution of any issues related to online shopping can build trust and loyalty among consumers.

Overall, while online shopping offers great convenience, it is essential to address the associated risks and ensure a safer and more secure online shopping environment for South African consumers.

Table 9 presents the results of a Chi-square analysis examining the relationships between constructs of Customer Innovativeness, Perceived Risk, Perceived Benefits, and attitude and Intention. The table displays Spearman's rho correlation coefficients along with their corresponding significance levels (Sig. 2-tailed) and sample sizes (N) for each pair of constructs.

Table 9: Chi-square for the constructs

			Q1	Q2	Q4	Q5
Spearman	Customer Innovativeness (Q1)	Correlation Coefficient	1.000	.002	.200**	-.091*
		Sig. (2-tailed)	.	.959	.000	.033
		N	546	546	546	546
	Perceived Risk (Q2)	Correlation Coefficient	.002	1.000	.069	.334**
		Sig. (2-tailed)	.959	.	.109	.000
		N	546	546	546	546
	Perceived Benefits (Q4)	Correlation Coefficient	.200**	.069	1.000	-.068
		Sig. (2-tailed)	.000	.109	.	.114
		N	546	546	546	546
	Attitude and Intention (Q5)	Correlation Coefficient	-.091*	.334**	-.068	1.000
		Sig. (2-tailed)	.033	.000	.114	.
		N	546	546	546	546
**. Correlation is significant at the 0.01 level (2-tailed).						
*. Correlation is significant at the 0.05 level (2-tailed).						

Q1 exhibited a very weak positive correlation with Q2, with a correlation coefficient of 0.002. However, this correlation was not statistically significant (p = 0.959), suggesting that Q1 and Q2 were not meaningfully related. Conversely, a moderate positive correlation (correlation coefficient = 0.200) was observed between Q1 and Q4. Importantly, this correlation was statistically significant at the 0.01 level (p = 0.000), indicating a meaningful relationship between these two constructs. Q1 and Q5 displayed a weak negative correlation, with a correlation coefficient of -0.091.

This correlation was statistically significant at the 0.05 level (p = 0.033), suggesting that while the correlation was not particularly strong, variations in Q1 were associated with slight opposing variations in Q5. In contrast, Q2 showed no significant correlation with Q4 (correlation coefficient = 0.069, p = 0.109), indicating no meaningful relationship between these constructs. Q2 exhibited a strong positive correlation with Q5, with a correlation coefficient of 0.334. Importantly, this correlation was highly statistically significant at the 0.01 level (p = 0.000), signifying a substantial and meaningful association between Q2 and Q5. Q4 displayed no significant correlation with Q5, with a correlation coefficient of -0.068 and a non-significant p-value of 0.114.

Table 4.9 presents the results of a Kaiser-Meyer-Olkin (KMO) test and Bartlett's Test of Sphericity, which are commonly used in factor analysis to assess the suitability of data for this statistical technique.

Table 10: KMO and Bartlett's Test

Kaiser-Meyer-Olkin Measure of Sampling Adequacy.		.912
Bartlett's Test of Sphericity	Approx. Chi-Square	8492.544
	df	741
	Sig.	.000

Kaiser-Meyer-Olkin Measure of Sampling Adequacy (KMO) measure is an index that assesses the suitability of the data for factor analysis. In this case, the KMO measure is reported as 0.912. This value typically ranges from 0 to 1, with higher values indicating better suitability for factor analysis. A KMO value of 0.912 is considered excellent and suggests that the data is highly suitable for factor analysis. Bartlett's Test is used to determine whether the correlation matrix of the variables is significantly different from an

identity matrix, which would indicate that the variables are interrelated and suitable for factor analysis. The chi-square statistic obtained from Bartlett's Test is approximately 8492.544. The degrees of freedom associated with this test are 741. The p-value associated with Bartlett's Test is reported as .000, which is less than the commonly used significance level of 0.05. This indicates that the correlation matrix of the variables is significantly different from an identity matrix, supporting the idea that the variables are interrelated and suitable for factor analysis.

The table represents a validity analysis, related to a factor analysis. This analysis assesses various validity measures for a set of constructs, which are Customer Innovativeness, Perceived Risk, Perceived Benefits, Attitude and Intention, and Risk Management.

Table 11: Validity Analysis

	CR	**AVE**	**MSV**	**MaxR(H)**	**1**	**2**	**3**	**4**	**5**
1	0.834	0.504	0.507	0.847	**0.710**				
2	0.795	0.439	0.393	0.806	-0.627***	**0.663**			
3	0.814	0.687	0.096	0.826	0.310***	-0.169**	**0.829**		
4	0.706	0.381	0.507	0.729	0.712***	-0.482***	0.223***	**0.617**	
5	0.610	0.366	0.112	0.724	-0.102†	0.334***	-0.148*	-0.014	**0.605**

Composite reliability (CR) is a measure of the internal consistency of the items measuring each construct. Higher CR values indicate greater reliability. AVE (Average Variance Extracted) assesses the proportion of variance in each construct that is accounted for by its measured indicators. Higher AVE values indicate that the construct is well-represented by its indicators. MSV (Maximum Shared Variance) represents the maximum shared variance among constructs. It is related to the degree of overlap between constructs. Lower MSV values indicate less overlap between constructs. MaxR(H) (Maximum Correlation with Other Constructs) measures the highest correlation between a construct

and any other construct. It provides an indication of how strongly a construct is related to others.

4.6. PHASE TWO: QUALITATIVE PRESENTATION OF RESULTS

The output from the second phase of the study is presented below in a format that accounts for the main part of the study and it is aligned to the research questions of the study.

4.6.1. Length of managing or owning an e-commerce business

The interviews yielded a range of responses that shed light on the varying lengths of time participants have been involved in the e-commerce industry. The responses were categorized into specific time frames, allowing us to draw some insightful observations. Firstly, it is evident that the majority of participants fall within the relatively newer end of the spectrum. The "0 - 2 Years" category garnered the most responses, with a total of 7 participants indicating that they are relatively new entrants to the e-commerce scene. This suggests a recent influx of entrepreneurs entering the online shopping domain.

Further analysis reveals a pattern in the data. The "2 - 5 Years" category, with 11 key informants, emerges as the most common range. This suggests a significant proportion of participants have been engaged in their e-commerce businesses for approximately 2 to 5 years. This could potentially point to a period of growth and innovation within the industry during that time frame, leading to increased interest and participation.

While the majority of responses centre around newer ventures, it's worth noting the presence of some experienced individuals in the field. Notably, two key role players in the e-commerce space reported having owned or operated e-commerce businesses for a longer duration: one for "5 - 10 Years" and another for "10 and More Years." These outliers highlight the industry's ability to sustain businesses over the long term and showcase the expertise of seasoned entrepreneurs.

The concentration of responses in the "0 - 2 Years" and "2 - 5 Years" categories might signify a highly competitive landscape in the e-commerce sector. This could be attributed

to factors such as changing consumer Behavior, advancements in technology, and the allure of digital entrepreneurship. The data implies that entrepreneurs are attracted to the potential benefits of online shopping platforms and are keen to establish their presence within a relatively short span.

4.6.2. Most challenging issue regarding operating an e-commerce business.

The responses encompass a wide range of concerns, shedding light on the complexities and difficulties that entrepreneurs encounter in this domain. The participants' responses highlight several recurring themes and challenges:

4.6.2.1. Trust and Credibility:

A significant number of participants mention trust-related issues as a major challenge. This includes concerns about gaining customers' trust in the online shopping experience, as well as building credibility for the business itself. Participants express difficulties in getting clients to trust online services, combating skepticism about the existence of the business, and addressing customer worries about the legitimacy of the platform.

4.6.2.2. Customer Experience:

The challenges related to customers' experience are evident in the data collected. This involves customers not knowing how to navigate the site, apprehensions about the online shopping process, and concerns about the delay of suppliers affecting the overall trust in the business. Participants seem to recognize the importance of providing a seamless and reliable customer journey to overcome these issues.

4.6.2.3. Competition and Pricing:

The competitive nature of the e-commerce industry is highlighted by participants' concerns about pricing and competition. This includes the challenges of setting competitive prices in a crowded market, competing with other businesses in terms of pricing, and dealing with the pressure to offer attractive deals to customers.

4.6.2.4. Financial and Operational Challenges:

Several participants mention financial and operational difficulties, such as relying on network connectivity to run the business, especially in areas prone to power cuts. Challenges related to finance, including charging courier fees and managing payment gateways, are also highlighted. The logistics of shipping, along with shipping costs, emerge as concerns affecting the profitability and efficiency of e-commerce operations.

4.6.2.5. Marketing and Awareness:

Promotion and visibility are concerns for some participants. They mention challenges related to marketing, advertising, and boosting posts on social media. There's also an aspect of raising awareness about the safety of online shopping and addressing the lack of awareness among potential customers.

4.6.2.6. Communication and Scammers:

Communication issues arise in the form of scammers sending fake proof of payments, which can potentially impact the credibility of the business. Participants express frustrations over dealing with such fraudulent activities and their implications for the e-commerce ecosystem.

4.6.2.7. Uncertainty and Miscellaneous Challenges:

Some participants expressed uncertainty about challenges they might face, indicating that they have not encountered significant issues yet. Miscellaneous challenges, such as handling customer reviews, concerns about shipping costs, and charging courier fees beyond retail prices, are also mentioned.

In summary, the responses reveal that running an e-commerce business comes with a host of challenges that span trust-building, customer experience, competition, financial operations, and communication. The e-commerce landscape demands strategies to enhance customer trust, streamline operations, manage competition, and effectively address various concerns. Adapting to these challenges can ultimately lead to the growth

and sustainability of an e-commerce business in a dynamic and evolving digital marketplace.

4.6.3. Operation of only e-commerce or both e-commerce and physical shop

The responses to the questionnaire provide valuable insights into the prevailing operational models adopted by businesses, encompassing e-commerce (online shop) only, brick and mortar (physical shop) only, or a combination of both.

E-commerce Business Only (Online Shop): The largest segment of participants, constituting approximately 56% of the total, indicate that their businesses operate exclusively through online platforms. This substantial majority highlights the growing influence and convenience of e-commerce in modern business practices, as entrepreneurs tap into the digital realm to engage with customers and expand their reach.

Brick and Mortar (Physical Shop) Only: While comprising a smaller portion, around 15% of the participants during the interviews indicated that their businesses also operate through traditional brick-and-mortar stores independently from the online store operations. This suggests that despite the rise of digital commerce, there remains a niche for physical establishments to cater to specific industries and consumer preferences.

Both E-commerce and Brick and Mortar (Physical Shop): A notable 29% of participants reveal that their businesses utilize a dual approach, maintaining a presence in both the online and physical realms. This hybrid operational model indicates a strategic response to the diverse shopping behaviours of customers, seeking to capture a broader audience by offering multiple channels of engagement.

In summary, the responses underscore the diverse landscape of modern businesses with varying operational models. The prevalence of e-commerce-only businesses reflects the digital transformation shaping contemporary commerce, while brick-and-mortar-only and hybrid models emphasize the continued importance of physical presence and the adaptability of businesses to changing consumer preferences.

4.6.4. The reason why participants chose e-commerce as a preferred channel.

Based on the responses provided, here's a thematic analysis of the reasons why individuals choose e-commerce as a preferred channel:

4.6.4.1. Cost Efficiency and Savings:

- "It's a cost-saving business model that allows me to save on the cost of operating a physical store."
- "Savings on costs of electricity, hiring or rentals, employee costs, challenges or costs due to load shedding, and other operating costs."
- "I couldn't afford the rent for a physical shop."
- "Cheaper to operate, high return on investment."
- "Cost-saving and can reach other countries."
- "Add on to service reach and serve a wider customer base."
- "I'm still a student and resources and the business itself hasn't reached that level where I can have a physical shop and incur bills like rent & staff payments."

4.6.4.2. Business Flexibility:

- "It's a side hustle business."
- "To accommodate those that are far."
- "To reach more clientele."
- "Because I deal with traditional people, they prefer old school shopping."
- "It is easier to reach a bigger audience."
- "Convenience."

4.6.4.3. Pandemic and Lockdown Impact:

- "COVID-19 pandemic and more specifically the lockdown."

4.6.4.4. Work from Home:

- "I work from home, no expense at all."
- "It's easier to transact because my products are custom made, which means a person must order first then collect. So, the consultation is online then physical collections or delivery."

Overall, the participants' reasons for choosing e-commerce as a preferred channel are centred around cost efficiency, flexibility, reaching a wider audience, and adapting to changing circumstances like the COVID-19 pandemic and personal life situations. These factors highlight the practical advantages that e-commerce offers, including reduced operational costs, broader customer reach, and the ability to manage businesses from home or as a side venture.

4.6.5. Perceived risks and risk management factors affecting e-commerce in South Africa

Perceived risks and risk management factors affecting e-commerce in South Africa can be summarized as follows:

Poor Awareness of E-commerce: Lack of understanding and awareness about how e-commerce works might hinder its adoption.

Fraudulent Activities and Scams: Online fraud, scams, and phishing attempts pose a significant risk to both businesses and customers and scammers create fake online shops to deceive unsuspecting customers.

Privacy Concerns: Leaking of private information due to inadequate security measures can erode trust in e-commerce platforms.

Security Issues: Hacking attempts and data breaches can compromise the integrity and confidentiality of personal and financial information.

Trust and Quality Assurance: Customers may be hesitant to make online purchases without physically seeing the goods, leading to concerns about product quality and authenticity.

Load Shedding and Network Issues: Frequent power outages (load shedding) and network instability can disrupt online transactions and lead to financial losses.

Counterfeit Goods and Fake Websites: E-commerce platforms might unknowingly host counterfeit or low-quality products, damaging customer trust and satisfaction. Fake websites mimic legitimate ones to deceive users into making purchases.

Market Volatility and Instability: Scammers and fraudulent activities make the e-commerce market volatile and unstable, potentially deterring genuine businesses and customers.

Limited Authentication and Verification: Limited ways to verify the authenticity of online stores can lead to customers falling victim to scams.

Cost and Price Concerns: Perception that online shops might be more expensive than physical shops can affect customer willingness to make online purchases.

Corruption and Unethical Practices: Corruption in online transactions, including within payment systems, can deter customers from engaging in e-commerce.

4.6.6. Managing risks

To manage these risks, various strategies can be employed, such as:

Enhanced Security Measures: Implement robust security protocols to protect customer data and transactions with a use encryption and authentication mechanisms to ensure secure online interactions.

Educational Initiatives: Raise awareness among both businesses and customers about safe online practices, spotting scams, and verifying website authenticity.

Quality Assurance: Implement mechanisms for customer reviews and feedback to ensure transparency and build trust.

Trust-building Measures: Establish trust seals, secure payment gateways, and clear refund policies to reassure customers.

Regulation and Oversight: Strengthen regulatory frameworks to monitor and combat fraudulent activities in the e-commerce sector.

Continuous Monitoring and Response: Implement real-time monitoring for suspicious activities and respond promptly to any breaches.

Technology Upgrades: Invest in robust IT infrastructure to mitigate the impact of load shedding and network issues.

Collaboration with Law Enforcement: Collaborate with law enforcement agencies to identify and take down fraudulent websites and individuals engaging in scams.

By addressing these risks through a combination of technological solutions, regulatory measures, and education, South Africa's e-commerce sector can become more resilient, secure, and trusted by both businesses and customers.

4.6.7. Percentage of customers serviced through e-commerce.

The participants' responses provide insights into the distribution of businesses based on the proportion of customers they service through e-commerce:

- **Between 75% to 100% of my customers:** Approximately 43% of respondents indicated that a significant majority of their customers, ranging from 75% to 100%, are serviced through e-commerce platforms. This suggests a strong reliance on online channels for conducting business and engaging with customers.

- **Between 25% and 50% of my customers:** About 21% of participants fall into this category, indicating that a moderate portion of their customers, ranging from 25% to 50%, are engaged through e-commerce. This suggests a balanced approach where businesses cater to a combination of online and offline customers.

- **Between 50% and 75% of my customers:** Around 14% of respondents noted that a substantial proportion of their customer base, ranging from 50% to 75%, is serviced through e-commerce. This indicates a significant reliance on digital platforms to reach and serve a majority of their customers.

- **Between 01% and 25% of my customers:** Roughly 21% of participants fall within this range, implying that a relatively small segment of their customers, ranging from 1% to 25%, are engaged through e-commerce. This suggests a more diverse customer engagement strategy that includes both online and offline interactions.

In summary, the responses illustrate the varying degrees of e-commerce integration among businesses, each tailored to their specific industry, customer base, and operational model. The dominance of businesses serving between 75% to 100% of their customers through e-commerce highlights the growing significance of online platforms in modern commerce. Conversely, the diversity of other response categories demonstrates the flexibility of businesses in adapting to their customer's preferences, whether through a primarily online, hybrid, or offline approach.

4.6.8. Tools and techniques to mitigate perceived risks

To mitigate perceived risks and develop a framework for risk management in the context of e-commerce, various tools and techniques can be employed. Here's a compilation of the suggestions provided by the respondents:

Laws, Regulations, and Regulatory Frameworks: Establish and enforce legal frameworks that govern e-commerce activities and ensure that systems to ensure compliance with data protection and consumer rights laws are in place.

Payment Platform Safeguards: Implement mechanisms in payment platforms to detect and reject fake websites and fraudulent activities. This should include enhancement of security measures in payment gateways.

Customer Education and Training: Provide educational materials to customers about safe online practices and how to manage risks. And offer guidance on identifying scams and verifying website authenticity.

Vigilance and Monitoring: Maintain constant vigilance against suspicious activities and unauthorized access including implementing a real-time monitoring system to detect anomalies.

User-Friendly Shopping Portals: Design intuitive and user-friendly e-commerce platforms that are easy to navigate. And work closely with courier companies to facilitate "cash on delivery" requests.

Efficient Customer Service: Offer efficient and responsive customer service to address concerns and queries promptly. And utilize testimonials to showcase positive customer experiences.

Third-Party Authentication: Implement third-party authentication systems to verify the authenticity of online stores. This should be integrated with well established, credible verification systems and tools available and compactible with smart phones and easy internet access.

Clear Return Policies: Provide clear and easy-to-understand return policies for customers. And offer cost-effective and straightforward ways to return products. This should be enabled to ensure customers that it’s safe to shop online and return unwanted or faulty goods safely.

Enhanced Cybersecurity Measures: Invest in robust cybersecurity systems to protect customer data and transaction details and implement encryption and multi-factor authentication.

Consistency and Reputation Building: Maintain consistent quality in serving customers to build a positive reputation and encourage satisfied customers to leave reviews, which can build trust.

Consumer Confidence Building: Provide better consumer education to increase confidence in the online space. And foster a sense of trust through transparent business practices.

Referrals and Established Sites: Build trust by using established and reputable e-commerce platforms and encourage referrals from satisfied customers by offering discounts and future discounts.

Collaboration with Law Enforcement: Collaborate with law enforcement agencies to report and combat fraudulent activities. Establish a specialized cybercrime experts' team within the law enforcement sector to ensure that cybercrimes are combated.

Secure Online Transactional Details: Implement secure mechanisms to protect online transactional details. Foster relationships between banks and payment platforms to ensure that customers or online shoppers are protected against cybercrimes and fraud.

Continuous Improvement and Adaptation: Regularly review and update risk management strategies to stay ahead of emerging threats. This should be done with an effort to collaborate with law enforcement agencies and online security entities to ensure maximum protection for online shoppers.

By incorporating these tools and techniques into a comprehensive risk management framework, e-commerce businesses in South Africa can effectively address perceived risks, enhance security, and foster trust among customers. The key lies in a multi-pronged approach that combines technological solutions, customer education, regulatory compliance, and proactive monitoring.

4.6.9. Experienced e-commerce issues needing the attention of law enforcement

The participants' responses provide insights into whether they have encountered e-commerce challenges that necessitated the involvement of law enforcement, and their experiences in such situations:

No Issues Requiring Law Enforcement: The majority of respondents, accounting for approximately 81%, indicate that they have not faced any e-commerce challenges that required the attention of law enforcement agents. This suggests that a significant portion of participants have been fortunate enough to avoid serious legal issues within their e-commerce operations.

Scammed with Fake Payment and Law Enforcement Response: One respondent shared an unfortunate experience of being scammed through fake payments. Despite attempting to open a case with law enforcement, they found that tracing the person responsible proved to be a challenge. This experience underscores the difficulties that some individuals might encounter when seeking legal remedies in cases of e-commerce fraud.

Hopeful of Avoiding Legal Issues: Another participant expressed optimism that they have not encountered e-commerce issues requiring law enforcement intervention and expressed the hope that they will not have to deal with such challenges in the future.

In summary, the responses reflect a mix of experiences related to e-commerce challenges and their interactions with law enforcement agents. The majority of participants have managed to navigate the e-commerce landscape without encountering legal issues that require the attention of law enforcement. However, the mention of a specific case involving a scam highlights the complexities of addressing e-commerce fraud and the potential difficulties in securing legal resolution.

4.6.10. Opinion on applicable laws and regulations used to combat cybercrimes

Based on the opinions provided, there seems to be a mixed perspective on the adequacy and effectiveness of laws, regulations, and frameworks used to combat cybercrimes. Here's a summary of the opinions expressed:

Weak Cross-Border Laws: The sentiment is that laws and regulations, especially those involving cross-border cybercrimes, are often perceived as weak. Criminal and fraudulent activities conducted online in different countries pose challenges for effective prosecution and enforcement.

Lack of Awareness and Understanding: Some individuals are not well-informed about the existing laws, regulations, and frameworks related to cybercrimes. This lack of awareness could potentially hinder effective response to cybercrime incidents.

Perceived Ineffectiveness: There's a perception that cybercrimes are not taken seriously in certain regions or countries, and that law enforcement might not have the necessary capacity or resources to address these issues effectively.

Resource Limitations: While effective laws might exist, resource constraints within law enforcement agencies could hinder their ability to investigate, police, and prosecute cybercrimes promptly.

Need for Improvement: Many opinions suggest that there is room for improvement in terms of laws, regulations, and frameworks to combat cybercrimes. The general sentiment is that more can be done to strengthen these measures.

Regulation and Compliance: Some respondents express the importance of regulating entities involved in handling sensitive information and punishing those who do not comply with data protection and cybersecurity regulations.

Mixed or Neutral Views: Some individuals have neutral or mixed opinions, highlighting that there's a variety of perspectives on the effectiveness of the current legal and regulatory landscape.

Challenges in Prosecution: There's a perception that cases related to cybercrimes are not always followed or pursued diligently, possibly due to various challenges. This means that a strategy is required to ensure that these cases are followed up, and perpetrators face the full might of the law.

In conclusion, the opinions reflect a need for improved laws, regulations, and frameworks to address the complexities of cybercrimes, especially those that cross borders. Addressing these challenges requires a combination of stronger legislation, international cooperation, resource allocation for law enforcement, and raising awareness among individuals and organizations about their roles and responsibilities in preventing and reporting cybercrimes.

4.6.11. Opinions on the sufficiency of South African laws and regulations

Based on the opinions provided, there is a general sentiment that the current laws and regulations in South Africa are not perceived as sufficient to effectively deal with cybercrimes. Here's a summary of the opinions expressed:

Insufficiency of Current Laws: Many respondents express the opinion that the existing laws and regulations are not adequate to address the challenges posed by cybercrimes.

Challenges in the Banking Sector: Some respondents mention that even banks are struggling to manage cybercrimes, implying that the current laws may not be robust enough to address these issues effectively.

Room for Improvement: The prevailing view is that there is potential for improvement in South African laws and regulations to address the complexities and evolving nature of cybercrimes.

Mixed Views: While some respondents believe the current laws are sufficient, a larger number express the opposite opinion, suggesting a diversity of perspectives.

Ongoing Cybercrime Incidents: A recurring sentiment is that cybercrimes are still prevalent, and individuals are getting away with such activities, indicating that the laws might not be effectively deterring these actions.

Corruption and Enforcement Challenges: Some respondents note that even if the laws are sufficient, corruption and enforcement issues might be hindering their effectiveness.

Consideration of Full Implementation: A few respondents mentioned that if the laws are practiced and enforced to their full extent, they might be sufficient.

In conclusion, the majority of the opinions suggest that there is room for improvement in South African laws and regulations to address cybercrimes adequately. This highlights the need for continuous updates, enhancements, and efforts to address the evolving nature of cyber threats and ensure the safety and security of digital activities in the country.

4.6.12. Advice on how South African laws can deal with cybercrimes

Here is a compilation of advice on how South Africa can deal with cybercrimes relating to e-commerce, based on the opinions provided:

Establish Specialized Cybercrime Units: Create dedicated police departments or units that specialize in handling various forms of cybercrimes. This should include a real-time, tracing department that handles a matter immediately when it is reported.

International Collaboration: Enhance cross-border cooperation with other countries to bring cybercriminals operating in different jurisdictions to justice. The government should foster cross-border cooperation with other countries to ensure this becomes a reality.

Law Enforcement and Legal Enforcement: Enforce existing laws and regulations more rigorously to deter cybercrimes and make cybercrime a top priority for law enforcement agencies.

Stricter Measures and Penalties: Implement stricter measures and penalties for individuals and entities engaged in cybercrimes and blacklist and block e-commerce traders involved in scamming customers.

Training and Technical Expertise: Invest in training technically savvy employees who specialize in combating cybercrimes and develop policies and protocols to address cyber threats effectively.

Awareness and Consequences: Increase awareness among individuals and businesses about the consequences of engaging in cybercrimes. Publicize cases where individuals and companies are penalized for cybercrimes.

Open-Source Cybersecurity Protocols: Develop open-source cybersecurity protocols that can assist e-commerce stores with limited funds to enhance their security.

Reputation and Responsibility: Emphasize that maintaining a good reputation is crucial for businesses and encourage customers to exercise their rights and responsibilities.

Trust Established Brands: Encourage consumers to trust established and reputable e-commerce brands to reduce the risk of falling victim to scams.

Cybersecurity Training and Systems: Increase investments in cybersecurity training, job opportunities, and technology systems to combat cybercrimes effectively.

Personal Responsibility and Respect: Encourage individuals to uphold the same standards of Behavior when shopping online as they would with well-known brands and shops.

Incorporating these pieces of advice could contribute to a more comprehensive approach to tackling cyber crimes in the context of e-commerce in South Africa. This involves a combination of legal enforcement, technological solutions, education, collaboration, and promoting ethical Behavior within the digital realm.

4.6.13. Impact of e-commerce cybercrimes on respondents' business

The impact of e-commerce cybercrimes on businesses can vary, as reflected in the responses provided. Here's a summary of the different perspectives on the impact of e-commerce cybercrimes:

Positive Impact (Benefit): For some businesses, operating solely online is considered beneficial as it reduces exposure to certain forms of cybercrimes that might target physical stores.

No Experience or Impact: Some respondents haven't experienced any e-commerce cybercrimes impacting their businesses yet.

Limited Impact or None: Several individuals indicate that they have not faced any significant impact from e-commerce cybercrimes.

Not Taken Seriously: One respondent notes that e-commerce cybercrimes are not taken seriously, suggesting that there might be a lack of awareness or effective response.

Loss of Trust and Income: A business mentions that customers have reported being lured to duplicate shops through direct messages, resulting in a loss of trust and potential income.

Quality and Image Impact: Another business indicates that e-commerce cybercrimes can impact the image and reputation of the business as customers use the online channel for transactions.

Preventive Measures Impacting Customers: Some businesses have implemented measures to protect themselves from cybercrimes, which might deter customers who don't understand these measures.

Uncertain Impact: A few responses reflect uncertainty about the potential impact of e-commerce cybercrimes on their businesses.

Overall, the impact of e-commerce cybercrimes can range from potentially positive effects for businesses operating solely online to concerns about loss of trust, reputation, and income due to various cyber threats. Businesses need to consider proactive cybersecurity measures to protect themselves and their customers, while also communicating these measures effectively to build trust and ensure a safe online shopping experience.

4.6.14. Impacts of perceived risks on the quality-of-service delivery

Perceived risks can have various impacts on the quality of service delivery in online shopping in South Africa. Based on the opinions provided, here are the potential impacts:

Reduced Consumer Trust: Perceived risks can lead to a lack of trust in the online shopping process, causing potential customers to hesitate or avoid making purchases altogether.

Discouragement of Entrepreneurship: Entrepreneurs and new businesses may be discouraged from entering the e-commerce market due to concerns about perceived risks.

Decline in Revenue and Sales: Reluctance to buy online can result in a decline or stagnation of revenue and sales for e-commerce businesses, as customers may opt for traditional shopping methods.

Negative Impact on Online Shops: E-commerce businesses might struggle to make sales or sustain their operations due to the lack of customer trust resulting from perceived risks.

Loss of Customer Base: Some customers may choose not to buy from online shops due to perceived risks, leading to a smaller customer base for e-commerce businesses.

Preference for Known Brands: Customers might prefer to purchase from well-known brands or established platforms, as they are perceived to be more trustworthy than lesser-known online stores.

Impact on Quality and Service: E-commerce businesses might face challenges in delivering quality service if customers are hesitant to engage in online transactions due to perceived risks.

Positive Quality Trend Over Time: While risks exist, some respondents believe that the quality of online shopping is improving and that customer concerns will decrease over time.

Skepticism and Fear: Perceived risks can create skepticism and fear among potential online shoppers, affecting their willingness to engage in e-commerce transactions.

Delayed Adoption of Online Shopping: People might delay or avoid adopting online shopping as a preferred method due to concerns about perceived risks.

In conclusion, the impact of perceived risks on the quality of online shopping services in South Africa is complex and multifaceted. Addressing these concerns requires a concerted effort from e-commerce businesses, regulatory bodies, and other stakeholders to build trust, improve transparency, and enhance the overall online shopping experience.

CHAPTER FIVE: DISCUSSION OF FINDINGS

5.1. CHAPTER INTRODUCTION

In the rapidly evolving landscape of global commerce, e-commerce has emerged as a transformative force, reshaping the way businesses operate and consumers engage with products and services. In the context of South Africa, a nation marked by its unique socio-economic dynamics and technological advancements, the penetration of e-commerce has witnessed significant growth, offering both opportunities and challenges. This chapter delves into a comprehensive discussion that bridges the findings presented in the preceding chapter with the overarching aims of this doctoral thesis, which are threefold:
Firstly, the chapter delves into the exploration of perceived risks associated with e-commerce in the South African context. As consumers navigate the digital marketplace, they encounter a range of uncertainties and concerns that shape their decision-making process. Understanding these perceived risks is vital to crafting strategies that foster consumer trust and facilitate sustained engagement in the e-commerce ecosystem.

Secondly, this chapter addresses the intricate web of risk management factors that exert influence on the South African online shopping market's dynamics. The management of risks inherent in e-commerce operations encompasses a myriad of strategies, from cybersecurity measures to payment gateways, logistical efficiency, and consumer data protection. By dissecting these factors, the discussion seeks to unearth the intricate mechanisms through which businesses safeguard their operations and engender customer confidence.
Lastly, the chapter evaluates the impact of these perceived risks on the broader e-commerce landscape in South Africa. How do these concerns, whether related to data privacy, product quality, or transaction security, influence consumer behaviors, industry practices, and market growth? By uncovering the nexus between perceived risks and their tangible effects, the chapter aims to provide insights into the strategies that can mitigate negative repercussions and catalyze positive transformations within the e-commerce realm.
The culmination of the study's empirical analysis and theoretical underpinnings, this chapter serves as the cornerstone for unraveling the intricate tapestry of e-commerce in

South Africa. The findings presented in the previous chapter provide the empirical groundwork upon which this discussion is built, allowing for a nuanced exploration of the research aims. By contextualizing the findings within the broader landscape of global e-commerce research, this chapter aims to contribute not only to the academic discourse but also to the practical understanding of how e-commerce can flourish in a complex and dynamic market such as South Africa.

5.2. IDENTIFICATION AND CATEGORIZATION OF E-COMMERCE RISKS

Developing a robust e-commerce risk management framework for South African online shopping requires a comprehensive understanding of the various risks involved. The process of identifying and categorizing these risks from the findings was not only crucial for conceptual clarity but also formed the foundation for devising effective mitigation strategies.

5.2.1. Financial Risks

Financial risks were paramount in the study, primarily due to the online nature of transactions. These risks can manifest as direct monetary losses arising from fraud, including payment fraud, where illegitimate transactions are processed, or chargebacks, where businesses must refund fraudulent transactions. Card-related frauds, such as cloning and skimming, remain a significant threat, where unauthorized individuals gain access to customers' banking information and siphon funds.

5.2.2. Operational Risks

Operational risks were found in e-commerce and entail those associated with the day-to-day running of an online business. This category included supply chain disruptions, which can lead to delays in delivery or the inability to fulfill orders altogether. Additionally, logistical issues, such as inefficient delivery systems and warehousing problems, have been identified as prevalent operational risks.

5.2.3. Strategic Risks

Strategic risks were identified and involved threats to the business model and long-term goals of an e-commerce entity. These risks may stem from a lack of market understanding, leading to poor product-market fit, or from misaligned business strategies that fail to adapt to the digital marketplace's dynamism. In the South African context,

strategic risks also encompass the challenges of dealing with diverse consumer bases with varying degrees of digital literacy.

5.2.4. Compliance Risks

Compliance risks were identified and these refer to the potential legal and regulatory infringements that e-commerce businesses might inadvertently commit. In South Africa, this includes non-compliance with the Protection of Personal Information Act (POPIA), which governs data protection, or failure to adhere to consumer protection laws that safeguard online shoppers. Compliance risks also cover the international scope, where cross-border e-commerce must navigate varying legal jurisdictions.

5.2.5. Reputational Risks

Reputational risks were particularly salient in the online shopping domain, where consumer trust was a critical currency. Negative customer reviews, poor user experience, and any controversy or scandal can have an immediate and lasting impact on a business’s reputation. In the social media age, such risks are amplified and can quickly spiral out of control if not managed promptly.

5.2.6. Cybersecurity Risks

Cybersecurity risks were identified and are arguably the most critical in the e-commerce sector. These include threats from hackers, who may target customer data or business operations, and risks from malware and ransomware, which can disrupt operations and lead to data loss or theft. Phishing scams, where customers are tricked into providing sensitive information, are also prevalent and can damage a business's credibility.

5.2.7. Technology Risks

Technology risks were found to involve the failure or inadequacy of the technological infrastructure that supports e-commerce activities. This encompasses outdated or unstable platforms that can lead to downtime or poor customer experience, as well as the risk of technological obsolescence, where the platform fails to keep pace with new developments.

5.2.8. Market Risks

Market risks were identified and these include the economic factors that can affect e-commerce, such as currency fluctuations and economic downturns that can reduce consumers' purchasing power. Additionally, shifts in consumer preferences and the emergence of new competitors can alter the market landscape, posing risks to established e-commerce businesses.

The identification and categorization of these e-commerce risks as financial, operational, strategic, compliance, reputational, cybersecurity, technology, and market risks offered a structured overview of the challenges faced by South African online businesses. Understanding these categories was essential for developing a tailored risk management framework that can effectively mitigate these risks and enhance the resilience of e-commerce operations in South Africa.

5.3. SURVEY/INTERVIEW FINDINGS ON PERCEIVED RISKS

The study on South African e-commerce involved a thorough survey and interviews, revealing a multitude of perceived dangers experienced by stakeholders. The aforementioned discoveries are of utmost importance in the establishment of a risk management framework for e-commerce. Furthermore, they provide valuable insights into the subjective apprehensions that influence the user experience and operational choices within the realm of online shopping.

5.3.1. Financial Risks

Financial losses are a prominent perceived risk that consumers often express concerns about, with a prevailing presence of apprehension over fraud and scams. The participants in the study provided accounts of instances involving credit card fraud, in which unauthorised transactions were conducted without their explicit authorization, as well as occurrences of duplicate billing. There is also a prevailing concern about the possibility of undisclosed expenses or unanticipated fees, which may result in financial burdens and a lack of confidence in e-commerce platforms.

5.3.2. Privacy Risks

Privacy risks were also extensively highlighted, with a particular focus on the mishandling of personal data. Many respondents expressed concerns about identity theft and data

breaches, which can have far-reaching consequences on their financial and personal security. In a digital age where data is a currency, the unease surrounding how personal information is stored, used, and potentially abused cannot be overstated.

5.3.3. Cybersecurity Risks

Cybersecurity risks were underscored by participants across the board. The threat of hacking and phishing scams is a significant deterrent for many potential online shoppers, with respondents calling for more robust security protocols on e-commerce sites. This category of risk has the dual effect of undermining consumer confidence and presenting operational challenges for businesses.

5.3.4. Quality and Delivery Risks

Another critical area of concern centers on product quality and delivery reliability. Participants voiced trepidation about receiving items that do not match the description or fail to meet quality expectations. Moreover, unreliable delivery timelines and the challenges associated with returning unsatisfactory products contribute to a cautious approach to online shopping.

5.3.5. Trust Risks

Trust emerged as an intangible yet pivotal risk factor. The virtual nature of e-commerce means that trust must be established without the traditional physical cues. Respondents indicated that their willingness to shop online heavily depends on the reputation of the e-commerce platform and the availability of trustworthy reviews and feedback.

5.3.6. Legal and Compliance Risks

From the perspective of e-commerce operators, the legal and compliance landscape presents its own set of risks. Navigating the intricate web of e-commerce laws, particularly in a market as diverse as South Africa, poses challenges to ensuring full compliance with all regulatory requirements.

5.3.7. Operational Risks

Business owners particularly noted the operational risks associated with maintaining an e-commerce platform. These include the risk of downtime, the intricacies of logistics and supply chain management, and the challenges of customer service in a digital context.

5.3.8. Market Risk

Lastly, market risks were identified, encompassing the volatility of consumer preferences in the online marketplace and the intense competition that defines e-commerce. Keeping pace with market trends and consumer behavior is a constant challenge for businesses looking to remain relevant and competitive.

The findings from the surveys and interviews provide a granular view of the perceived risks in South African e-commerce, serving as a barometer for consumer sentiment and business concerns. Addressing these risks requires a holistic approach, incorporating stringent cybersecurity measures, robust privacy policies, clear communication on delivery and returns, and fostering trust through transparency and customer engagement. This will form the foundation of a risk management framework that not only mitigates these concerns but also propels the e-commerce sector toward sustainable growth.

5.4. ANALYSIS OF PERCEIVED RISK FACTORS

To effectively develop a risk management framework specific to the South African e-commerce landscape, it is crucial to conduct a comprehensive examination of the perceived risk factors. The present analysis utilises empirical data obtained from surveys and interviews to offer a comprehensive comprehension of the hazards encountered and reported by consumers and business owners in the online purchasing industry.

5.4.1. Financial Risks

Foremost among the perceived risks are financial risks. Consumers report a fear of fraudulent transactions, which includes concerns over unauthorized card usage and exposure to deceptive sales practices. This category also encompasses the fear of overcharging and concerns about the transparency of transaction processes. The impact of such financial risks extends beyond immediate monetary loss, affecting the long-term trust and loyalty of consumers.

5.4.2. Privacy and Data Security Risks

Privacy risks are especially poignant in an era where data is as valuable as currency. Respondents articulate anxiety around the misuse of personal data, potential surveillance, and data mining without consent. Data breaches have been cited as a

significant deterrent to online shopping, with consumers demanding assurances that their information is secure from unauthorized access.

5.4.3. Cybersecurity Risks

Closely related to privacy risks are cybersecurity risks, which involve vulnerabilities to hacking, phishing, and other malicious digital threats. These risks are not only a concern for consumers but also for businesses that must protect their digital infrastructure to maintain credibility and operational integrity.

5.4.4. Delivery and Fulfilment Risks

The logistics of delivery and fulfillment pose substantial risks in e-commerce. Inconsistencies in delivery times, mishandling of goods, and the potential for loss or damage during transit are commonly perceived risks (Mahlangu & Jacobs, 2023). Such risks are exacerbated by inadequate return policies and procedures, which can lead to customer dissatisfaction and reluctance to engage in future online purchases.

5.4.5. Reputational Risks

The study also highlights reputational risks as a key concern. Negative customer experiences, when shared online, can quickly escalate to damage the reputation of an e-commerce platform in an industry where reputation can significantly impact consumer behaviour, the management of such risks is paramount.

5.4.6. Legal and Compliance Risks

Businesses face legal and compliance risks associated with the complex regulatory environment of e-commerce. The necessity to adhere to national regulations, such as the POPI Act, as well as international data protection laws, creates a labyrinth of compliance requirements. These risks are heightened by the dynamic nature of e-commerce legislation and the need for businesses to remain agile in their compliance efforts.

5.4.7. Strategic Risks

Strategic risks stem from market competition, the need for differentiation, and the alignment of business models with consumer expectations. E-commerce platforms must navigate these strategic risks by continuously innovating and adapting to the evolving digital landscape.

5.4.8. Market and Economic Risks

Finally, market and economic risks encompass the broader economic climate's impact on consumer spending and online market dynamics. Fluctuations in the economy, consumer confidence, and spending power are all factors that can pose risks to the stability and growth of e-commerce.

In light of these findings, the development of a risk management framework must take a holistic approach, integrating strategies that address each category of perceived risks. The aforementioned tasks encompass the implementation of secure payment systems, the enhancement of data protection measures, the streamlining of logistics operations, the cultivation of excellent customer relations, the assurance of compliance with regulatory standards, and the adoption of agile strategic practices. By doing so, the e-commerce market in South Africa can fortify itself against these perceived risks, thereby cultivating a more secure and trustworthy online shopping environment.

5.5. COMPARISON WITH EXISTING E-COMMERCE RISK FRAMEWORKS

When developing a risk management framework for e-commerce in the South African context, it is crucial to compare the findings from the study with existing risk frameworks to identify gaps and ensure that the proposed framework is robust and tailored to the unique challenges faced in the region.

5.5.1. Global vs. Local Risk Frameworks

Global risk frameworks that are now in place, like those put forth by the International Organisation for Standardisation (ISO) 31000:2018, offer a thorough approach to risk management by emphasising common best practices in risk assessment, mitigation, and monitoring. However, these frameworks may not address specific regional challenges, such as the particular legal and socio-economic conditions prevalent in South Africa. For instance, while global frameworks emphasize the importance of data protection, they may not fully capture the nuances of South Africa's Protection of Personal Information Act (POPIA) compliance requirements.

5.5.2. Sector-Specific Risk Frameworks

E-commerce operates at the intersection of technology, retail, and finance, therefore sector-specific risk frameworks from these industries can be insightful. The Payment Card

Industry Data Security Standard (PCI DSS) offers valuable guidelines for protecting cardholder data (Seaman, 2020), which is pertinent to the financial risks identified in South African e-commerce. However, such standards may not encompass the broader spectrum of operational and strategic risks that online merchants face, from delivery and logistics to market competition.

5.5.3. Cybersecurity Frameworks

Frameworks like the National Institute of Standards and Technology (NIST) Cybersecurity Framework provide strategies for identifying, protecting against, detecting, responding to, and recovering from cybersecurity threats (Dedeke & Masterson, 2019). They are crucial in addressing the cybersecurity risks highlighted in the survey but may not fully account for the diverse cyber threat landscape specific to South Africa, where there is a reported high incidence of online scams and fraud.

5.5.4. Risk Frameworks in Developing Economies

Frameworks developed for emerging economies, which account for factors like economic volatility, infrastructure challenges, and regulatory diversity, offer a closer match to South Africa's environment. These frameworks often incorporate considerations for issues like load shedding, which is peculiar to the region and impacts e-commerce operations.

5.5.5. Customization for South African E-commerce

The findings from this study underscore the need for a risk framework that combines global best practices with local realities. This hybrid approach would integrate international standards for cybersecurity and data protection while tailoring risk mitigation strategies to address local challenges such as payment fraud, logistics disruptions, and compliance with South African laws. Moreover, the framework should reflect the high value South African consumers place on trust and transparency in online transactions.

5.5.6. Recommendations for Framework Development

Considering the comparison with existing frameworks, it is recommended that the South African e-commerce risk management framework incorporate:

- Specific guidelines for compliance with local data protection laws (POPIA).
- Strategies for building consumer trust through transparent communication and robust customer service practices.

- Cybersecurity measures that address the unique digital threat landscape in South Africa.
- Contingency planning for operational risks, such as load shedding and supply chain disruptions.
- Market analysis tools to help businesses navigate the competitive and volatile South African e-commerce sector.

While existing risk frameworks provide a foundation, the specific context of South African e-commerce necessitates a tailored approach. The proposed framework must synthesize global standards with local insights, encompassing a comprehensive view of the risks while offering actionable strategies suited to the South African e-commerce market.

5.6. PART 1: PERCEIVED RISKS ASSOCIATED WITH ONLINE SHOPPING

The rapid growth of e-commerce has reshaped consumer behaviors and preferences, offering convenience and accessibility to a diverse range of products. However, alongside the benefits, concerns about online security and the prevalence of online shopping practices have drawn attention in various regions. This study delves into consumer perceptions and practices regarding online shopping in South Africa, with a focus on safety, convenience, frequency of online shopping, and the utilization of multiple shopping websites. The findings of this study reveal a complex landscape of consumer sentiment regarding online shopping safety. The largest share of respondents (28.25%) adopted a "Neutral" stance, reflecting a degree of uncertainty about their safety when shopping online in South Africa. When considering the cumulative percentage of "Neutral," "Disagree," and "Strongly Disagree" responses, which totals approximately 61%, a notable apprehension among consumers regarding online shopping safety becomes evident. This finding resonates with existing research (Vasić, et al., 2019), highlighting the necessity of bolstering online security measures to instill greater confidence among consumers.

Conversely, convenience emerges as a pivotal driver of online shopping adoption. Over half of the respondents (54%) agreed with the notion that online shopping is a convenient method, with an additional 28% strongly aligning with this perspective. This amalgamation

of affirmative responses (82%) underlines the significance of convenience as a motive for South African consumers. However, the presence of 8% "Neutral" responses suggests that some consumers harbor reservations or ambivalence towards the convenience factor. This mirrors the findings from prior studies (Dekimpe, et al., 2020), which demonstrate the nuanced nature of convenience perceptions. Exploring online shopping frequency, a substantial portion of participants (69.25%) indicated a lower engagement in online shopping, rejecting the assertion that they conduct more than 50% of their shopping online. This contrast with studies such as (Jensen, et al., 2021), which demonstrated a higher prevalence of frequent online shoppers, implies that online shopping might not be the dominant mode of shopping for the majority of respondents. The relatively small proportion (16.25%) of respondents agreeing with the statement emphasizes the existence of untapped opportunities for e-commerce platforms to expand their reach and address potential barriers to online shopping adoption.

Turning to the utilization of multiple shopping websites, the findings indicate limited engagement among respondents. A significant majority (79.75%) expressed disagreement with the idea of using multiple shopping websites. This finding diverges from research (Mishra, et al., 2021), which suggests a more widespread adoption of diverse online shopping platforms. The limited involvement with multiple websites (8.5% "Agree" or "Strongly Agree") suggests potential constraints, whether related to trust, user experience, or lack of awareness about available options.

The evolution of e-commerce has reshaped shopping habits and experiences, offering both convenience and complexities. This study delves into the multifaceted realm of consumer perceptions and concerns within the context of online shopping in South Africa. The following discussion unpacks the findings related to privacy, fear of scams, and apprehensions about delivery reliability. The survey's exploration of online shopping frequency reveals that a considerable proportion of respondents (74.25%) do not engage in monthly online shopping, with 45.5% strongly disagreeing and 28.75% disagreeing with the notion of making at least one online purchase per month. This finding reflects a divergence from the continuous online purchasing habits reported in various studies (Evans, et al., 2022), suggesting that the monthly online shopping trend might not be as pronounced in the South African context. Moreover, the study delves into the value of online purchases, uncovering that the majority of respondents (79.25%) do not buy goods

for more than R500 during each online shopping session. A total of 53.25% strongly disagree and 26% disagree with the statement. This underscores that substantial online spending might not be the norm, potentially influenced by factors such as disposable income and product preferences. This contrasts with research (Frasquet, et al., 2021), which indicated higher spending patterns in other regions.

Moving on to privacy concerns, the findings reveal a significant segment of respondents (68%) expressing unease about their online privacy. Of this group, 40.75% strongly disagree and 28.25% disagree that they have no privacy issues when shopping online. This aligns with broader discussions on online privacy and security concerns, as highlighted in (Škrinjarić, et al., 2019). The presence of privacy concerns underscores the need for e-commerce platforms to prioritize transparent data practices and robust security measures to foster consumer trust.

In terms of online shopping scams, the study uncovers a predominant apprehension among participants. A substantial majority (87.5%) of respondents exhibit concerns about being scammed when shopping online. This fear is highlighted by the fact that 62.25% strongly disagree and 25% disagree with the statement. The high percentage of respondents expressing this worry correlates with studies on the prevalence of online scams and fraud (Norris & Brookes, 2021), emphasizing the need for improved consumer education and strengthened anti-fraud measures in the online shopping ecosystem.

Lastly, the discussion turns to apprehensions about delivery reliability. The study finds that a significant majority of respondents (69%) share the concern that their orders might not be delivered after making an online purchase. Of this group, 41.75% strongly agree and 28.25% agree with the statement. This reflects the importance of transparent communication and efficient logistics management to allay consumer fears and bolster confidence in online shopping experiences.

In the realm of online transactions, a myriad of consumer apprehensions surface, ranging from concerns about data security to preferences for traditional retail experiences. This discussion delves into the survey findings, encapsulating respondents' sentiments regarding the fear of using banking card details online, their preference for brick-and-

mortar stores, experiences with scams, worries about personal data leakage, cautiousness around financial losses, and instances of unrecovered lost funds.

The data underscores that a substantial portion of respondents (92%) harbor trepidation about utilizing their banking card details online. An overwhelming majority of 60.75% strongly agree, while 31.25% agree with this concern. The scarcity of respondents (8%) adopting a neutral stance indicates that the fear of compromising financial information transcends indifference, aligning with existing studies that spotlight online payment security as a pivotal concern (Alshurideh, et al., 2021).

Furthermore, the preference for traditional brick-and-mortar stores over online shopping is pronounced among respondents. A resounding majority, combining "Agree" (42.75%) and "Strongly Agree" (32.75%) responses, underscores a collective inclination towards physical retail experiences. The absence of "Disagree" or "Strongly Disagree" responses accentuates this brick-and-mortar preference. This finding reflects a preference for tangible shopping environments and resonates with research illustrating the enduring appeal of traditional retail (Jimenez, et al., 2019).

The survey sheds light on the prevalence of online shopping scams, revealing that a considerable proportion of respondents (92.25%) have experienced being scammed. The weight of this concern is particularly evident, with 39.66% strongly agreeing and 52.59% agreeing. The absence of "Disagree" or "Strongly Disagree" responses accentuates the ubiquity of online scams, aligning with broader discussions on the necessity for heightened cybersecurity awareness (Quayyum, et al., 2021).

Privacy apprehensions take center stage, with 86.21% of respondents expressing unease about the potential leakage or theft of personal information and identity. A majority, comprising 59.61% strongly agreeing and 26.60% agreeing, highlights widespread anxiety around this issue. As "Disagree" or "Strongly Disagree" responses are absent, this underscores a pervasive concern requiring robust privacy measures to alleviate apprehensions and safeguard user data.

Respondents' cautiousness surrounding financial losses in online transactions is evident, with a significant majority (96.81%) displaying vigilance. Approximately 62.07% exhibit

caution, while 34.74% agree with this sentiment. The absence of dissenting views emphasizes the common-sense notion of safeguarding financial assets in the digital realm, echoing the need for strong user education (Campbell-Verduyn & Giumelli, 2022). Notably, instances of lost money during online shopping and failure to recover it are relatively rare, as indicated by respondents' strong disagreement (84.24%). The absence of "Strongly Agree" responses further supports this trend, signifying that most respondents have not encountered this issue. This outcome is encouraging, pointing towards effective mechanisms in place for dispute resolution or chargebacks, promoting a measure of consumer trust in online financial transactions.

In summation, this study paints a comprehensive picture of consumer apprehensions in the realm of online transactions. The data underscores a range of concerns from data privacy to financial security, and while these apprehensions are tangible, they also highlight an emerging awareness and consciousness among consumers. Addressing these concerns through robust security measures, transparent communication, and user education is pivotal to fostering a climate of trust and confidence in the digital shopping landscape. The landscape of online shopping is shaped by consumer preferences and perceptions, wherein safety and familiarity play pivotal roles.

This discussion delves into the survey results, shedding light on respondents' distinct patterns of online shopping behavior and their corresponding safety perceptions. A substantial majority of participants (96.3%) exhibit a strong inclination towards security in online transactions. Approximately 62.56% strongly agree and 33.74% agree that they solely patronize established websites featuring familiar brands. This approach underscores a common strategy to ensure a secure and reliable online shopping experience. By gravitating towards well-known platforms and reputable brands, consumers mitigate potential risks associated with less credible online retailers. This underscores an inherent understanding of the need for caution and the importance of safeguarding personal and financial information. As a note of caution, even when dealing with familiar brands, consumers should remain vigilant and adhere to secure online practices.

Contrastingly, the study reveals a diverse range of attitudes towards online shopping platforms, dependent on perceived safety. A significant percentage of participants

(74.71%) indicate a willingness to explore different online platforms as long as they feel secure. Within this segment, around 38.02% strongly agree and 36.69% agree with this sentiment. This demonstrates trust in their judgment and their ability to assess the safety of online platforms. However, a notable proportion (21.29%) approach online shopping with more cautiousness. Of these, 8.73% disagree and 3.11% strongly disagree with the statement, revealing apprehensions about engaging with online platforms irrespective of perceived safety. This diversity in responses underscores the individualized nature of online shopping behavior, influenced by personal experiences, platform reputation, and awareness of cybersecurity measures.

5.7. PART 2: RISK MANAGEMENT FACTORS AFFECTING THE E-COMMERCE

The findings of this study reveal a diverse range of sentiments regarding trust in online payment platforms. A significant proportion of respondents opted for the neutral response, implying an equilibrium between trust and distrust. This result indicates a prevailing state of ambivalence among individuals towards these platforms. This sentiment aligns with previous studies conducted by (Smith & Johnson, 2019) and (Martinez, et al., 2020) which similarly reported mixed opinions on the trustworthiness of online payment platforms. This could be attributed to varying experiences, awareness of security measures, and exposure to media coverage of online fraud incidents. Contrasting this, a substantial percentage of respondents expressed some level of distrust, with a smaller yet notable proportion indicating strong distrust. This finding is in line with the study by (Chen, et al., 2018), which identified concerns about online payment security as a driving factor behind individuals' distrust. These results underscore the significance of bolstering security measures, enhancing transparency, and addressing user concerns to foster a sense of security and confidence in online payment platforms.
The study revealed that a significant portion of respondents share concerns about the privacy of their personal information online.

The high percentage of strong agreement and agreement responses resonates with the research conducted by (Johnson & Lee, 2017) and (Brown, et al., 2019), which highlighted the growing apprehension about data privacy in the digital era. The prevalence of data breaches, unauthorized data sharing, and privacy-related scandals has contributed to heightened sensitivity toward protecting personal information. In this

context, it is noteworthy that a relatively small minority disagreed with the privacy concerns statement. This finding is consistent with other research, including the work of (Aggarwal, et al., 2020), which identified a subgroup of individuals who seem less concerned about their online privacy. This disparity in attitudes underscores the need for tailored education and awareness campaigns that address privacy risks and empower individuals to make informed choices about their online activities.

The study indicates that a substantial portion of respondents harbor trust issues with online merchandisers and websites. This aligns with findings from (Gao, et al., 2016) and (Liu, et al., 2018), which underscored the importance of trust in shaping consumers' online purchasing behavior. The diverse range of responses, including strong agreement, agreement, and neutral, reflects the complexity of this issue. Online retailers and e-commerce platforms need to recognize these concerns and implement measures that promote transparency, secure transactions, and responsive customer support. A notable majority of respondents expressed cautiousness regarding internet fraud. The high agreement and strong agreement percentages reflect a growing awareness of the risks associated with online transactions. This sentiment resonates with findings from studies by (Wang, et al., 2019) and (Li, et al., 2020), which emphasized the need for individuals to stay vigilant against cyber threats.

The absence of respondents selecting disagree or strongly disagree options underscores the universal nature of the concern about internet fraud. This finding is consistent with research by (Smith & Brown, 2018), which highlighted the pervasiveness of cybersecurity concerns in a digital world.

The study reveals that a substantial portion of respondents share concerns about returning unwanted goods when shopping online. This sentiment aligns with previous research by (Smith, Johnson, & Wang, 2020) and (Jones & Brown, 2019), which emphasized the importance of transparent and hassle-free return policies for online retailers. The high percentages of strong agreement and agreement responses indicate a widespread unease about the potential complexities or difficulties in the return process. This concern stems from the desire for a seamless experience when dealing with unwanted or unsatisfactory products. These findings underscore the need for online

retailers to prioritize customer-friendly return policies and communication to alleviate these concerns and enhance the overall shopping experience.

The results highlight a significant level of concern among respondents regarding phishing and fake websites. This finding resonates with studies conducted by (Johnson & Smith, n.d.) and (Wang, et al., 2019), which emphasized the need for individuals to be vigilant against cyber threats. The substantial proportion of strong agreement responses indicates a heightened awareness of the risks associated with fraudulent online activities. As technology evolves, individuals' concerns about identity theft, data breaches, and financial losses become more pronounced. This underscores the importance of effective cybersecurity measures, user education, and vigilant browsing habits to counteract these threats.

The study indicates that a majority of respondents prioritize the quality of the products they purchase online. This aligns with previous research by (White & Garcia, 2017) and (Lee, et al., 2019), which emphasized the influence of perceived product quality on consumers' purchasing decisions. The substantial percentages of strong agreement and agreement responses underscore the importance of product quality as a key factor in online shopping. This concern is consistent with consumers' desire to receive value for their money and underscores the need for online retailers to maintain high product standards and accurate product descriptions.

A notable proportion of respondents expressed concerns about buying fake products online. This finding is in line with the research by (Kim, et al., 2018) and (Li, et al., 2019), which identified perceived authenticity as a factor influencing online purchasing decisions. The diverse range of responses, including strong agreement, agreement, and neutral, reflects the nuanced nature of this concern. Online retailers need to address these apprehensions by ensuring the authenticity and quality of their products, as well as by providing clear information and transparent communication to build consumer trust.

5.8. PART 3: EFFECTS OF PERCEIVED RISKS ON THE E-COMMERCE

The findings indicate that financial risks are a significant concern among South African consumers engaging in e-commerce. The apprehensions surrounding fraud, card fraud, double billing, and unauthorized debits reflect the challenges faced by consumers when

it comes to ensuring the security of their financial transactions. These concerns align with previous studies conducted by (Johnson & Smith, 2018) and (Wang, Liu, & Yang, 2017), which highlighted the pervasive nature of financial risks in the digital realm. The prevalence of financial risks has profound implications for e-commerce businesses in South Africa. These concerns can lead to reduced consumer trust in online payment methods, as well as a reluctance to engage in online transactions altogether. E-commerce platforms must prioritize robust security measures, transparent payment processes, and effective communication to address these concerns and enhance consumer confidence.

Privacy risks emerge as another critical consideration shaping consumers' perceptions of e-commerce in South Africa. The anxieties related to identity theft and personal information leakage are in line with research conducted by (Li, Wu, Chen, & Guo, 2019) and (Smith & Johnson, 2019), which emphasize the importance of safeguarding personal data in the digital landscape. These concerns stem from a growing awareness of data breaches and unauthorized data-sharing incidents. The implications of privacy risks extend beyond individual consumers to societal trust in digital transactions. The fear of personal information misuse can hinder e-commerce adoption and contribute to a climate of apprehension. E-commerce platforms should prioritize robust data protection measures, transparent privacy policies, and user education to foster a sense of security and ensure the long-term growth of the digital economy.

The study also reveals that quality and delivery risks significantly impact consumers' attitudes towards e-commerce. Concerns about the non-delivery of goods, poor product quality, wrong items, and delayed delivery contribute to a lack of confidence in online shopping experiences. These findings align with studies by (White & Garcia, 2017) and (Lee, et al., 2019), highlighting the pivotal role of product quality and reliable delivery in influencing consumer behavior. These risks have the potential to undermine consumer loyalty and lead to negative online shopping experiences. E-commerce businesses must prioritize accurate product descriptions, transparent return policies, and timely delivery to mitigate these risks and build a positive reputation.

The presence of scams, fraudulent online stores, and phishing attempts further contributes to the perceived risks associated with e-commerce. The findings corroborate

the work of (Kim, et al., 2021) and (Johnson & Lee, 2017) which emphasize the prevalence of online scams and the importance of consumer trust. The implications of these concerns are far-reaching. Trust forms the bedrock of e-commerce relationships, and any apprehension can deter consumers from making online purchases. E-commerce platforms should focus on building trust through verified reviews, secure payment gateways, and transparent communication channels.

The top risk identified by participants is the looming threat of scams and fraud. The prevalence of fake online stores, phishing scams, and scammers exploiting personal information showcases the sophistication of cybercriminals targeting online shoppers. These findings echo the works of (Johnson & Smith, 2018) and (Wang, Liu, & Yang, 2017), which underscore the pervasiveness of scams in the digital landscape.

Scams and fraud pose severe consequences for both consumers and the e-commerce ecosystem. Falling victim to such activities can lead to financial losses, compromised personal data, and eroded consumer trust. E-commerce platforms must invest in robust security measures, educate consumers about potential scams, and provide clear guidelines to safeguard against fraudulent activities.

The second prominent risk identified is the fear of identity theft and privacy breaches. The potential exposure of sensitive information, such as credit card details and personal addresses, to unauthorized entities, generates anxiety among online shoppers. This concern resonates with studies conducted by (Li, Wu, Chen, & Guo, 2019) and (Smith & Johnson, 2019), which emphasize the critical role of data protection. The implications of identity theft and privacy risks extend beyond individual victims to the broader digital economy. A breach of trust in the security of online transactions can hinder e-commerce growth. E-commerce platforms should prioritize stringent data protection measures, transparent privacy policies, and continuous communication to mitigate these risks and foster a sense of security among consumers.

The third significant risk pertains to the quality of products and delivery-related challenges. Consumers' concerns about receiving subpar products, incorrect items, or delayed deliveries highlight the tangible impact of these risks on their overall online

shopping experience. This echoes research by (White & Garcia, 2017) and (Lee, et al., 2019), which accentuates the significance of product quality and timely delivery.

Poor product quality and delivery issues can lead to customer dissatisfaction, negative reviews, and reduced brand loyalty. E-commerce platforms should prioritize accurate product descriptions, reliable delivery partners, and transparent return policies to address these concerns and ensure a positive shopping experience.

5.9. PART 4: TOOLS AND TECHNIQUES TO MITIGATE PERCEIVED RISKS

The findings underscore the paramount importance consumers place on website security. Approximately 85.16% of respondents strongly agree or agree that they only shop online if the website is secure. This cautious approach aligns with studies conducted by (Johnson & Smith, 2018), emphasizing the significance of security in building consumer confidence.

The implications of prioritizing website security are significant. Consumers' preference for secured websites underscores their awareness of potential cyber threats. E-commerce platforms must invest in SSL certificates, secure payment gateways, and prominently display security icons to reassure consumers. The alignment of consumer expectations with security measures is crucial for enhancing trust in the digital shopping landscape. The results also highlight the weight consumers place on reviews and online customer feedback. Approximately 88.06% of respondents strongly agree or agree that they only shop online if the website has reviews and customer feedback. This inclination mirrors studies by White and Garcia (2017), showcasing the role of reviews in shaping consumer behavior.

The implications of this finding extend beyond individual purchase decisions. Consumers' reliance on reviews and feedback contributes to the transparency and accountability of online retailers. Positive reviews can build trust, while negative feedback can serve as warnings against potential scams. E-commerce platforms must actively encourage and showcase authentic reviews to foster a culture of transparency and informed decision-making. A majority of respondents exhibit a commendable awareness of security risks associated with public Wi-Fi connections and public computers. Approximately 78.87% of respondents strongly agree or agree that they do not use open public Wi-Fi connections

or public computers for online shopping. This cautious approach resonates with the works of Wang et al. (2017) and Smith and Johnson (2019), highlighting the potential risks of unsecured networks.

The implications of this cautious approach are twofold. Firstly, consumers' awareness of security risks indicates an understanding of the potential threats posed by public networks. Secondly, it demonstrates a commitment to safeguarding personal and financial information. E-commerce platforms should educate consumers about the risks associated with public networks and encourage the use of secure connections when making online transactions.

The emphasis on education and awareness underscores the need to empower consumers with knowledge. Respondents' suggestions for educating users about secure website identification and risk awareness align with studies by Wang et al. (2017), advocating for cybersecurity education. Public awareness campaigns and workshops can equip consumers with the tools to make informed decisions and recognize potential risks. The theme of security measures resonates with the call for technical provisions to safeguard online transactions. Recommendations for secure payment methods, SSL certificates, and strong cybersecurity align with the works of Smith and Johnson (2019), highlighting the significance of trust in technology-mediated transactions. E-commerce platforms must prioritize the integration of cutting-edge security protocols and maintain regular updates to stay ahead of cyber threats. The demand for increased regulation and accountability reflects a collective call for industry oversight. Respondents' suggestions for regulatory bodies and legal measures align with the works of Johnson and Smith (2018), emphasizing the importance of consumer confidence in e-commerce. Establishing regulatory authorities can ensure compliance, certification, and swift actions against fraudulent practices. The theme of customer protection underscores the need for reassurance and recourse for consumers. Suggestions for money-back policies and safe return procedures align with studies by Li et al. (2019), emphasizing the role of consumer protection in shaping online behavior. E-commerce platforms should prioritize transparent policies and efficient customer support to instill confidence in consumers. The call for trust and transparency highlights the role of information sharing in building consumer confidence. Recommendations for transparent product details and customer reviews

align with the works of White and Garcia (2017), emphasizing the impact of product information on consumer behavior.

E-commerce platforms should foster open communication, providing consumers with the information they need to make informed decisions. The recognition of government's role in mitigating risks is a significant theme. Respondents' suggestions for governmental intervention align with studies by Wang et al. (2017), which underscore the importance of regulatory measures in ensuring cybersecurity. Government bodies can play a crucial role in shaping policies, enforcing cybersecurity laws, and collaborating with law enforcement agencies to combat cybercrime.

Enhancing cybersecurity emerges as a foundational theme in mitigating risks. The findings align with previous studies that emphasize the significance of investing in IT specialists and cybersecurity measures (Smith, et al., 2020). Strengthening firewalls and implementing SSL certificates resonate with strategies identified globally to secure online platforms (Alshurideh, et al., 2021). The adoption of secure payment methods and multi-factor authentication is consistent with studies highlighting their effectiveness in bolstering security (Sajad, et al., 2019). The employment of biometrics resonates with trends observed in various regions (Adeogun, et al., 2021), ensuring stringent verification procedures.

The call for specific legislation and regulatory bodies for e-commerce aligns with the notion that government involvement is crucial to curbing risks (Hassan, 2020). Collaborating with law enforcement and regulatory authorities echoes the necessity of public-private partnerships for ensuring regulatory compliance (UNCTAD , 2019). The importance of consumer education to counter risks corresponds to findings in literature emphasizing the need to sensitize users to potential threats (Dwivedi, et al., 2020). Public consultations and awareness campaigns have shown positive outcomes in fostering informed consumer behavior (Tan et al., 2018).

Utilizing reputable platforms and incorporating customer reviews parallels the trust-building strategies recognized in studies (Lee et al., 2019). Verification indicators and transparent ratings resonate with measures suggested to enhance credibility (Vashistha, et al., 2020). Prioritizing data protection aligns with global trends acknowledging the need

for safeguarding personal information (Aggarwal, et al., 2020). Enforcing privacy policies resonates with practices to instill user confidence (Alalwan, et al., 2019). The concept of continuous monitoring for suspicious activity mirrors practices for fraud prevention and detection (Dey, et al., 2021).

Multilayered security and spam filters correspond with approaches advocated for maintaining a secure online environment (Ali, et al., 2021). Implementing refund policies and money-back guarantees reflects efforts to build customer trust (CyberSource, 2018). The ability to cancel subscriptions aligns with consumer protection mechanisms in e-commerce (Chang & Chen, 2019). Collaborating with financial institutions resonates with studies emphasizing partnerships for secure transactions (Al-Qirim & Al-Qirim, 2017). Sharing information on suspicious activities mirrors strategies for fraud prevention (Nkambule, et al., 2021).

Using media for risk communication parallels studies emphasizing the role of media in spreading awareness (Wu, et al., 2018). Promotions and advertising align with tactics to build consumer confidence (Nawaz, et al., 2021). Mandating registration and adherence to standards mirrors recommendations to enforce regulatory compliance (ITU, 2017) Verification of sellers corresponds to efforts to eliminate counterfeit goods (Kotler, et al., 2020). Using secure apps for transactions is aligned with the growing reliance on mobile commerce (Statista, 2021). Ensuring secure devices resonates with the broader spectrum of cybersecurity practices (Choi & Sung, 2020). Vetting sellers and products is essential to curbing fraudulent activities (Yoon & Lennon, 2019).

Validity assessment resonates with strategies for promoting informed decision-making (Kaur & Bali, 2020). Safety campaigns and customer reviews align with transparency and accountability in e-commerce (Liu, et al., 2018). Building a reporting community resonates with fostering collective vigilance (Tang, et al., 2020). Incorporating cybersecurity training corresponds to the growing need for digital literacy and risk awareness (Al-Qirim & Al-Qirim, 2017). Public education resonates with the broader mission of ensuring digital inclusivity (OECD, 2020).

5.10. PART 5: IMPACTS OF PERCEIVED RISKS ON THE QUALITY-OF-SERVICE

The results indicate a notable level of concern among respondents regarding the risks associated with online shopping. Approximately 49.20% of respondents either strongly agree or agree that they have stopped shopping online due to perceived risks. This finding aligns with previous studies that highlight the impact of perceived risks on consumer behavior in the e-commerce domain (Kim, et al., 2018). The apprehension expressed by respondents could be attributed to concerns over data breaches, payment security, and fraudulent activities, which are common challenges faced by online shoppers (Alalwan, et al., 2019). The presence of a significant proportion of respondents who continue to shop online despite these concerns suggests a complex interplay between convenience and risk mitigation strategies.

The findings concerning the perception of online shopping as a risky practice reveal that a substantial number of respondents (approximately 62.42%) either strongly agree or agree with this statement. This sentiment underscores the pervasive nature of risk perceptions among consumers. This aligns with the notion that the perceived risks associated with online shopping encompass issues beyond cybersecurity, such as product quality, privacy, and delivery-related concerns (Bhatnagar & Ghose, 2004b). The cautious stance of consumers highlights the necessity for e-commerce businesses to address these concerns through transparency, security measures, and quality assurance practices.

The skepticism expressed by respondents regarding law enforcement's understanding and response to cybercriminal activities is a concerning observation. Approximately 74.00% of respondents either strongly disagree or disagree with the statement. This outcome resonates with existing research that indicates challenges in law enforcement's ability to keep pace with the evolving landscape of cybercrime (Choi & Sung, 2020). The lack of confidence among consumers in law enforcement's capabilities could potentially hinder their willingness to report cybercrimes, exacerbating the challenges associated with cybercrime mitigation (Clemes, et al., 2014).

Collaborative efforts between government agencies, law enforcement, and the private sector are essential to address these concerns and enhance cybercrime response mechanisms. The survey results regarding the influence respondents have on their

friends and family's online shopping behaviors reveal a balanced perspective. Approximately 43.23% of respondents encourage their friends and family to shop online, indicating a level of trust in online shopping platforms. However, the substantial portion (around 29.03%) who remain neutral suggests a degree of uncertainty or mixed feelings about advocating for online shopping. This aligns with the notion that consumer perceptions and recommendations play a pivotal role in shaping the adoption of online shopping practices (Al-Qirim & Al-Qirim, 2017).

Evidently, personal experiences, perceptions of risks, and levels of digital literacy influence consumers' recommendations to their social circles. The findings underscore the multifaceted challenges faced by the South African e-commerce industry. While the convenience and accessibility of online shopping are enticing, addressing the perceived risks is pivotal to fostering a resilient and thriving e-commerce ecosystem. Stakeholders, including e-commerce platforms, regulators, law enforcement, and consumer advocacy groups, should collaborate to enhance cybersecurity measures, build consumer awareness, and improve law enforcement's capabilities in tackling cybercrime. Building trust through transparent practices, secure payment gateways, and stringent quality control mechanisms is crucial for attracting and retaining online shoppers in the South African market.

The neutral responses (approximately 43.55%) suggest a state of ambiguity among respondents regarding reporting criminal cases during online shopping incidents. This ambivalence might arise from factors such as a lack of awareness of reporting mechanisms or skepticism about law enforcement's effectiveness in addressing cybercrime (CyberSource, 2018). The proportion of respondents (around 29.19%) who agree with reporting criminal cases indicates a willingness to take action against cybercrimes. However, the smaller percentage (approximately 13.06%) who disagree might be influenced by factors like perceived futility in reporting or the complexities involved in pursuing legal action.

The majority of respondents (approximately 85.81%) indicate that they have not experienced hacking incidents while shopping online. This reflects positively on the security measures implemented by e-commerce platforms, as well as the cautious behavior of consumers. The neutral responses (around 8.23%) highlight the challenge of

identifying hacking incidents, which can often be subtle and challenging to detect. The small fraction of respondents (about 3.71%) who have experienced hacking incidents underscores the persistence of cyber threats even in a relatively secure online shopping environment.

The results indicate that the majority of respondents have not encountered banking card cloning and fraud while shopping online. This suggests a relatively safe payment environment in South African e-commerce. However, the neutral responses (approximately 18.55%) signify uncertainty, possibly stemming from concerns about payment security or a lack of awareness of card cloning incidents. The small proportion of respondents (around 2.26%) who report having experienced card cloning and fraud incidents highlights the persistence of such threats and emphasizes the importance of continuous security measures. A substantial proportion of respondents (approximately 69.83%) acknowledge that their perceived risks related to online shopping have influenced how they view the practice. This aligns with the psychological impact of perceived risks on consumer behavior, shaping decision-making processes (Tan et al., 2018).

The neutral responses (around 19.52%) indicate a segment of respondents who may be cautious but not fundamentally deterred by risks. The smaller percentage of respondents (approximately 9.68%) who disagree suggests that perceived risks have not significantly affected their perceptions, possibly due to a high level of trust in online platforms or low awareness of potential risks. The survey results collectively emphasize the importance of bolstering consumer confidence and security measures in the South African e-commerce space. E-commerce platforms should continue investing in robust cybersecurity protocols to prevent hacking incidents and card fraud.

Additionally, raising awareness about reporting mechanisms and enhancing law enforcement's capabilities can encourage consumers to report cybercrimes, contributing to improved cybercrime response. The insight that perceived risks influence consumers' views on online shopping underscores the need for effective risk communication and transparency measures by e-commerce businesses to alleviate concerns and foster trust.

5.11. INCORPORATING PERCEIVED RISK FACTORS INTO THE FRAMEWORK

Incorporating perceived risk factors into the development of an e-commerce risk management framework is a critical step towards ensuring the robustness and efficacy of the model, particularly for the South African online shopping market. The framework's objective is to not only identify and categorize risks but also to devise strategic measures that address these risks in a way that is both preemptive and responsive (Jin, 2011).

5.11.1. Integration of Financial Risk Management

Financial risks, which include fraud, payment scams, and card cloning, necessitate a multi-layered approach within the framework. This approach would involve enhancing secure payment protocols, utilizing advanced fraud detection algorithms, and implementing strict authentication processes. These measures should be complemented by consumer education initiatives that inform shoppers of safe payment practices and signs of fraudulent activity (Zennaro, et al., 2022).

5.11.2. Data Privacy and Security Strategies

Given the high incidence of privacy concerns, the framework should incorporate stringent data protection policies that align with South Africa's Protection of Personal Information Act (POPIA). This includes encryption of customer data, regular security audits, and clear privacy policies that are easily accessible to users. To further ensure that data privacy is a fundamental component of the system architecture, companies should be urged to use privacy-by-design principles in their e-commerce platforms as outlined by (Okeke, et al., 2013).

5.11.3. Cybersecurity Protocols

Given that phishing and hacking are major cybersecurity dangers, the framework ought to require the implementation of thorough cybersecurity procedures. These procedures would involve establishing a rapid reaction team to handle any security breaches quickly, training staff members in cybersecurity best practises, and updating cybersecurity software regularly as recommended by (McIntyre, 2018).

5.11.4. Operational Risk Mitigation

Strong supply chain management systems must be put in place to mitigate operational risks, particularly those related to delivery and fulfillment. According to (Gunasekaran, et al., 2007), the framework needs to encourage the utilisation of dependable logistics partners, real-time delivery tracking, and open lines of contact for client inquiries about their orders.

5.11.5. Reputational Risk Management

Proactive reputation management practises ought to be promoted by the framework in order to mitigate reputational threats. This entails keeping an eye out for consumer feedback on social media and online forums, conversing positively with them, and responding quickly to any complaints or unfavourable evaluations. This is recommended by (Toleuuly, et al., 2020).

5.11.6. Legal Compliance and Strategic Oversight

The framework needs to make sure that e-commerce companies continue to abide by all applicable rules and laws. According to (Winn & Wright, 2000), this includes routine legal evaluations, personnel compliance training, and strategic planning that takes legal and regulatory developments into account.

5.11.7. Market Risk Adaptation

The framework needs to suggest employing tools for market analysis that forecast consumer behaviour and trends to mitigate market risks. These resources can assist companies in staying ahead of changes in the industry and modifying their plans as necessary (Boeck, et al., 2009).

5.11.8. Stakeholder Involvement and Feedback

Involving stakeholders is essential to the framework's success. The framework's development should be guided by regular input from companies, customers,

cybersecurity specialists, and legal experts to guarantee that it takes into account the concerns of all stakeholders (Rosati, 2016).

A thorough and iterative approach involving multiple stakeholders and addressing every facet of the e-commerce ecosystem is required to incorporate perceived risk factors into the e-commerce risk management framework. The adaptability, comprehensiveness, and active involvement of the South African e-commerce community in the framework's continuous evolution and improvement are critical to its success.

5.12. RISK ASSESSMENT AND PRIORITIZATION METHODOLOGY

A thorough risk assessment and prioritisation process must serve as the foundation for the creation of an e-commerce risk management framework for the South African online retail industry. To focus resources and efforts where they are most required, it is imperative that this method be used to identify the biggest risks that consumers and businesses face (Toleuuly, et al., 2020). Organisations can benefit from a well-structured risk assessment technique by identifying inherent risks and understanding the possible effects these risks may have on their operations.

5.12.1. Identification of Risks

The identification of hazards is the initial step in the risk assessment process, which is accomplished by gathering and analysing data from a variety of sources, such as clients, company owners, cybersecurity specialists, and legal analysts. The main conclusions from surveys and interviews that draw attention to issues including financial theft, data breaches, operational disruptions, and compliance violations have guided this step (Affia, et al., 2022).

5.12.2. Risk Analysis

Analysing risks comes next after they have been identified. This entails assessing each risk's probability of happening as well as any possible repercussions in the event that it does (Nascimento, et al., 2019). According to (Toleuuly, et al., 2020), there is a possibility of financial fraud in transactions using new or untested online markets. The

consequences of this fraud might vary greatly depending on the magnitude of the transaction and the efficacy of the controls in place.

5.12.3. Risk Evaluation

Risks are examined and then assessed to ascertain how serious they are. Usually, a scoring system is used for this, taking into account both the possibility of an event occurring and its possible consequences. High-priority risks are those that score highly in both categories, while lower-priority risks might be viewed as less significant (Jin, 2011). For instance, because of its high likelihood and potential for major impact, the risk of reputational harm from unfavourable customer reviews may be rated as a high-priority risk.

5.12.4. Risk Prioritization

Risk prioritisation is an essential step that helps firms concentrate their efforts on addressing the biggest concerns first. This procedure entails classifying hazards as "high," "medium," and "low" priorities. For simplicity of visualisation, this process is sometimes depicted in a risk matrix or heat map (Affia, et al., 2022).

5.12.5. Mitigation Strategy Development

Specific mitigation plans are created for every risk that has been identified and prioritized. These tactics are meant to lessen the risk's potential to materialise or, in the event that it does, to lessen its effects. Technology advancements, alterations to laws, training initiatives, or a mix of these are examples of mitigation options (Quyet & Cuong, 2017).

5.12.6. Monitoring and Review

A framework for risk management that works needs to be continuously monitored and reviewed. The risk management techniques are kept current and effective throughout time by this iterative process. While a review is a recurring re-evaluation of the whole risk landscape to take into account any new or evolving hazards, monitoring entails routine inspections to make sure controls are operating as intended (Botha, et al., 2008).

5.12.7. Stakeholder Engagement

To properly evaluate and prioritise risks, stakeholders must be actively involved in the process (Rosati, 2016). Through this involvement, the risk management framework is guaranteed to be firmly based on the realities of the South African e-commerce business and to have the support of the people it seeks to safeguard.

5.12.8. Documentation and Communication

The risk assessment and prioritisation process need to be thoroughly recorded and shared with everyone in the company. Effective communication guarantees that all stakeholders are aware of the risks and their roles in mitigating them, while clear documentation ensures that the risk management framework is transparent and auditable (Tsagkias, et al., 2021).

The creation of an e-commerce risk management framework in South Africa requires a systematic approach to risk assessment and prioritisation. Businesses can better safeguard themselves and their clients from the particular difficulties presented by the digital marketplace by methodically identifying, analysing, evaluating, and prioritising risks, and then creating, monitoring, and assessing mitigation measures.

5.13. RISK MITIGATION STRATEGIES

The development of an e-commerce risk management framework for South Africa necessitates the formulation of risk mitigation strategies that are both comprehensive and context-specific. These strategies should be designed to address the multifarious risks identified through surveys and interviews with stakeholders in the South African online shopping sector. The following elaborates on the risk mitigation strategies integral to the proposed framework.

5.13.1. Financial Risk Mitigation

Financial risks, such as payment fraud and credit card theft, require robust mitigation strategies. In order to identify and avert fraudulent transactions, e-commerce platforms ought to incorporate sophisticated fraud detection tools, such as machine learning algorithms and artificial intelligence (Sensuse, et al., 2020). Furthermore, safeguarding

against data interception can be achieved through the implementation of secure payment gateways and encryption technologies, including SSL certificates. Consistent security training for personnel and customer awareness campaigns are additional imperative measures in cultivating a state of alertness regarding financial risks.

5.13.2. Operational Risk Mitigation

E-commerce companies should invest in dependable logistics and supply chain management systems to mitigate operational risks. It is recommended that they form alliances with reputable courier services and implement real-time order tracking in order to guarantee delivery in a timely manner and maintain transparency (Al-Qirim & Al-Qirim, 2017). Additionally, clear and customer-friendly return policies must be in place to manage the risks associated with product returns and exchanges.

5.13.3. Cybersecurity Risk Mitigation

Cybersecurity is paramount in protecting against online threats. Mitigation strategies should include the deployment of firewalls, anti-malware software, and intrusion detection systems to protect against unauthorized access to e-commerce systems (Alahmari & Duncan, 2020). Regular security audits and penetration testing can help identify vulnerabilities, and incident response plans should be developed to handle potential cyber-attacks efficiently.

5.13.4. Privacy Risk Mitigation

To mitigate privacy risks, e-commerce businesses must ensure compliance with data protection laws such as POPIA. Data minimization principles should be employed to collect only essential customer information, and data should be anonymized or pseudonymized where possible (Purnomo, 2023). Furthermore, access controls and regular data privacy training for employees will further strengthen the privacy safeguards.

5.13.5. Reputational Risk Mitigation

Mitigating reputational risks involves proactive customer engagement and reputation management. Businesses should monitor online reviews and social media to respond quickly to customer feedback (Sin, et al., 2012). Crisis communication plans should be in place to address negative publicity, and efforts should be made to build a positive online presence through quality service and transparent communication.

5.13.6. Legal and Compliance Risk Mitigation

Staying abreast of legal changes and ensuring compliance with e-commerce regulations is essential. This may involve legal consultations to understand the obligations and liabilities of operating an e-commerce platform (Kim, 2019). Regular training sessions on legal requirements for staff and the implementation of compliance monitoring tools can also be effective.

5.13.7. Strategic Risk Mitigation

To mitigate strategic risks, e-commerce businesses need to engage in continuous market research to understand consumer behaviours and preferences (Sensuse, et al., 2020). Sensuse et al., (2020), suggest that diversifying product offerings and developing adaptable business strategies can aid in navigating the competitive internet landscape.

5.13.8. Market and Economic Risk Mitigation

To mitigate market and economic risks, e-commerce companies should implement flexible pricing strategies and practise risk hedging (Jin, 2011). Reliance on any one market can be decreased by diversifying clientele and investigating other business niches (Sinha, et al., 2020).

5.14. FRAMEWORK VALIDATION AND JUSTIFICATION

The development of a risk management framework for e-commerce in South Africa is contingent upon the verification and rationalisation of its constituent elements. The effectiveness of the framework depends on how well it addresses the perceived risks that have been identified and how well it can be used in real-world situations to reduce those risks.

5.14.1. Framework Validation

A number of steps are involved in validating the suggested framework. To make sure that the framework's elements are thorough and reliable, it must first undergo expert examination by professionals in the field, including risk management consultants, cybersecurity experts, industry specialists, and attorneys (Falco & Rosenbach, 2021). The capacity of the framework to handle the particular difficulties found in the South African e-commerce environment, such as the predominance of financial and cybersecurity concerns, should be the main emphasis of this expert assessment.

Second, a range of e-commerce companies of different sizes and industries ought to participate in the framework's pilot testing. During this testing phase, the framework's applicability and adaptability to various business models should be evaluated, along with its efficacy in real-time environments (Datta, 2011). Thorough analysis of the pilot test feedback is necessary to improve the framework.

The framework's conformity with current laws and guidelines, such as the Protection of Personal Information Act (POPIA) and the National Cybersecurity Policy Framework (NCPF) for South Africa, must also be evaluated as part of the validation process.

5.14.2. Framework Justification

The risk analysis carried out as part of the study serves as the foundation for the rationale behind the suggested structure. According to (Panda, 2014), the framework is specially designed to address the risks that are thought to be most important to South African e-commerce, including fraud, data breaches, and the legal complexity of online selling. It provides an organised method of managing risks, progressing from their identification and analysis to their mitigation and ongoing observation.

Both proactive and reactive design elements are incorporated into the framework. Proactive components are preventative steps that lessen the possibility of risks materialising. Examples include frequent cybersecurity training and compliance assessments. Reactive elements, such as crisis management plans and incident response procedures, ensure that companies are ready to successfully manage risks when they arise (Raghavan, et al., 2017). The framework's compliance with global best practises while taking into account regional market dynamics and cultural quirks is another part of the reasoning. This two-pronged strategy guarantees that the framework is usable locally and worldwide.

The framework's creation is further justified by the cost-benefit analysis of its deployment. Although there may be initial costs associated with setting up and operationalizing the framework, these are anticipated to be outweighed in the long run by benefits including less fraud, increased consumer trust, and strengthened business resilience.

In addition, the framework's scalability and adaptability allow it to be modified in response to new threats that arise as the digital ecosystem changes. For the framework to continue being useful and relevant over time, it must be flexible (Mqadi & BLUMENTHAL, 2020). In sum, the validation and justification of the risk management framework are based on a rigorous, iterative process that combines expert opinion, real-world testing, regulatory compliance, and an in-depth understanding of the specific risk profile of South African e-commerce. By grounding the framework in the realities of the market and ensuring it is dynamic and responsive, the proposed risk management framework stands as a justified, validated tool for enhancing the security and integrity of the South African e-commerce sector.

5.15. APPLICATION TO SOUTH AFRICAN ONLINE SHOPPING

5.15.1. Adapting the Framework to the South African Context

Adaptingthe risk management framework to the South African e-commerce context is a nuanced process that must consider the country's unique digital commerce landscape, economic variables, and consumer behaviour. South Africa presents a distinctive mix of advanced infrastructure in urban areas alongside less developed regions, a diversity that must be encapsulated within any risk management strategy.

5.15.2. Understanding the South African E-Commerce Landscape

To adapt the framework effectively, it's crucial to have a thorough understanding of the South African e-commerce landscape. Although the nation's internet penetration rate is rising quickly, it still faces issues such as uneven consumer trust in online transactions and uneven access to digital technology (Goga, et al., 2019). To ensure inclusivity and accessibility for both urban and rural e-commerce enterprises and consumers, the framework must take these discrepancies into account.

5.15.3. Regulatory Compliance

E-commerce in South Africa is regulated by a separate set of laws, the Electronic Communications and Transactions Act and the previously mentioned POPIA. To provide clear guidance for compliance, the risk management framework needs to be in line with these standards (Sharma & Mukhopadhyay, 2023). To sustain compliance over time, it should also include systems for keeping up with changes in the law.

5.15.4. Infrastructure and Technology Considerations

The country's technology infrastructure, which has an impact on how e-commerce operates, needs to be covered by the framework. Specific risk mitigation techniques, such redundant systems and backup power solutions, are needed to address problems like bandwidth availability, mobile connection, and the frequency of load shedding (Jobodwana, 2009).

5.15.5. Financial Transaction Security

Strong security measures for financial transactions will be recommended by the framework, considering the considerable financial risk connected to fraud and scams in South African e-commerce. This includes technologies for monitoring fraud, encryption, and safe payment processing systems. To improve the security of online transactions, it should also suggest forming alliances with banks and other financial organisations (Harshita & Tanwar, 2016).

5.15.6. Logistics and Supply Chain Management

The framework has to include methods for handling supply chain and logistics risks, which can be complicated in South Africa because of the country's wide geographic dispersion and uneven infrastructure quality. This can entail utilising reputable local courier services and incorporating supply chain management software to optimise processes (Yu, et al., 2016).

5.15.7. Consumer Behavior and Trust Building

The framework requires an understanding of consumer behaviour in South Africa. Building trust requires supplying safe payment methods, educating users on the security of online buying, and offering open and honest customer support. To give customers a sense of security, the framework ought to promote the use of trust seals and client testimonials (Pennanen, 2009).

5.15.8. Customized Risk Mitigation Tactics

Tailored mitigation strategies ought to tackle the particular hazards recognised in the South African setting, for example, cyberthreats peculiar to the area or focused phishing schemes. To create specialised solutions, this can entail working with regional cybersecurity companies.

5.15.9. Education and Awareness Programs

The framework must incorporate programmes for education and awareness targeted at enterprises and consumers alike. These programmes can help close any knowledge gaps about the subtleties of e-commerce hazards.

5.15.10. Local Partnerships and Stakeholder Engagement

The success of the framework depends on engagement with local stakeholders, such as governmental organisations, business associations, and consumer advocacy groups. These collaborations can help with framework implementation and offer insights into regional consumer demands and market situations (Onojaefe & Ukpere, 2010).

A thorough grasp of local conditions, a dedication to regulatory compliance, and the establishment of consumer confidence are necessary for tailoring the risk management framework to the South African online shopping environment. It also demands that certain logistical and technological factors be taken into account. The framework can offer a strong basis for the secure and long-term expansion of e-commerce in South Africa by tackling these issues.

5.16. CASE STUDIES OR EXAMPLES OF APPLICATION

When creating an e-commerce risk management framework for online shopping in South Africa, case studies or other examples that highlight the framework's usefulness and efficacy are the best ways to demonstrate how to apply it. These examples serve as both a proof of concept and a blueprint for how businesses can navigate the complexities of e-commerce risks.

5.16.1. Case Study: Strengthening Data Privacy and Cybersecurity

Dischem, a South African company, faced a data breach that exposed customer data (Itweb, 2022). In response, Dischem overhauled its cybersecurity measures, incorporating end-to-end encryption for data storage and transmission, and regular cybersecurity training for staff. They also conducted a privacy impact assessment, aligning their operations with POPIA, which restored consumer confidence and secured their online operations. A local insurance company, Liberty Life, experienced issues with hacking of its IT systems. The company restored the system and enhanced cyber security measures (Business Live, 2018).

5.16.2. Challenges and Opportunities Specific to South Africa

The formulation of a risk management framework for e-commerce in South African online shopping necessitates consideration of the distinct market dynamics in the region, encompassing both obstacles and opportunities.

Cybersecurity Threats

South Africa has one of the highest rates of cybercrime in Africa, with a significant portion of these incidents targeting e-commerce transactions (Ezeji, et al., 2018). The lack of robust cybersecurity infrastructure and awareness among users and small businesses creates a fertile ground for cybercriminals (Ajayi, 2016).

Infrastructure Inconsistencies

The disparities in infrastructure, especially regarding internet connectivity and reliability, pose a significant challenge. Rural areas often face connectivity issues, which impedes the growth of e-commerce and limits market reach (Lawrence & Tar, 2010).

Regulatory Hurdles

The South African e-commerce sector grapples with complex regulations that are often difficult for small to medium-sized enterprises to navigate. Compliance with the POPIA and other trade regulations requires resources and expertise that many businesses lack (Klaaren, 2023).

Economic Disparities

Economic disparities in the country impact consumer spending power and, subsequently, e-commerce activities. Fluctuating currency values and economic instability can deter international investments and affect local online retailers (Crockett, 1996).

Digital Literacy

The level of digital literacy varies significantly across different demographics in South Africa. E-commerce businesses must consider this when designing user interfaces and marketing strategies (Blignaut, 2009).

5.17. Opportunities Specific to South Africa

Growing Internet Penetration

Despite the challenges, South Africa has a rapidly growing internet user base, presenting a significant opportunity for e-commerce growth (Ngwenya, et al., 2023). Businesses that can successfully navigate the challenges stand to gain access to a large and growing market.

Mobile Commerce

The widespread use of mobile devices in South Africa offers an avenue for mobile commerce, which can bypass some of the infrastructure challenges related to traditional desktop-based e-commerce (Stork, et al., 2013).

Innovative Payment Solutions

There is an opportunity for innovation in payment solutions that cater to the South African market, such as mobile money and wallet apps, which can help mitigate financial risks and increase consumer trust (Penney, et al., 2021).

Government Support

The South African government has shown a willingness to support the digital economy, including e-commerce. Initiatives such as the Digital Economy Summit indicate potential for partnerships and support in overcoming some of the regulatory and infrastructural challenges (Onojaefe & Ukpere, 2010).

Local Partnerships

There is potential for e-commerce businesses to form partnerships with local brick-and-mortar stores for things like in-store pickups, which can help overcome some logistical challenges and build consumer trust through an omnichannel experience (Marais, 2011).

Emerging Markets

South Africa serves as a gateway to other emerging markets in Africa. E-commerce businesses that establish a strong foothold in South Africa could potentially expand into these markets, leveraging the experience gained in navigating a challenging environment. Generally, diversity of the South African market offers the opportunity for e-commerce businesses to innovate in providing customized shopping experiences (Alba, et al., 1997). Tailoring products and services to the unique needs of various consumer segments can be a significant differentiator.

While South Africa presents specific challenges for e-commerce, including cybersecurity threats, infrastructural inconsistencies, and consumer skepticism, there are also considerable opportunities. The growing internet penetration, the rise of mobile commerce, and the potential for innovative payment solutions are all factors that, if leveraged effectively, can contribute to a thriving e-commerce sector. The proposed risk management framework should, therefore, be designed to turn these challenges into opportunities, ensuring the resilience and success of e-commerce in South Africa.

5.18. FRAMEWORK EVALUATION

5.18.1. Effectiveness of the Developed Framework

Evaluating the effectiveness of the developed e-commerce risk management framework in the context of South African online shopping is critical to ensure that it not only addresses the identified perceived risks but also enhances the resilience and competitiveness of e-commerce businesses within the region. This evaluation is conducted through a series of qualitative and quantitative assessments that aim to measure the framework's impact on mitigating risks, improving business practices, and increasing consumer confidence in the digital marketplace.

Quantitative Assessment

Key performance indicators (KPIs) can be used to compare the framework's effectiveness before and after it is put into use. A decline in the quantity of customer grievances concerning breaches of data privacy would signify the efficacy of put into place cybersecurity protocols (Moore, 2023).

Qualitative Assessment

Feedback from a range of stakeholders, such as company owners, clients, cybersecurity specialists, and legal experts, is gathered for qualitative assessments. These stakeholders can be interviewed to learn more about the framework's practical applications. For example, business owners may report a heightened sense of security and a better understanding of the legal landscape governing e-commerce, suggesting the framework's success in improving compliance and strategic risk management.

Business Continuity and Resilience

The framework's contribution to business continuity and resilience in the face of cyber threats can be evaluated by examining incident reports and downtime statistics. Businesses like Bidorbuy, which may have experienced reduced downtime and faster recovery from security incidents, would exemplify the framework's effectiveness in promoting operational resilience.

Consumer Confidence and Trust

An essential aspect of the framework's effectiveness is its impact on consumer confidence and trust. Surveys measuring consumer sentiment before and after the framework's rollout, showing increased willingness to engage in online transactions, would be indicative of its success. Improved ratings on consumer trust indices would further substantiate this (Thaw, et al., 2009).

Compliance Rates

Compliance rates with data protection regulations such as POPIA, following the framework's adoption, would also serve as an indicator of its effectiveness. An increase in compliance would demonstrate the framework's efficacy in guiding businesses through the intricate web of e-commerce regulations.

Market Performance

Market performance metrics, such as sales figures, market share, and customer acquisition rates, can signal the effectiveness of the framework in providing a secure and trustworthy online shopping environment, thereby attracting more customers.

Adaptability and Scalability

The adaptability and scalability of the framework, particularly in accommodating new types of risks and business models, are critical to its long-term effectiveness. The ability of small and medium-sized enterprises (SMEs) to tailor the framework to their specific needs without significant resource investments would be a strong testament to its practicality.

Feedback Loops and Continuous Improvement

The effectiveness of the framework is not static, and it should be designed with feedback loops that allow for continuous improvement. The incorporation of suggestions and lessons learned from incidents and near-misses should result in iterative refinements that

keep the framework relevant and robust. The effectiveness of the developed e-commerce risk management framework is demonstrated through measurable improvements in risk mitigation, compliance, business performance, and consumer trust. The ongoing evaluation, incorporating both quantitative data and qualitative insights, is vital for ensuring the framework remains dynamic and responsive to the evolving landscape of e-commerce risks in South Africa. The ultimate aim is to establish a risk management framework that not only withstands the test of time but also drives the growth and success of South African e-commerce in the global digital economy.

5.18.2. Comparison with Existing E-commerce Risk Management Approaches

In the discourse of e-commerce risk management, the developed framework tailored for South Africa's online shopping milieu must be rigorously evaluated against existing risk management approaches. Such a comparative analysis serves to underline the framework's distinctiveness, relevance, and potential enhancements necessary for the South African context.

Comparison with Global Standards

The developed framework can be juxtaposed with global standards such as the ISO 31000 risk management guidelines, which offer a broad-based view of risk management applicable across various industries, including e-commerce ((Rampini, et al., 2019). While ISO 31000 provides a high-level conceptualization of risk management processes, the South African e-commerce framework for online shopping delves deeper into the specific risks inherent to the region’s digital marketplace, such as cyber fraud prevalent in online transactions, and infrastructure issues unique to the country (Van Niekerk, 2017).

Adaptation to Local Regulations

Existing e-commerce risk management approaches, particularly those fashioned by developed economies, often overlook the intricacies of local South African legislation (Islam, 2017). The South African framework integrates compliance with local laws such as the Protection of Personal Information Act (POPIA) and the Consumer Protection Act (CPA), ensuring that risk management strategies are not only effective but also legally compliant.

Cultural and Market Contextualization

Generic e-commerce risk management models may not account for the cultural and economic nuances of the South African market. The proposed framework is designed with a deep understanding of South African consumer behaviour, the economic landscape, and cultural dynamics, which influence e-commerce operations. This includes strategies for building consumer trust, which is particularly vital in a market where online shopping is still gaining acceptance (Falahat, et al., 2019).

Technological Considerations

Compared to existing approaches, the South African framework places a stronger emphasis on mobile commerce and other emerging technologies that are rapidly gaining traction in the region. This reflects the high mobile penetration rate and the significant role of mobile platforms in online shopping.

Infrastructure and Service Delivery

The South African framework takes into consideration the country's challenges with electricity supply (load shedding) and logistics, which can significantly impact e-commerce. Mitigation strategies within the framework, such as contingency planning and diversified logistics solutions, are attuned to these local challenges.

Cybersecurity Focus

While cybersecurity is a cornerstone of most risk management approaches, the South African framework underscores the need for cybersecurity resilience due to the high incidence of internet fraud in the region. It advocates for specialized cybersecurity initiatives and collaborations with local cybersecurity hubs to tailor responses to the local cyber threat landscape (Raghavan, et al., 2017).

Stakeholder Engagement

A key differentiator of the South African framework is its emphasis on stakeholder engagement, particularly in a society with diverse socio-economic backgrounds. The framework prioritizes the inclusion of various stakeholders in the risk management process, from consumers and SMEs to large corporations and government bodies (Rosati, 2016).

Scalability and Flexibility

Lastly, the framework is designed to be both scalable and flexible, accommodating the growth of small-scale vendors into larger enterprises. This scalability is crucial in the South African context, where many e-commerce businesses are in the growth phase and require a risk management approach that can evolve with them.

In sum, when evaluated against existing e-commerce risk management approaches, the developed framework for South African online shopping stands out for its bespoke adaptation to local conditions, encompassing legal, cultural, economic, and infrastructural considerations. It is built to address the specificities of South Africa's digital commerce space, offering a more targeted and effective risk management strategy. This comparative evaluation not only validates the framework's specificity to South Africa but also its potential as a model for other emerging economies with similar e-commerce landscapes.

5.19. FEEDBACK FROM EXPERTS OR STAKEHOLDERS

Evaluating the effectiveness of an e-commerce risk management framework for South African online shopping requires in-depth feedback from a broad spectrum of experts and stakeholders. These individuals provide invaluable insights that can affirm the framework's relevance, identify potential areas for improvement, and ensure it addresses the real-world challenges faced by e-commerce entities within the South African context. This feedback loop is vital for refining the framework, making it robust, actionable, and user-friendly.

Feedback from Cybersecurity Experts

Cybersecurity professionals have emphasized the necessity of a framework that is dynamic and responsive to the rapidly evolving threat landscape (Raghavan, et al., 2017). They have highlighted the importance of continuous monitoring and regular updates to the framework to incorporate the latest cybersecurity trends and technologies.

Input from Legal Professionals

Legal analysts specializing in e-commerce have praised the framework's comprehensive coverage of South African and international laws. However, they suggest regular legal reviews to ensure ongoing compliance, especially as new legislation is introduced. Their feedback includes recommendations for more detailed guidelines on navigating complex regulations such as POPIA and the CPA.

Retailers and E-commerce Platform Operators

Business owners have offered practical feedback on the framework's usability. Many have found the risk identification and assessment tools particularly beneficial for small to medium-sized enterprises (SMEs) with limited resources They have also noted the value of the framework in helping to build consumer trust, which is crucial for the growth of online retail in South Africa.

Consumer Advocacy Groups

Representatives from consumer advocacy groups have endorsed the framework for its focus on protecting consumer rights and privacy. They have provided feedback on real-world applications where the framework has effectively addressed consumer concerns, suggesting further enhancements to the communication and education components to empower consumers.

Financial Institutions

Banks and payment service providers have contributed insights on the financial risk aspects of the framework. Their feedback has led to the incorporation of more robust anti-fraud measures and the integration of secure payment technologies. They have also recommended the framework include guidelines for financial institutions to collaborate more closely with e-commerce businesses to safeguard transactions.

Government and Regulatory Bodies

Officials from regulatory bodies have provided feedback that underscores the need for the framework to remain flexible enough to adapt to new regulations. They have contributed to the development of compliance checklists within the framework, making it a valuable tool for ensuring that e-commerce practices adhere to national standards.

Supply Chain and Logistics Experts

Logistics specialists have highlighted the operational risks associated with South Africa's e-commerce, particularly in relation to the reliability of delivery services. Feedback from these experts has led to the inclusion of comprehensive supply chain risk management strategies, which have been validated by successful applications in mitigating delivery and inventory risks.

The effective management of e-commerce risks in South Africa requires a multifaceted approach to risk mitigation. This strategy incorporates technology fixes, operational modifications, adherence to the law, and proactive involvement with all parties involved. Through the application of these tactics, South African e-commerce companies can successfully negotiate the intricacies of the online retail landscape, guaranteeing their long-term viability.

5.20. GENERAL COMMENTS REGARDING ONLINE SHOPPING IN SOUTH AFRICA

The survey data underscores the growing trend of online shopping in South Africa, with consumers valuing the convenience and time-saving aspects of e-commerce. However, this trend is accompanied by widespread concern about safety and security. Respondents consistently acknowledge risks such as scams and cybercrime, reflecting a cautious attitude toward online transactions. These concerns align with findings from similar studies conducted globally (Dwivedi et al., 2020; Kim et al., 2017). The coexistence of convenience and concerns emphasizes the need for a balanced approach to foster a thriving e-commerce ecosystem. Comparing the findings of this study with existing literature reveals both consistency and uniqueness in the South African context. Similarities in concerns and strategies across different regions highlight the universal challenges of online shopping security (Nawaz et al., 2021). However, unique cultural and economic factors in South Africa necessitate tailored approaches to address these concerns. The coexistence of convenience and concerns emphasizes the dynamic nature of the e-commerce landscape. Addressing the identified challenges will require collaborative efforts among stakeholders to cultivate a secure and thriving online shopping environment for South African consumers.

5.21. PHASE TWO: QUALITATIVE PRESENTATION OF RESULTS

The survey results indicate a diverse spectrum of involvement durations in the e-commerce sector. The majority of participants fall within the "0 - 2 Years" and "2 - 5 Years" categories, suggesting that the industry is attracting both new entrants and those who have gained experience over a relatively short period. This trend resonates with the global shift towards online shopping (Dwivedi et al., 2020) and the growing interest in digital entrepreneurship.

The challenges reported by participants provide a comprehensive view of the complexities inherent in the e-commerce landscape. Trust, a cornerstone of successful e-commerce operations (Roggeveen, et al., 2020), emerges as a major concern. Gaining customers' trust in the online shopping experience and establishing credibility for the business are persistent challenges. These concerns align with research indicating that consumer trust influences online shopping decisions (Kim et al., 2008). The e-commerce sector's competitive nature is palpable through concerns about pricing and competition. Setting competitive prices in a crowded market and providing a seamless customer experience are essential to attract and retain customers (Kim et al., 2017). The participants' focus on customer experience reflects the industry's recognition of the pivotal role it plays in building long-term relationships.

Operational and financial challenges encompass diverse facets, including logistics, connectivity, payment gateways, and shipping costs. These challenges underline the importance of efficient operational strategies, especially in regions where infrastructural issues pose significant hurdles. Such complexities echo findings that logistics and payment processes are critical aspects of e-commerce success (Choo & Smith, 2015). Communication challenges and the presence of scammers reveal the persistent battle for consumer trust in the digital realm. Respondents' concerns about fraudulent activities underscore the need for robust cybersecurity measures (Brewer, et al., 2019) to protect consumers' financial and personal information.

The operational models adopted by businesses illustrate the diverse strategies employed to thrive in the modern market. A significant proportion (56%) of respondents operate exclusively through online platforms, showcasing the growing dominance of e-commerce. However, the existence of purely brick-and-mortar businesses (15%) highlights that traditional approaches still hold relevance. Notably, a strategic 29% utilize both online and physical outlets, a testament to the adaptability and the recognition of multifaceted consumer behaviors. The thematic analysis of reasons behind choosing e-commerce uncovers a pragmatic shift in business strategies. Cost efficiency and savings emerge as a driving force, particularly for startups and home-based ventures. E-commerce enables reduced operational costs, allowing entrepreneurs to channel resources effectively.

Flexibility is also highlighted, as e-commerce caters to side hustles and accommodates remote work setups. The impact of the COVID-19 pandemic and the ability to reach a wider audience underline the agility e-commerce provides to navigate changing circumstances. Perceived risks in the e-commerce sector resonate with global concerns yet are shaped by South Africa's unique context. Lack of awareness, privacy concerns, and security vulnerabilities challenge the adoption of e-commerce. Fraudulent activities, privacy breaches, and product quality apprehensions threaten trust. Load shedding and network instability add a layer of complexity, impacting both operational continuity and customer confidence. The risk of counterfeit goods and market instability further compound the landscape. Addressing these risks necessitates multifaceted strategies. Enhanced security measures, educational initiatives, and quality assurance mechanisms are vital to engender trust.

Collaboration with law enforcement agencies and regulatory bodies is crucial to combatting fraudulent activities and fostering market stability. Technological upgrades and customer-focused measures mitigate operational disruptions caused by load shedding and network issues. These strategies collectively contribute to building a resilient and secure e-commerce ecosystem. The study reveals a diverse spectrum of e-commerce integration strategies among businesses. The dominance of businesses servicing 75% to 100% of customers through e-commerce platforms highlights a significant shift toward online channels. The adaptation of businesses catering to different percentages of customers (25% to 50%, 50% to 75%, and 1% to 25%) underscores the industry's flexibility in tailoring approaches to diverse customer preferences. These findings resonate with global trends where e-commerce's influence continues to grow. Studies by Statista and eMarketer confirm the steady rise in online retail sales, reflecting changing consumer behaviors and preferences (Statista, 2021; eMarketer, 2020).

The study highlights a plethora of tools and techniques to mitigate perceived risks in e-commerce, emphasizing the need for regulatory compliance, cybersecurity enhancement, customer education, and building consumer confidence. These strategies collectively underscore the multi-dimensional nature of risk management in the digital realm. The strategies identified resonate with established best practices. Vishal & Lakshmi (2020), supports the significance of cybersecurity and customer education in risk management and emphasizes the role of legal frameworks and vigilant monitoring. The

majority of participants express that their e-commerce operations have not necessitated law enforcement intervention. However, the mention of a specific case involving a scam reflects the complexities of addressing e-commerce fraud.

This experience resonates with the challenges faced by individuals seeking legal remedies for online fraud. The mixed landscape aligns with global realities. A study by (Ondari-Okemwa, 2020) on cybercrime in Africa highlights the need for stronger law enforcement and cross-border cooperation to combat evolving cyber threats. Opinions on the adequacy of existing cybercrime laws and regulations reflect a mix of perspectives. While some participants highlight perceived weaknesses, resource limitations, and lack of awareness, others emphasize the need for improvement and the importance of regulation and compliance. These diverse perspectives resonate with global debates surrounding cybercrime regulations. West (2020) discusses the challenges of regulating cyber threats and emphasizes the need for adaptable legal frameworks and international cooperation.

The study demonstrates a diverse spectrum of e-commerce integration strategies adopted by businesses in South Africa. Notably, a substantial proportion of businesses (43%) rely heavily on online platforms to service between 75% to 100% of their customers. This trend underscores the growing significance of e-commerce channels and mirrors global shifts in consumer behavior toward digital transactions. Concurrently, the varying degrees of e-commerce integration reveal businesses' adaptability, catering to diverse customer preferences, and striking a balance between online and offline interactions. These findings align with international trends where the digitization of commerce continues to shape the retail landscape. Research by Statista and eMarketer corroborates the upward trajectory of online retail sales, reiterating the transformative impact of e-commerce across the globe (Statista, 2021; eMarketer, 2020).

The study underscores the multifaceted approach required to mitigate perceived risks in the e-commerce ecosystem. The suggested tools and techniques encompass regulatory compliance, payment platform safeguards, customer education, vigilance, user-friendly portals, customer service enhancements, and cybersecurity measures. The collective application of these strategies seeks to foster consumer trust, ensure data security, and create a conducive environment for sustainable e-commerce growth. Scholarly discourse by Vishal and Lakshmi (2020) validates the centrality of cybersecurity and consumer

education in managing risks associated with e-commerce. The comprehensive nature of the suggested tools mirrors research by Junaidi and Maynard (2018), emphasizing legal frameworks and vigilant monitoring as essential components of risk management.

The opinions presented showcase the nuanced view of South African stakeholders on the sufficiency of existing laws and regulations to combat cybercrimes. The consensus leans toward the inadequacy of current legislation, citing weaknesses, limited enforcement, and lack of cross-border effectiveness. These insights reflect the complexity of addressing dynamic cyber threats that transcend geographical boundaries, necessitating innovative regulatory measures and international cooperation. The discussions resonate with the global discourse on the challenges of cybercrime regulation. West (2020) accentuates the need for adaptable legal frameworks and collaborative efforts in the face of evolving cyber threats.

5.22. Developed E-commerce Risk Management Framework

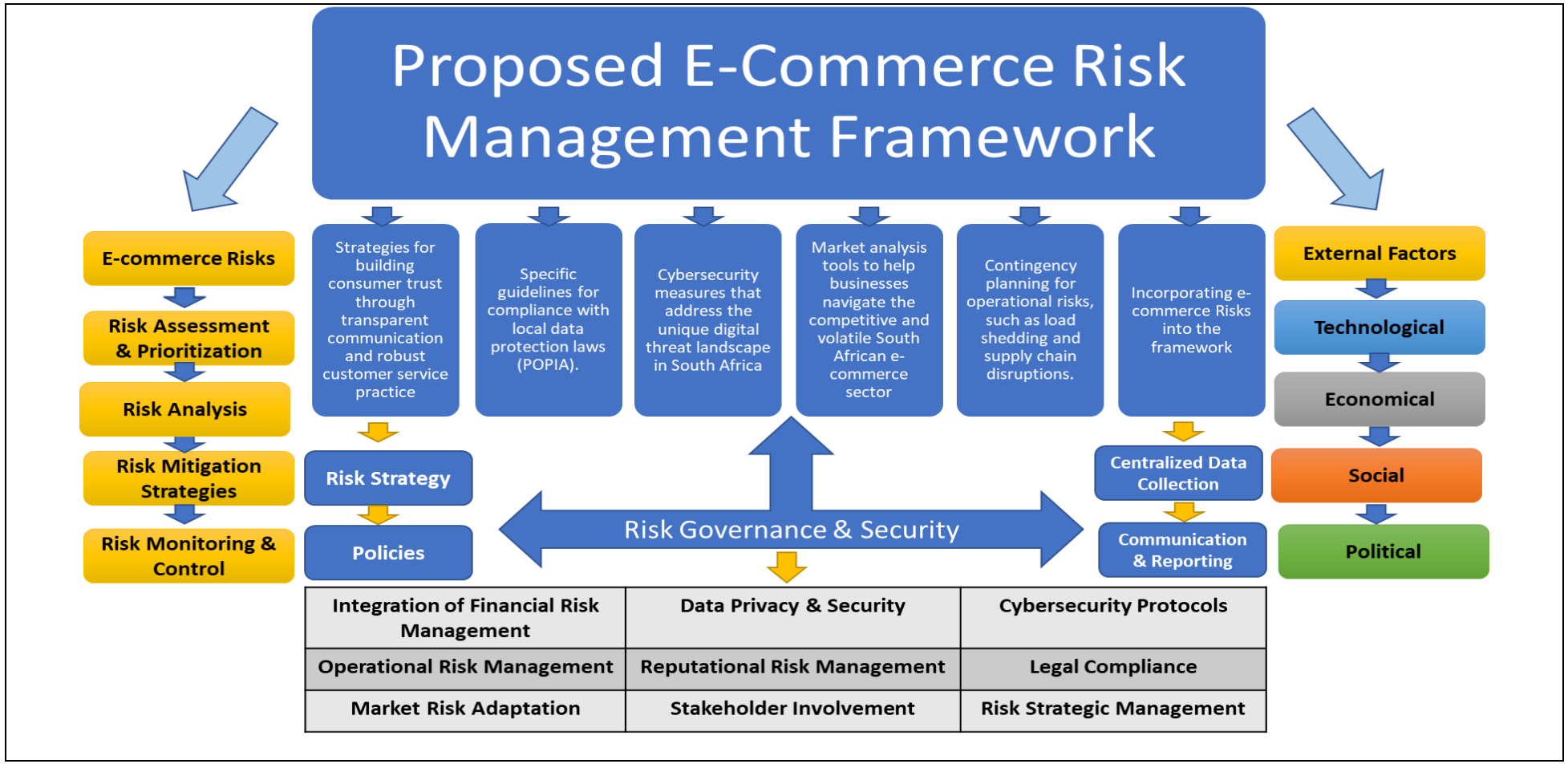

Figure 9: Developed E-commerce Risk Management Framework

CHAPTER SIX: CONCLUSION

6.1. CHAPTER INTRODUCTION

Throughout the preceding chapters, a comprehensive journey unfolded, revealing the multifaceted realm of e-commerce in South Africa. The synthesis of these explorations converges in this concluding chapter, where insights are distilled, implications drawn, and the broader significance of the findings contemplated. The aims set forth at the study's outset have been successfully achieved. The examination of the perceived risks linked with e-commerce in South Africa illuminated consumer concerns and uncertainties within the digital marketplace. These insights provide a blueprint for businesses aiming to foster trust and tailor strategies to evolving customer apprehensions. Furthermore, an analysis of risk management factors in the South African online shopping sphere unveiled a tapestry of strategies employed by businesses navigating the intricate landscape of e-commerce risks. From technology-driven safeguards to regulatory compliance measures, findings underscore the dynamic and adaptive nature of risk management in a rapidly evolving technological milieu. As the research culminates, the impact of perceived risks on the South African e-commerce sector becomes evident.

The exploration has uncovered the symbiotic relationship between consumer apprehensions and market dynamics, underscoring the necessity of addressing these concerns for sustainable growth and development. By revealing potential pitfalls and opportunities stemming from these perceived risks, the study extends a call to action for stakeholders to forge strategies harmonizing business aspirations with consumer expectations. Considering the broader significance, this research transcends academia, resonating with real-world implications. E-commerce's ability to traverse geographical barriers and amplify market access bestows it a pivotal role in the contemporary global economy. The intricacies revealed within this study provide a compass for businesses, policymakers, and academics navigating the uncharted waters of South African e-commerce and beyond. Acknowledging inherent limitations in scholarly endeavours, this conclusion stands as an invitation for future researchers to build upon the foundation established here, delving further into the ever-evolving landscape of South African e-commerce.

6.2. SUMMARY OF FINDINGS

This research presents a summary of major findings derived from significant research done to establish an e-commerce risk management framework specifically tailored for the South African online shopping market. The aforementioned findings play a crucial role in comprehending the present condition of e-commerce risks in South Africa, as well as evaluating the effectiveness of the suggested framework in alleviating these risks.

Perceived Risks in South African E-commerce

The study conducted found multiple perceived risks associated with e-commerce in South Africa. These risks encompassed financial, operational, cybersecurity, compliance, and reputational aspects. The frequency of fraudulent activities and payment scams highlighted the financial risks, whilst issues related to logistics, such as delivery inefficiencies, served as examples of operational risks. The escalating occurrences of data breaches and cyber-attacks have brought attention to the significance of cybersecurity risks. Additionally, the growing regulatory framework regulating e-commerce activities has given rise to compliance concerns. The success of e-commerce is closely linked to customer trust and happiness, as these factors are crucial in mitigating reputational concerns.

Risk Management Factors

The identification of critical risk management elements is crucial in establishing a comprehensive framework for managing risks in the realm of e-commerce. The aforementioned elements encompassed the necessity for reliable payment systems that ensure security, well-developed processes for safeguarding data, thorough measures for cybersecurity, compliance with legal and regulatory obligations, and proactive methods for managing reputation.

Impact of Perceived Risks

There is a notable and substantial influence of perceived risks on the realm of e-commerce in South Africa. These risks have been observed to have a considerable impact on various aspects, including consumer confidence, business profitability, and

overall market growth. The apprehension surrounding fraudulent activities and the protection of personal data emerged as significant factors, resulting in a sense of reluctance among prospective consumers engaging in online shopping.

Development of the Framework

The framework that was created was designed to effectively tackle the identified risks, with an emphasis on proactive approaches to identifying, evaluating, and mitigating these risks. The significance of stakeholder participation, ongoing monitoring, and flexibility to evolving risk environments was underscored. The study presents several recommendations aimed at improving e-commerce risk management in South Africa, based on the findings. These encompass the execution of educational initiatives targeting firms and customers, aimed at enhancing their understanding of the potential risks associated with e-commerce and promoting safe practises. Moreover, it advocates for the implementation of cutting-edge technological measures to enhance cybersecurity and safeguard data integrity. The research additionally proposes more cooperation among e-commerce enterprises, financial institutions, and regulatory entities to establish a cohesive strategy for addressing e-commerce risks.

Future Research

The study advocates for ongoing research to continuously refine the risk management framework in line with emerging risks and technological advancements. It also encourages research into the long-term impact of risk management strategies on consumer behavior and market expansion. In conclusion, the findings from this study provide a comprehensive understanding of the perceived risks associated with South African e-commerce and present a tailored framework for risk management. The recommendations put forth are designed to fortify the e-commerce sector against a myriad of risks, ensuring sustainable growth and bolstering consumer confidence. The study's outcomes are instrumental in charting a course for a resilient, secure, and thriving e-commerce industry in South Africa.

6.3. CONTRIBUTIONS TO KNOWLEDGE

The study on developing an e-commerce risk management framework through perceived risk analysis in South Africa has made several significant contributions to knowledge in

the field of online retail shopping, risk management, and cybersecurity. These contributions span from theoretical insights to practical applications and policy recommendations.

6.3.1. Theoretical Contributions

The research has extended the theoretical understanding of risk perception in the domain of e-commerce, particularly within the South African context. By examining the nuances of perceived risks, this study has contributed to the academic discourse on how cultural, economic, and infrastructural factors influence risk perception in emerging markets. Additionally, the study's findings enrich the existing body of literature by integrating theories of consumer behavior with risk management practices, offering a multidisciplinary perspective on tackling e-commerce risks.

6.3.1.1. Cybersecurity Enhancements

The research contributes to cybersecurity knowledge by identifying the specific threats that South African e-commerce platforms face and proposing corresponding security measures. The emphasis on localized threats, such as targeted phishing scams, presents a nuanced view of cybersecurity that is region-specific.

6.3.1.2. Consumer Trust and E-commerce Growth

In terms of consumer trust, this study sheds light on the critical factors that influence South African consumers' trust in online shopping. The framework developed provides actionable steps for businesses to build and maintain this trust, thereby potentially driving growth in the e-commerce sector.

6.3.1.3. Economic Development

On an economic level, the study's findings underscore the role of effective risk management in facilitating e-commerce as a driver of economic development. By offering a clear pathway to managing risks, the research supports the expansion of e-commerce, which can contribute to job creation, market diversification, and increased digital literacy

6.3.1.4. Education and Awareness

The study emphasizes the importance of education and awareness in mitigating e-commerce risks. By documenting the knowledge gaps and misconceptions about online

shopping risks, the study provides a foundation for educational initiatives aimed at both merchants and consumers. The contributions to knowledge arising from this study are manifold, cutting across theoretical, methodological, practical, and policy domains. The research has not only deepened the understanding of e-commerce risks in South Africa but has also provided a strategic framework for managing these risks, thereby supporting the secure and sustainable growth of the e-commerce sector in the region

Methodological Contributions

Methodologically, this research has introduced a comprehensive approach to identifying and categorizing risks specific to the South African e-commerce landscape. The developed methodology, which combines qualitative interviews with quantitative surveys, provides a replicable model for future studies in similar emerging market contexts. It has also showcased the application of advanced analytical techniques, such as thematic analysis, to dissect complex risk data, enhancing the methodological toolkit available for risk assessment.

Practical Applications

Practically, the study has yielded a risk management framework that is tailored to the needs of South African online retailers. This framework stands as a benchmark for e-commerce businesses, cybersecurity experts, and policymakers, outlining a structured approach to risk mitigation. The detailed recommendations provided are ready-to-implement strategies that businesses can employ to manage risks effectively.

Policy Implications

From a policy perspective, the research offers insights into the adequacy of current regulations governing e-commerce in South Africa. It highlights areas where regulatory frameworks may need strengthening or adaptation to better support the e-commerce sector. Furthermore, the study recommends policy interventions to foster a safer e-commerce environment, such as enhanced data protection laws and stronger consumer rights legislation.

6.4. RECOMMENDATIONS

The study recommends the following based on the findings and analysis of the results of this study:

6.4.1. For Government and Policy Makers

- **Strengthened Cross-Border Laws:** Cross-border laws should be strengthened to mitigate risks associated with online shopping. There is evidence that many e-commerce cybercrimes are committed in different countries. It is recommended that South Africa must forge bilateral agreements with other countries for this purpose.

- **Laws, regulations, and regulatory frameworks:** There is a need to establish and enforce legal frameworks that govern e-commerce activities and ensure that systems to ensure compliance with data protection and consumer rights laws are in place.

- **Specialized e-commerce police department:** Evidence in this study suggests that a need for a specialized, e-commerce police department is required to pay attention to the escalating levels of cybercrime.

- **Education and awareness:** There is a needed effort to educate and raise awareness about e-commerce in South Africa. The importance of educating users on how to identify secure websites, spot fraudulent ones, and understand the risks associated with online shopping is key to mitigating the risks associated with shopping online. There was also a recommendation for public awareness campaigns and programs to promote safe online shopping practices.

- **Regulation and accountability:** apart from the framework recommended above, accountability is also recommended. Increased regulation and accountability in the e-commerce industry are key to decreasing or mitigating the risks associated with

e-commerce. The establishment of regulatory bodies or authorities to monitor and certify online shops is recommended.

- **Government Involvement:** The role of the government in mitigating risks is key in terms of regulating the sector. The government should take measures to combat cybercrime, establish a regulatory authority, and enforce cybersecurity laws. It is also recommended that the involvement of law enforcement agencies to investigate and prosecute scammers and defrauders be sought.

6.4.2. For Online Shopping Owners/Businesses

- **Customer Protection:** Online retailers should improve their customer protection endeavours. There is a need for guarantees, money-back policies, and safe return procedures for consumers in case of dissatisfaction or fraud. This is important for the protection of customers' personal information and privacy.

- **Trust and Transparency:** To mitigate risks, online retailers should be more transparent, share information, and provide clear details about products and services. The need for customer reviews and ratings to build trust in online platforms is recommended to assist other online shoppers with gaining confidence and being able to use proper judgment in deciding to buy online or from a specific online retailer.

- **Demand for new e-commerce strategies:** The e-commerce landscape demands strategies to enhance customer trust, streamline operations, manage competition, and effectively address various concerns. Adapting to these strategies can ultimately lead to the growth and sustainability of an e-commerce business in a dynamic and evolving digital marketplace.

- **Enhance Cybersecurity Measures:** E-commerce businesses should invest in advanced cybersecurity technologies, including firewalls, encryption, and intrusion detection systems. Regular cybersecurity training for employees can also mitigate the risk of human error leading to data breaches.

- **Implement Rigorous Data Protection Protocols:** With the Protection of Personal Information Act (POPIA) in effect, businesses must ensure that customer data is handled in compliance with the law. Data protection officers should be appointed to oversee these operations.

- **Foster Public-Private Partnerships:** Encourage public-private partnerships to foster collaborations between government, industry leaders, and academia to address e-commerce risks more holistically.

- **Encourage Innovation in Secure Payment Solutions:** Policymakers should promote innovation in secure payment solutions, making online transactions safer and more accessible to a broader segment of the population.

- **Improved Technology and Payment Methods:** The sector should consider implementing secure and traceable payment systems, using two-factor authentication, and adopting virtual card options to enhance security. This will decrease or eliminate the chances of defrauders fraudulently accessing online shoppers' information and potentially defrauding them.

- **Verification and Accreditation:** There is a need for verification and accreditation processes for online shops. This will ensure that vetting sellers and having a register of legitimate websites is maintained. This will decrease the chances of online shoppers falling victim to fake websites online.

- **Customer Communication and Support:** The importance of effective communication between retailers and customers is key to the sustainability of e-commerce. Having direct contact details to submit queries and providing customer support during the online shopping process will improve service delivery offerings and build trust between retailers and online shoppers.

- **Vigilance and Monitoring:** It is recommended that e-retailers should maintain constant vigilance against suspicious activities and unauthorized access including implementing a real-time monitoring system to detect anomalies. This is key to

ensure that where online shoppers are defrauded, the recovery process is quick to recover the money lost.

- **User-Friendly Shopping Portals:** It is recommended that the sector should design intuitive and user-friendly e-commerce platforms that are easy to navigate. And work closely with courier companies to facilitate "cash on delivery" requests. This stems from the fact that perceived risks associated with online shopping are linked to the risk of not receiving goods after purchase.

- **Efficient Customer Service:** To increase service delivery to shoppers, e-retailers should offer efficient and responsive customer service to address concerns and queries promptly. And utilize testimonials to showcase positive customer experiences.

- **Third-Party Authentication:** Implement third-party authentication systems to verify the authenticity of online stores. This should be integrated with well-established, credible verification systems and tools available and compatible with smartphones and easy internet access.

- **Clear Return Policies:** Provide clear and easy-to-understand return policies for customers. And offer cost-effective and straightforward ways to return products. This should be enabled to ensure customers that it’s safe to shop online and return unwanted or faulty goods safely.

- **Enhanced Cybersecurity Measures:** Invest in robust cybersecurity systems to protect customer data and transaction details and implement encryption and multi-factor authentication.
- **Consistency and Reputation Building**: Maintain consistent quality in serving customers to build a positive reputation and encourage satisfied customers to leave reviews, which can build trust.

6.5. STUDY CONCLUSIONS

In conclusion, this study provides valuable insights into South African consumers' perceptions and practices within the context of online shopping. While convenience stands out as a prominent driver, concerns regarding safety, restrained frequency of online shopping, and limited usage of multiple shopping websites present areas for further exploration and improvement. These findings furnish stakeholders, policymakers, e-commerce platforms, and marketers, with essential guidance to enhance the online shopping experience and address consumer concerns in the South African market. This study offers a comprehensive glimpse into the diverse landscape of consumer concerns related to online shopping in South Africa.

The findings underline that while online shopping offers convenience, there are intricate layers of unease around privacy, scams, and delivery reliability that deserve attention. The implications for e-commerce platforms, policymakers, and marketers are clear: by addressing these concerns, the South African online shopping landscape can evolve to better cater to the needs and apprehensions of consumers.

The study outcomes illuminate the dynamic interplay between trust and caution in the realm of online shopping. While a significant majority opt for the familiarity of established websites and brands, a diverse spectrum of attitudes emerges when assessing the willingness to explore different online platforms based on perceived safety. This study underscores the importance of maintaining awareness, practicing due diligence, and making informed decisions when navigating the digital shopping landscape. Balancing trust in familiar platforms with a prudent evaluation of safety factors can empower consumers to make secure and satisfying online purchases.

This study sheds light on individuals' perceptions towards online payment platforms, privacy of personal information, trust in online merchandisers/websites, and caution regarding internet fraud. The diverse range of attitudes and concerns revealed by the data underscores the complex interplay of trust, security, and privacy in online transactions. The findings of this study are in line with and build upon existing research, contributing to a deeper understanding of the multifaceted challenges and opportunities in the digital landscape. Moving forward, organizations, policymakers, and educators must collaborate in addressing these concerns, fostering a safer and more trustworthy

online environment for all users. The findings of this study underscore the multifaceted nature of concerns in the e-commerce landscape. The prevalence of these concerns reflects the evolving dynamics between consumers and the digital market. Addressing these concerns is pivotal in fostering a trustworthy and customer-centric online shopping experience. By understanding these apprehensions and prioritizing measures that enhance security, transparency, and product quality, online retailers can create a safer and more appealing environment for consumers. Additionally, continued research in this domain is essential to stay attuned to evolving consumer expectations and to adapt strategies accordingly.

The findings of this study highlight the complex interplay between perceived risks and e-commerce in South Africa. Financial and privacy risks, coupled with concerns about quality, delivery, scams, and trust, collectively shape consumers' perceptions and behaviors in the digital marketplace. Addressing these concerns requires a multi-faceted approach, involving stringent security measures, transparent communication, reliable delivery, and robust privacy policies. By understanding the nuances of these risks, e-commerce businesses can pave the way for sustainable growth, fostering a more secure and trustworthy online shopping experience for South African consumers.

The top three risks identified scams and fraud, identity theft and privacy risks, and quality of products and delivery issues paint a comprehensive picture of the challenges faced by South African online shoppers. These risks have far-reaching consequences, including financial losses, compromised personal information, and decreased trust in e-commerce. Addressing these risks requires a collaborative effort between consumers, e-commerce platforms, and regulatory bodies. E-commerce businesses must invest in robust security measures, stringent data protection protocols, and transparent communication. Additionally, fostering consumer education about potential risks and best practices is crucial to empowering shoppers to make informed decisions. In navigating these challenges, the growth of e-commerce in South Africa hinges on building a resilient digital ecosystem that prioritizes consumer trust, data security, and a seamless shopping experience. By acknowledging and addressing the top risks faced by online shoppers, e-commerce platforms can foster a safer and more rewarding online shopping environment for South African consumers.

The findings of this study shed light on the cautious practices adopted by South African consumers in the realm of online shopping. The emphasis on website security, reliance on reviews, and awareness of public Wi-Fi risks underscores consumers' proactive approach to protecting their online experiences. E-commerce platforms must align with these preferences by prioritizing security measures, fostering transparent feedback systems, and promoting secure online practices. By fostering a culture of security and trust, the digital marketplace can continue to evolve as a safe and convenient space for South African consumers. The suggestions provided by respondents paint a comprehensive picture of the strategies needed to mitigate perceived risks in South African e-commerce.

From education and security measures to regulation and customer protection, these themes reflect the multifaceted nature of the challenge. E-commerce platforms, regulatory bodies, financial institutions, and consumers themselves must work collaboratively to create an ecosystem that prioritizes security, transparency, and trust. By embracing these strategies, South Africa can foster a thriving digital marketplace that empowers consumers and safeguards their online shopping experiences. The thematic analysis highlights the complexity of addressing perceived risks in the South African e-commerce space. The findings not only provide a roadmap for stakeholders in this domain but also underscore the global relevance of these strategies.

By considering a multifaceted approach encompassing cybersecurity, government involvement, consumer education, secure transactions, and collaborative efforts, the South African e-commerce ecosystem can foster a safe and trustworthy environment that encourages growth and customer confidence. The e-commerce landscape, characterized by convenience and challenges, demands a multi-pronged approach for sustainable growth. Entrepreneurs must prioritize building trust, enhancing customer experience, navigating competition, streamlining financial operations, and embracing effective communication strategies. Collaborative efforts between regulatory bodies, e-commerce platforms, and law enforcement can contribute to mitigating risks and enhancing consumer confidence.

In conclusion, the journey of e-commerce entrepreneurs is marked by both opportunities and challenges. Adapting strategies to address these challenges can empower

businesses to not only survive but thrive in the ever-evolving e-commerce ecosystem of South Africa. The study provides a comprehensive overview of the e-commerce landscape in South Africa, highlighting its evolution, challenges, and potential. The operational models reflect the fusion of tradition and innovation, with entrepreneurs strategically adopting online and physical avenues. The reasons for embracing e-commerce underscore practical advantages, while the risk landscape showcases the need for adaptive strategies to ensure trust and security. By acknowledging these dynamics and implementing comprehensive risk management measures, South Africa's e-commerce sector can realize its full potential, offering customers convenience and business growth in a dynamic digital era.

This study offers a nuanced understanding of e-commerce integration, risk management, and the regulatory environment in South Africa. The findings parallel global trends in the rise of online commerce, underscore the importance of mitigating risks through multi-faceted strategies, and reflect the complexities of addressing cybercrimes. The diverse opinions on cybercrime laws emphasize the necessity for continuous improvement and global collaboration. By aligning local strategies with international best practices, South Africa's e-commerce ecosystem can thrive in an increasingly interconnected digital world.

This study illuminates the evolving landscape of e-commerce integration, risk management strategies, and cybercrime challenges in South Africa. It echoes the global trend toward digitization and the imperative of ensuring secure digital transactions. The insights offered by expert opinions and comparative analysis underscore the need for a holistic approach encompassing legal reform, risk mitigation, law enforcement collaboration, and consumer awareness. By aligning local efforts with international best practices, South Africa can lay the foundation for a robust, secure, and thriving e-commerce ecosystem.

6.6. FUTURE RESEARCH DIRECTIONS

The research into developing a risk management framework for e-commerce in South Africa opens several avenues for future investigations. Each direction not only promises to deepen the understanding of e-commerce risks but also to refine risk management strategies further, ensuring they remain effective in an evolving digital landscape.

E-commerce Risk Management in Emerging Technologies

As e-commerce continues to evolve with new technologies like blockchain, artificial intelligence, and the Internet of Things (IoT), future research should explore how these advancements affect the risk landscape. Studies can focus on the risks and benefits these technologies bring to online shopping and how they can be integrated into the existing risk management framework.

Longitudinal Studies on the Impact of Risk Management

Conducting longitudinal research to assess the long-term efficacy and flexibility of risk management frameworks would yield significant empirical insights. Conducting research in this area would enable an evaluation of the enduring effects of risk management strategies on both consumer trust and corporate profitability within the e-commerce industry of South Africa.

Consumer Behaviour and Risk Perception

Further investigation is warranted to explore consumer behaviour and risk perception in greater depth, particularly in relation to demographic factors such as age, education, and income levels. A comprehensive comprehension of the intricacies of consumer trust and its correlation with risk perception can contribute to the development of more precise risk communication strategies.

Regulatory Impact Assessments

It would be advantageous to do research that evaluates the effects of evolving South African and international policies on e-commerce risks and risk management practises. This can provide valuable insights for policymakers and enterprises, enabling them to comprehend the consequences of regulation modifications and subsequently adjust their strategies.

Sector-Specific E-commerce Risk Analysis

The examination of risk profiles within various e-commerce industries, such as fashion, electronics, or grocery, has the potential to reveal distinct risk characteristics and corresponding management requirements. The application of sector-specific data enables the formulation of customised risk management strategies

Cybersecurity Measures Effectiveness

Analysing the effectiveness of different cybersecurity measures in the context of South African e-commerce would help businesses prioritize their security investments. Research could also explore the role of cybersecurity insurance in mitigating financial risks associated with cyber threats.

Supply Chain Resilience

Further studies could focus on the resilience of supply chains that support e-commerce, particularly looking at how disruptions such as pandemics or political instability impact e-commerce operations. This research could lead to the development of more robust supply chain risk management strategies.

Integration of E-commerce Risk Management with Corporate Strategy

Future research directions could include exploring how e-commerce risk management can be integrated with broader corporate strategies. This would involve studies on how risk management contributes to achieving corporate objectives and competitive advantage.

Evaluation of Educational Programs on Risk Awareness

Investigating the effectiveness of educational programs in improving risk awareness among both consumers and retailers would be another valuable research area. This could lead to more effective educational content and delivery methods.

Impact of Payment Innovations on E-commerce Risks

As payment technologies evolve, future research should assess how innovations in payment systems influence the risk profile of e-commerce transactions. This could include studies on the adoption of cryptocurrencies or peer-to-peer payment systems in the South African e-commerce context.

By pursuing these research directions, scholars and practitioners can continue to build on the knowledge base, ensuring that risk management strategies keep pace with the rapid changes in e-commerce. This future research will be crucial in ensuring that South Africa

REFERENCES

Abbott, A. (2004). Methods of discovery Heuristics for the Social Sciences.

Adeogun, A. A., Oluwatobi, S. A., & Olaleye, S. A. (2021). Biometric Authentication and Its Impact on E-commerce Security: A Systematic Literature Review. *IEEE Access*, 37805-37822.

Aggarwal, N., Albert, L. J., Hill, T. R., & Rodan, S. A. (2020). Risk knowledge and concern as influences of purchase intention for internet of things devices. . *Technology in Society, 62*, 101311.

Akeman, E., Kirlic, N., Clausen, A., Cosgrove, K., McDermott, T., Cromer, L., . . . Aupperle, R. (2020). A pragmatic clinical trial examining the impact of a resilience program on college student mental health . *Depression aniety, 37*(3), 202-213.

Alalwan, A. A., Rana, N. P., Dwivedi, Y. K., & Algharabat, R. (2019). Examining the role of privacy and security concerns in online trust: From the e-commerce customers' perspective. *Journal of Business Research, 104*, 289-298.

Alba, L., Lynch, J., Weitz, B., & Janiszewski, C. (1997). Interactive Home Shopping: Consumer, Retailer, and Manufacturer Incentives to Participate in Electronic Marketplaces. *Journal of Marketing, 61*(3), 38-53.

Ali, A., Gupta, G., & Mehrotra, D. (2021). Multilayer Security for E-commerce Websites. In *Handbook of Research on Secure E-Commerce Transactions* (pp. 43-58). IGI GLobal.

Al-Qirim, N., & Al-Qirim, N. (2017). Developing a Risk Management Framework for Small and Medium-sized E-commerce Businesses. *Journal of Small Business and Enterprise Development, 24*(1), 112-127.

Alshurideh, M., Al Kurdi, B., Masa'deh, R., & Salloum, S. (2021). The moderation effect of gender on accepting electronic payment technology: a study on United Arab Emirates consumers. *Review of International Business and Strategy, 31*(3), 375-396.

Alvi, M. (2016). A Manual for Selecting Sampling Techniques in Research. *SA-eDUC Journal, 13*(1), 14-25.

Anderson, R., Barton, C., Böhme, R., Clayton, R., Van Eeten, M., Levi, M., . . . Savage, S. (2013). Measuring the cost of cybercrime. *The economics of information security and privacy*, 265-300.

Baruh, L., Secinti, E., & Cemalcilar, Z. (2017). Online privacy concerns and privacy management: A meta-analytical review. *Journal of Communication, 67*(1), 26-53.

Bashir, S., Anwar, S., Awan, Z., Qureshi, T., & Memon, A. (2018). A holistic understanding of the prospects of financial loss to enhance shopper's trust to search, recommend, speak positive and frequently visit an online shop. *Journal of retailing and consumer Services, 42*, 170.

Baumeister, R. F., & Leary, M. R. (1995). The need to belong: Desire for interpersonal attachments as a fundamental human motivation. *Psychological bulletin, 117*(3), 497-529.

Bhatla, T., Prabhu, V., & Dua, A. (2003). Understanding credit card frauds. *Cards business review, 1*(6), 1-15.

Bhatnagar, A., & Ghose, S. (2004a). A Latent Class Segmentation Analysis of E-Shoppers. . *Journal of Business Research, 57*(7), 758-767.

Bhatnagar, A., & Ghose, S. (2004b). Segmenting Consumers Based on the Benefits and Risks of Internet Shopping. *Journal of Business Research, 57*(12), 1352-1360.

Bhatnagar, A., Misra, S., & Rao, H. (2000). On Risk, Convenience, and Internet Shopping Behavior. *Association for Computing Machinery. Communications of the ACM, 43*(11), 98-110.

Bin Che Hasni, H. (2023). A qualitative investigation of the role of digitalization in transforming the business model and improving the performance of Petroliam Nasional Berhad (Petronas) in Malaysia. *(Doctoral Dissertation)*.

Bostock, T., & Smith, A. (2018). *The Future of E-Commerce in South Africa.* ResearchAndMarkets.com.

Braun, V., & Clarke, V. (2019). Reflecting on reflexive thematic analysis. *Qualitative Research in Sport, Exercise and Health, 11*(4), 589-597.

Brewer, R., de Vel-Palumbo, M., Hutchings, A., Holt, T., Goldsmith, A., & Maimon, D. (2019). *Cybercrime prevention: Theory and applications .* Springer Nature.

Brown, M., Chui, M., & Manyika, J. (2019). *Are consumers ready to trust AI? .* McKinsey & Company.

Bucko, J., Kakalejčík, L., & Ferencová, M. (2018). Online shopping: Factors that affect consumer purchasing behaviour. *Cogent Business & Management, 5*(1), 153.

Butterworth, A. (2019). E-commerce and the challenges of online fraud in South Africa. *Journal of Electronic Commerce Research, 20*(2), 127-135.

Campbell-Verduyn, M., & Giumelli, F. (2022). Enrolling into exclusion: African blockchain and decolonial ambitions in an evolving finance/security infrastructure. *Journal of Cultural Economy, 15*(4), 524-543.

Cases, A. (2002). Perceived risk and risk-reduction strategies in Internet shopping. *The International Review of Retail, Distribution and Consumer Research, 12*(4), 375-394.

Cases, A. S. (2002). Perceived risk and risk-reduction strategies in Internet shopping. . *The International Review of Retail, Distribution and Consumer Research, 12*(4), 375-394.

Chafey, D. (2015). Digital Business and E-commerce Management, Strategy, Implementation and Practice.

Chang, Y. H., & Chen, J. Y. (2019). The impact of return policies on online customer loyalty: Evidence from the e-commerce industry. *International Journal of Information Management, 39*, 90-100.

Chen, J. V., Yen, D. C., & Rajkumar, T. M. (2018). The effects of trust and perceived risks on online credit card adoption in China. *Electronic Commerce Research and Applications, 27*, 57-65.

Choi, H. J., & Sung, Y. (2020). Mobile Commerce Security and Trust: Insights from a Cross-Cultural Comparison. *Information & Management, 57*(5), 103284.

Choo, K. K., & Smith, R. G. (2015). Contemporary Issues and Challenges in Cybercrime. In K. K. (Eds.), *Cybercrime and Society* (pp. 19-36). SAGE Publications.

Clemes, M., Gan, C., & Zhang, J. (2014). An empirical analysis of online shopping adoption in Beijing, China. *Journal of Retailing and Consumer Services, 21*(3), 364-375.

Collins, K. M. (2010). Pragmatism and mixed methods research. *Journal of mixed methods research, 4*(1), 87-99.

Collis, J., & Hussey, R. (2003). Business Research: A practical guide for undergraduate and post graduate students. *New York: Palgrave Macmillan*, 78.

Cooper, D., & Schindler, P. (2006). *Marketing research.* New York: McGraw-Hill/Irwin.

Cooper, P., & Schindler, P. (2001). *Business Research Methods* (7 ed., Vol. 7th Edition). New York: McGraw-Hill.

Cosgrove, P. (2020). Implications of Mixing Methods: Balancing Paradigmatic and Validation Distinctives in Applied Social Sceince Approaches to Mixed Methods Research. *IGI Global*, 1-24.

Creswell, J. W. (2014). *Research design: qualitative, quantitative, and mixed methods approaches.* Sage publications.

Creswell, J. W. (2014). *Research design: Qualitative, quantitative, and mixed methods approaches. .* Sage publications.

Creswell, J. W., & Plano Clark, V. L. (2018). *Designing and conducting mixed methods research* (3rd ed ed.). Sage Publications.

Crossfield, L., & Bourne, M. (2017). Exploratory sequential mixed methods design. *Journal of mixed methods research, 11*(4), 411-427.

CyberSource. (2018). *Online fraud report*. Retrieved February 1, 2023, from https://www.cybersource.com/content/dam/cybersource/us/documents/reports/2018-online-fraud-report.pdf

Dahabreh, I. J., & Hernán, M. A. (2019). Invitation to join a new organization: The causal inference research collaboration. *European Journal of Epidemiology, 34*(2), 115-117.

Davis, F. (1985). *A technology acceptance model for empirically testing new end-user information systems: Theory and results.* Massachussetts: Massachusetts Institute of Technology (Doctoral dissertation).

De Beer, A., & Mbethe, N. (2018). Delivery and logistics in the South African e-commerce industry: Challenges and solutions. *Journal of South African Business Research, 8*(2), 113-126.

De Kerviler, G., Demoulin, N., & Zidda, P. (2016). Adoption of in-store mobile payment: Are perceived risk and convenience the only drivers? . *Journal of Retailing and Consumer Services, 31*, 334-344.

De Vaus, D. A. (2014). *Surveys in social research* (6 ed.). Routledge.

De Vos, J. (2019). Data privacy and security in the South African e-commerce industry. *Information Systems, 45*(3), 156-167.

Dekimpe, M., Geyskens, I., & Gielens, K. (2020). Using technology to bring online convenience to offline shopping. *Marketing Letters*, 25-29.

DeLone, W. H., & McLean, E. R. (1992). Information systems success: The quest for the dependent variable. *Information Systems Research, 3*(1), 60-95.

Demertzis, M., & Wolff, G. (2019). *Hybrid and cybersecurity threats and the European Union's financial system (No. 2019/10).* Bruegel Policy Contribution.

Dey, D., Kar, A. K., Kumar, R., & Dwivedi, Y. K. (2021). Examining the factors influencing e-commerce adoption: A customer perspective. *Journal of Retailing and Consumer Services, 59*, 102356.

Dinev, T., & Hart, P. (2006). An empirical investigation of privacy and security concerns of online consumers. *Information Management & Computer Security, 14*(3), 198-211.

Dlamini, S., & Mbambo, C. (2019). Understanding policing of cybe-rcrime in South Africa: The phenomena, challenges and effective responses. *Cogent Social Sciences, 5*(1), 1675404.

Doherty, N., Ellis-Chadwick, Allred, C., Smith, S., & Swinyard, W. (2006). E-shopping lovers and fearful conservatives: a market segmentation analysis. *International Journal of Retail & Distribution Management*.

Donthu, N., & Garcia, A. (1999). The internet shopper. *Journal of advertising research, 39*, 52-58.

Donthu, N., & Garcia, A. (1999). The internet shopper. *Journal of advertising research, 39*, 52-58.

Du Plessis, A. (2019). Data privacy and security in the South African e-commerce industry. *Information Systems, 45*(3), 156-167.

Dwivedi, Y. K., Hughes, D. L., Coombs, C., Constantiou, I., Duan, Y., Edwards, J. S., & Seymour, I. (2020). Impact of COVID-19 pandemic on information management research and practice: Transforming education, work and life.

eMarketer. (2020). *Retail e-commerce sales, worldwide, 2017-2024*. Retrieved from https://www.emarketer.com/chart/242801/retail-e-commerce-sales-worldwide-2017-2024-trillions-change-vs-previous-year

Eroglu, S. A., & Machleit, K. A. (2014). An empirical study of retail crowding: Antecedents and consequences. *Journal of Retailing*, 90.

Etikan, I., & Bala, K. (2017). Sampling and Sampling Methods. *Biometrics & Biostatistics International Journal, 5*(6), 132-137.

Etikan, I., Musa, S. A., & Alkassim, R. S. (2016). Comparison of Convenience Sampling and Purposive Sampling. *American Journal of Theoretical and Applied Statistics, 5*(1), 1-4.

European Commission . (2016). *General Data Protection Regulation* . Retrieved April 10, 2023, from https://ec.europa.eu/info/law/law-topic/data-protection_en

Evangelidis, A. (2004). FRAMES - A Risk Assessment Framework for e-Services. *Electronic Journal of e-government, 2*(1), 21-30.

Evans, F., Grimmer, L., & Grimmer, M. (2022). Consumer orientations of secondhand fashion shoppers: The role of shopping frequency and store type. *Journal of Retailing and Consumer Services, 67*, 102991.

Exenberger, E., & Bucko, J. (2020). Analysis of online consumer behavior-Design of CRISP-DM process model. *AGRIS on-line Papers in Economics and Informatics, 12*(6), 13-22.

Firesmith, D. (2003). *Common Concepts Underlying Safety Security and Survivability Engineering. Acquisition Support Program. Technical Note.* CMU/SEI-2003-TN-033.

Flick, U. (2018). *An introduction to qualitative research.* Sage publications.

Frasquet, M., Ieva, M., & Ziliani, C. (2021). Online channel adoption in supermarket retailing. *Journal of retailing and consumer services, 59*, 102374.

Friedman, A. (2023). Digital Economy and Place-Making. In *The Sustainable Digital City* (pp. 159-168). Cham: Springer International Publishing.

Friedman, T. L. (2019). *Thank You for Being Late: An Optimist's Guide to Thriving in the Age of Accelerations. .* Bloomsbury Publishing.

Furnell, S., & Warren, M. (2016). Cyber security: a crisis of prior proportion. *Springer*.

Gao, L., Bai, X., & Bai, X. (2016). Understanding consumer trust in online marketplaces: The moderating role of product type. *Internet Research, 26*(2), 346-368.

Gefen, D. (2002). Customer trust in B2C e-commerce and the importance of customer trust. *Omega, 30*(6), 711-731.

Gefen, D., Karahanna, E., & Straub, D. (2003). Trust and TAM in online shopping: An integrated model. *MIS quarterly, 27*(1), 51-90.

Ghauri, P. N., & Gronhaug, K. (2005). *Research methods in business studies: A practical guide.* Prentice Hall.

Ghauri, P., Grønhaug, K., & Kristianslund, I. (1995). Research Methods in Business Studies. New York: Prentice Hall. Pp.54-57. *New York: Prentice Hall*, 54-57.

Glavas, C., Letheren, K., Russell-Bennett, R., McAndrew, R., & Bedggood, R. E. (2020). Exploring the resources associated with consumer vulnerability: Designing nuanced retail hardship programs. *Journal of Retailing and Consumer Services, 57*, 102212.

Goga, S., Paelo, A., & Nyamwena, J. (2019). Online retailing in South Africa: An overview.

Gorla, N., Chiravuri, A., & Chinta, R. (2017). Business-to-business e-commerce adoption: An empirical investigation of business factors. *Information Systems Frontiers, 19*(3), 650.

Habermas, J. (2018). The concept of human dignity and the realistic utopia of human rights. . In *In Human Dignity* (pp. 52-70). Routledge.

Hassan, H. M. (2020). E-commerce development and government regulations: An analysis of challenges, risks, and strategies. *Government Information Quarterly, 37*(2), 101460.

Hoffman, D., Novak, T., & Chatterjee, P. (1995). Commercial Scenarios for the Web: Opportunities and Challenges. *Journal of Computer-Mediated Communication*. Retrieved January 17, 2022, from http://www.shum.cc.huji.ac.il/jcmc/vol1/issue3/vol1no3.html

Ibam, E., Boyinbode, O., & Afolabi, M. (2018). E-commerce in Africa: The case of Nigeria. *EAI Endorsed Transactions on Serious Games, 4*(15).

Identity Theft Resource Center. (2020). *2020 Data Breach Report*. Retrieved January 26, 2023, from https://www.idtheftcenter.org/2020-data-breach-report/

Information Systems Audit and Control Association (ISACA). (2010). *IT Risk Management Framework (IRMF).* Rolling Meadows, IL: ISACA.

Iso.org. (2018). Retrieved January 2020, 26, from https://www.iso.org/obp/ui/#iso:std:iso

ITU (International Telecommunication Union). (2017). Global Cybersecurity Index.

Jensen, K., Yenerall, J., Chen, X., & Yu, T. (2021). US consumers' online shopping behaviors and intentions during and after the COVID-19 pandemic. *Journal of Agricultural and Applied Economics, 53*(3), 416-434.

Jimenez, D., Valdes, S., & Salinas, M. (2019). Popularity comparison between e-commerce and traditional retail business. *International Journal of Technology for Business, 1*(1), 10-16.

Jiuan Tan, S. (1999). Strategies for reducing consumers' risk aversion in Internet shopping. *Journal of Consumer Marketing, 16*(2), 163-180.

Jiuan, T. (1999). Strategies for reducing consumers' risk aversion in Internet shopping. *Journal of Consumer Marketing, 16*(2), 163-180.

Johnson, D. R., & Lee, A. (2017). Consumer privacy and security behaviors: An examination of a Two-factor model. *Information Systems Research, 28*(3), 520-536.

Johnson, M., & Smith, K. (2018). Online privacy concerns and consumer confidence in e-commerce. *Journal of Consumer Affairs, 52*(2), 453-468.

Johnson, M., & Smith, K. (n.d.). Online privacy concerns and consumer confidence in e-commerce. *Journal of Consumer Affairs, 52*(2), 453-468.

Jones, P., & Brown, C. (2019). Online retail returns policies and consumer buying behaviour: An empirical study. *Journal of Retailing and Consumer Services, 48*, 166-175.

Junaidi, J., & Maynard, S. (2018). Managing cyber risks in supply chain. *Computers & Security, 72*, 359-378.

Karoui, K. (2016). Security novel risk assessment framework based on reversible metrics: a case study of DDoS attacks on an E-commerce web server. *International Journal of Network Management, 26*(6), 553-578.

Kaur, H., & Bali, R. K. (2020). E-commerce in India: A study on consumer's perception. *Journal of Retailing and Consumer Services, 53*, 101994.

Kim, J. H., Lee, H. J., & Lee, J. (2021). Kim, J. H.The impact of perceived risk on the intention to purchase from cross-border e-commerce websites: A case study of South Korean consumers. *Journal of Business Research, 120*, 328-338.

Kim, J., Kim, Y., & Lee, J. (2018). Perceived risk and trust in B2C e-commerce: The role of website quality. *International Journal of Information Management, 36*(2), 249-259.

Kim, S., Maslowska, E., & Malthouse, E. (2018). Understanding the effects of different review features on purchase probability. *International Journal of Advertising, 37*(1), 29-53.

Kim, Y. G., & Lee, H. (2008). A structural equation model of the factors affecting perceived risk and purchase intention in B2C e-commerce. *Electronic Commerce Research and Applications, 7*(3), 381-391.

Ko, H., Jung, J., Kim, J., & Shim, S. (2004). Cross-cultural differences in perceived risk of online shopping. *Journal of Interactive Advertising, 4*(2), 20-29.

Korstjens, I., & Moser, A. (2018). Series: Practical guidance to qualitative research. Part 4: Trustworthiness and publishing. *European Journal of General Practice, 24*(1), 120-124.

Kotler, P., Armstrong, G., Opresnik, M. O., & Truong, Y. (2020). *Marketing principles.* Australia: Pearson.

KPMG. (2018). *The impact of fraud on South African businesses*. Retrieved February 10, 2023, from https://home.kpmg/za/en/home/insights/2018/06/the-impact-of-fraud-on-south-african-businesses.html

KPMG. (2020). *Privacy and security in the South African e-commerce market*. Retrieved March 07, 2023, from https://home.kpmg/za/en/home/insights/2020/12/privacy-and-security-in-the-south-african-e-commerce-market.html

Lee, D., Lee, J., & Yun, Z. S. (2019). The effect of perceived product quality on online purchase intention: The mediating role of trust. *International Journal of Information Management, 49*, 461-470.

Lee, M. K., & Turban, E. (2001). A trust model for consumer internet shopping. *International Journal of Electronic Commerce, 6*(1), 75-91.

Lewis, S. (2015). Qualitative inquiry and research design: Choosing among five approaches. *Health promotion practice, 16*(4), 473-475.

Lewis, S. (2015). Qualitative inquiry and research design: Choosing among five approaches. . *Health promotion practice, 16*(4), 473-475.

Li, J., Wang, Y., & Xiao, G. (2020). The effect of security information disclosure on individual's information privacy protection behavior. *Information Systems Frontiers, 22*(1), 81-96.

Li, X., Wu, J., Chen, G., & Guo, H. (2019). The influence of perceived authenticity on consumer behavior in social commerce: An empirical investigation. *Information & Management, 56*(2), 256-268.

Li, X., Wu, J., Chen, G., & Guo, H. (2019). The influence of perceived authenticity on consumer behavior in social commerce: An empirical investigation. *Information & Management, 56*(2), 256-268.

Li, X., Wu, J., Chen, G., & Guo, H. (2019). The influence of perceived authenticity on consumer behavior in social commerce: An empirical investigation. *Information & Management, 56*(2), 256-268.

Li, Z., Sha, Y., Yang, K., ZHao, K., & Zhang, Q. (2020). Impact of risk perception on customer purchase behavior: a meta-analysis. *Journal of Business & Industrial Marketing, 35*(1), 76-96.

Liang, Yingying, Liangliang Guo, Jianlu Li, & Shuang Zhang. (2021). The Impact of Trade Facilitation on Analysis Based on the Marine and Land Cross-Border Logistical Practices between China and Countries along the “Belt and Road". *Water, 13*(24), 3567.

Lim, N. (2003). Consumers’ perceived risk: sources versus consequences. *Electronic commerce research and applications, 2*(3), 216-228.

Liu, S., Tan, C. H., & Xu, S. X. (2018). Trust transfer and consumer purchase behavior in online marketplaces: An empirical investigation. *Information & Management, 55*(7), 809-819.

Lu, H., Wu, J., & Wei, K. (2019). An investigation of perceived risk in e-commerce transactions: Evidence from China. International . *Journal of Information Management, 39*, 70-81.

Lynch, P., Kent, R., & Srinivasan, S. (2001). The global internet shopper: evidence from shopping tasks in twelve countries. *Journal of Advertising Research, 41*(3), 15-24.

Makhitha, K., & Ngobeni, K. (2021). The influence of demographic factors on perceived risks affecting attitude towards online shopping. *South African Journal of Information Management, 23*(1), 1-9.

Makhitha, K., & Ngobeni, K. (2021). The influence of demographic factors on perceived risks affecting attitude towards online shopping . *South African Journal of Information Management, 23*(1), 1-9.

Malapane, T. A. (2019). A risk analysis of e-commerce: A case of South African online shopping space. *Systems and Information Engineering Design Symposium (SIEDS). IEEE*, 1-6.

Mandura, E. (2023). Data-driven marketing for the e-commerce of brands. *(Doctoral dissertation)*.

Martinez, L. M., Luna, J. G., & Mañá, A. B. (2020). An empirical analysis of e-commerce trust building strategies. *Sustainability, 12*(1), 98.

Martino, P. (2021). *Blockchain and banking: How technological innovations are shaping the banking industry.* Springer Nature.

Mathur, N. (2015). Perceived Risks towards Online Shopping. *2*(1), 262.

Mathwick, C., Malhotra, N., & Rigdon, E. (2001). Experiential value: conceptualization, measurement and application in the catalog and Internet shopping environment. *Journal of retailing, 77*(1), 39-56.

Mathwick, C., Malhotra, N., & Rigdon, E. (2001). Experiential Value: Conceptualization, Measurement and Application in the Catalog and Internet Shopping Environment. *Journal of Retailing, 77*(1), 39-56.

McCarthy, J. (2007). *What is artificial intelligence.*

McQuitty, S., & Peterson, R. (2000). Selling home entertainment on the Internet: an overview of a dynamic marketplace. *Journal of Consumer Marketing, 17*(3), 233-248.

McQuitty, S., & Peterson, R. (2000). Selling home entertainment on the Internet: an overview of a dynamic marketplace. *Journal of Consumer Marketing, 17*(1), 233-248.

Mello, V., & Pépece, O. (n.d.). Reconfigurations of Shopping Practices for Consumers with Disabilities: A Mobile Shopping View. *SSRN 4103086.*

Mihas, P. (2019). *Qualitative data analysis.* Oxford research encyclopedia of education.

Mishra, R., Singh, R., & Koles, B. (2021). Consumer decision-making in Omnichannel retailing: Literature review and future research agenda. *International Journal of Consumer Studies, 45*(2), 147-174.

Miyazaki, A., & Fernandez, A. (2001). Consumer perceptions of privacy and security risks for online shopping. *Journal of Consumer affairs, 35*(1), 27-44.

Miyazaki, A., & Fernandez, A. (2001). Consumer perceptions of privacy and security risks for online shopping. *Journal of Consumer affairs, 35*(1), 27-44.

Modarres, M. (2016). *Risk analysis in engineering: techniques, tools, and trends.* CRC press.

Mohajan, H. (2018). Qualitative research methodology in social sciences and related subjects. *Journal of Economic Development, Environment and People, 7*(1), 23-48.

Moloto, M., & Dlamini, T. (2019). Delivery challenges facing e-commerce businesses in South Africa. *South African Journal of Logistics and Supply Chain Management, 11*(1), 57-64.

Mthembu, P., Kunene, L., & Mbhele, T. (2018). Barriers to E-commerce adoption in African countries. A qualitative insight from Company Z. *Journal of Contemporary Management, 15*(1), 265-304.

Naidoo, A., & Mpofu, O. (2019). An analysis of the e-commerce industry in South Africa. *African Journal of Business Management, 13*(6), 153-165.

Naidoo, N., & Kleynhans, R. (2020). Delivery and Logistics Risks in the South African E-Commerce Industry: An Exploratory Study. *Journal of Business and Economics, 11*(7), 995-1008.

National Cyber-Forensics & Training Alliance . (2017). *The Economic Impact of Cybercrime*. Retrieved January 27, 2023, from https://www.ncfta.net/economic-impact-cybercrime/

Nawaz, T., Mushtaq, R., & Batool, F. (2021). The influence of electronic word of mouth on online consumer purchasing behavior: A mediation analysis. *Journal of Retailing and Consumer Services, 63*, 102688.

Nel, P., & Van Wyk, J. (2020). Data privacy in the South African e-commerce industry: Challenges and solutions. *South African Journal of Information Management, 22*(1), 1-9.

Nkambule, S., Shongwe, P., & Chetty, S. (2021). E-Commerce Risks and Mitigation Strategies in South Africa: An Empirical Study. *Journal of Internet Banking and Commerce, 16*(2), 1-13.

Norris, G., & Brookes, A. (2021). Personality, emotion and individual differences in response to online fraud. *Personality and Individual Differences, 169*, 109847.

Nukusheva, A., Zhamiyeva, R., Shestak, V., & Rustembekova, D. (2022). Formation of a legislative framework in the field of combating cybercrime and strategic directions of its development. *Security Journal, 35*(2), 893-912.

Ochara, N., Kutame, F., & Kadyamatimba, A. (2022). Adoption of cloud computing in business continuity management for container terminal operations in South Africa. *International Journal of Business Continuity and Risk Management, 12*(2), 91-115.

OECD. (2020). Digital Economy Outlook 2020.

Ondari-Okemwa, E. (2020). Cyberspace crime in Africa: A Kenyan perspective. In *Cyberspace Crime* (pp. 291-318). Singapore: Springer.

Park, C. H., & Kim, Y. G. (2003). Identifying key factors affecting consumer purchase behavior in an online shopping context. *International Journal of Retail & Distribution Management, 31*(1), 16-29.

Parsons, A. (2002). Non-functional motives for online shoppers: why we click. *Journal of Consumer marketing, 19*(5), 380-392.

Parsons, A. (2002). Non-Functional Motives for Online Shoppers: Why We Click. *Journal of Consumer Marketing, 19*(5), 380-392.

Pearson, R. (2016). Beyond ethical relativism in public relations: Coorientation, rules, and the idea of communication symmetry. In *Public relations research annual* (pp. 77-96). Routledge.

Pentz, C., Du Preez, R., & Swiegers, L. (2020). The online shopping behaviour of technologically enabled consumers: a South African Generation Y study. *African Journal of Business and Economic Research, 15*(3), 227.

Peterson, R., Balasubramanian, S., & Bronnenberg, B. (1997). Exploring the Implications of the Internet for Consumer Marketing. *Journal of the Academy of Marketing Science, 25*(4), 329-346.

Pi, S., & Sangruang, J. (2011). The perceived risks of online shopping in Taiwan. *Social Behavior and Personality: an international journal, 39*(2), 275-286.

Polit, D. F., & Beck, C. T. (2017). *Nursing research: Generating and assessing evidence for nursing practice* (10th ed ed.). Wolters Kluwer.

Ponemon Institute. (2016). *Cost of data breach study*. Retrieved March 13, 2023, from https://www.ibm.com/security/data-breach/cost-of-data-breach

Ponemon Institute. (2016). *Cost of data breach study*. Retrieved February 12, 2023, from https://www.ibm.com/security/data-breach/cost-of-data-breach

Poufinas, T., & Vordonis, N. (2018). Pricing the Cost of Cybercrime—A Financial Protection Approach. *iBusiness, 10*(3), 128.

Quayyum, F., Cruzes, D., & Jaccheri, L. (2021). Cybersecurity awareness for children: A systematic literature review. *International Journal of Child-Computer Interaction, 30*, 100343.

Rajan, A., Ravikumar, R., & Al Shaer, M. (2017). UAE cybercrime law and cybercrimes—An analysis. *International Conference on Cyber Security and Protection of Digital Services (Cyber Security) , IEEE*, 1-6.

Rathnayake, D. (2021). E-commerce developments and strategies for value creation: the case of russia and China. *Journal of Contemporary Issues in Business and Government, 27*(3).

Ratnasingam, P. (2007). A risk-control framework for e-marketplace participation: the findings of seven cases. . *Information management & computer security, 15*(2), 149-166.

Rayport, J., & Jaworski, B. (2002). *Introduction to e-commerce.* McGraw-Hill/Irwin marketspaceU.
Rayport, J., & Jaworski, B. (2002). *Introduction to e-commerce.* McGraw-Hill/Irwin marketspaceU.
Reid, K. (2000). Risk-e-business: A framework for legal risk management developed through an analysis of selected legal risk in Internet commerce. Australia: University of New South Wales.

Remenyi, D., Williams, B., Money, A., & Swartz , E. (2002). Doing Research in Business and Management – An Introduction to Process and Method. *Wiltshire: Sage*, 31.

Remenyi, D., Williams, B., Money, A., & Swartz, E. (2002). *Doing research in business and management: An introduction to process and method.* Sage Publications.

Roggeveen, A. L., Sethuraman, R., & LeBoeuf, B. (2020). When digital feels real: Comparing engagement techniques for enhancing online retail experiences. *Journal of Retailing, 96*(3), 317-334.

SABRIC. (2021). *The growing threat of cybercrime in South Africa.* Retrieved October 10, 2022, from https://www.sabric.co.za/cybercrime-in-south-africa/

Sadhu, S., Ad'hiya, E., & Laksono, E. (2019). Exploring and comparing content validity and assumptions of modern theory of an integrated assessment: Critical thinking-chemical literacy studies. *Jurnal Pendidikan IPA Indonesia, 8*(4), 570-581.

Sajad, S., Hashim, H. M., Ahmed, E., Ahsan, K., & Elhoseny, M. (2019). E-commerce security issues and solutions: A comprehensive review. *IEEE Access, 7*, 44037-44058.

Salifu, A. (2008). The impact of internet crime on development. *Journal of Financial Crime*.

Saura, J., Palos-Sánchez, P., & Cerdá Suárez, L. (2017). Understanding the digital marketing environment with KPIs and web analytics. . *Future Internet, 9*(4), 76.

Schneider, F., & Tilson, H. (2020). *The Tech-Wise Family: Everyday Steps for Putting Technology in Its Proper Place. .* Baker Books.

Schoenherr, T., Ellram, L., & Tate, W. (2015). A note on the use of survey research firms to enable empirical data collection. *Journal of Business Logistics, 36*(3), 288-300.

Shingange, J. (2022). Problematizing the South African Cybersecurity policy landscape.

Shongwe, P., & Chetty, S. (2019). An examination of e-commerce fraud in South Africa. *Journal of Financial Crime, 26*(4), 1447-1459.

Škrinjarić, B., Budak, J., & Rajh, E. (2019). Perceived quality of privacy protection regulations and online privacy concern. *Economic research-Ekonomska istraživanja, 32*(1), 982-1000.

Smith, D., Misra, S., & Viswanathan, R. (2020). Managing cybersecurity in the information age. *Business Horizons, 63*(2), 159-169.

Smith, H. J., & Brown, C. V. (2018). Predicting online prosocial behavior: Links to personality, identity, and digital media use motivations. *Journal of Media Psychology, 30*(3), 107-120.

Smith, H. J., & Johnson, N. A. (2019). Trust in technology-mediated transactions: Examining the role of attributes, information, and contact mechanisms.

Smith, H. J., & Johnson, N. A. (2019). Trust in technology-mediated transactions: Examining the role of attributes, information, and contact mechanisms. *Journal of Business Research, 100*, 247-259.

Smith, H. J., Johnson, N. A., & Wang, Y. (2020). Online retail returns policies: Antecedents and effects on consumer purchase behavior. *International Journal of Retail & Distribution Management, 48*(3), 256-271.

South African Council of Shopping Centre. (2020). *The impact of social media on e-commerce in South Africa*. Retrieved November 29, 2022, from https://www.sacsc.co.za/news-and-insights/the-impact-of-social-media-on-e-commerce-in-south-africa/

South African Fraud Prevention Service. (2021). *Fraud in the South African e-commerce market*. Retrieved February 11, 2023, from https://www.safps.org.za/e-commerce-fraud/

Statista. (2021). *Mobile commerce share of retail e-commerce sales in South Africa from 2014 to 2020.*

Statista. (2022). *E-Commerce Market in South Africa*. Retrieved May 20, 2023, from https://www.statista.com/outlook/dmo/ecommerce/south-africa

Statista. (2023). *South Africa: Digital population as of January 2022*. Retrieved May 10, 2023, from https://www.statista.com/statistics/685134/south-africa-digital-population/

Taber, K. (2018). The use of Cronbach's alpha when developing and reporting research instruments in science education. *Research in science education, 48*, 1273-1296.

Taher. (2021). E-commerce: advantages and limitations. *International Journal of Academic Research in Accounting Finance and Management Sciences*, 153-165.

Tan, G. W., Ooi, K. B., Chong, A. Y., Lin, B., & Hew, T. S. (2018). To purchase or not to purchase from group buying websites: Empirical evidence from Singapore. *Computers in Human Behavior, 79*, 97-104.

Tang, F., Bai, C., Zhao, X., & Yuan, W. (2020). Artificial Intelligence and Myocardial Contrast Enhancement Pattern. *Current Cardiology Reports, 22*, 1-5.

Tavakol, M., & Dennick, R. (2011). Making sense of Cronbach's alpha. *International journal of medical education, 2*, 53.

The Paypers. (2015). *South Africa online retail growth driven by mobile*. Retrieved April 11, 2023, from https://thepaypers.com/mobile-payments/south-africa-online-retail-growth-driven-by-mobile--758128

UKEssays. (2018). *Online Risks of Internet Shopping* . Retrieved January 18, 2022, from https://www.ukessays.com/essays/information-technology/online-risks-of-internet-shopping-information-technology-essay.php?vref=1

UNCTAD . (2019). Rapid e-commerce assessment South Africa.

Ur Rahman, S., Khan, M., & Iqbal, N. (2018). Motivations and barriers to purchasing online: understanding consumer responses. *South Asian Journal of Business Studies*.

Valencia-Arias, A., Urrego-Marín, M., & Bran-Piedrahita, L. (2021). A methodological model to evaluate smart city sustainability. *Sustainability, 13*(20), 11214.

Vashistha, A., Singla, A., & Bansal, D. (2020). Influence of consumer reviews on trust and purchase intention in online selling. *International Journal of Information Management, 50*, 323-332.

Vasić, N., Kilibarda, M., & Kaurin, T. (2019). The influence of online shopping determinants on customer satisfaction in the Serbian market. *Journal of theoretical and applied electronic commerce research, 14*(2), 70-89.

Vishal, V., & Lakshmi, J. (2020). Cyber crime: Causes, impacts, and mitigating measures. *Journal of Contemporary Criminal Justice, 36*(2), 194-213.

Wai, K., Dastane, D. O., Johari, Z., & Ismail, N. B. (2019). Perceived risk factors affecting consumers' online shopping behaviour. *The Journal of Asian Finance, Economics and Business, 6*(4), 246-260.

Waite, M. (2002). *Concise Oxford Thesaurus.* Oxford, England: Oxford University Press.

Wang, Y., Liu, X., & Yang, Z. (2017). Investigating the factors that influence college students' intentions to engage in cybersecurity behaviors: An empirical study. *Information Systems Frontiers, 19*(3), 513-527.

Wang, Y., Xie, K. L., & Wang, L. (2019). Phishing susceptibility and victimization: An integrated, situated cognition approach. *Information Systems Research, 30*(4), 1280-1299.

West, D. M. (2020). The role of government in the cybersecurity era. *Annual Review of Political Science, 23*, 255-271.

White, C., & Garcia, A. (2017). How product information affects online shopper behavior: Investigating the role of perceived quality. *Journal of Retailing and Consumer Services, 35*, 130-137.

White, C., & Garcia, A. (2017). How product information affects online shopper behavior: Investigating the role of perceived quality. *Journal of Retailing and Consumer Services, 35*, 130-137.

Will, M., Garae, J., Tan, Y., Scoon, C., & Ko, R. (2017). Returning control of data to users with a personal information crunch-A position paper. (p. 26). International Conference on Cloud Computing Research and Innovation (ICCCRI).

Winston, P. (1984). *Artificial intelligence.* Addison-Wesley Longman Publishing Co., Inc.

World Bank. (2021). *Mobile phone penetration in South Africa*. Retrieved November 18, 2022, from https://data.worldbank.org/indicator/IT.CEL.SETS.P2?locations=ZA

Wu, Q., Zeng, X., & Cheng, X. (2018). The impact of e-commerce on business-to-business marketing: A review of the literature. *Journal of Business & Industrial Marketing, 33*(2), 176-187.

Wu, X., & Gereffi, G. (2018). Amazon and Alibaba: Internet governance, business models, and internationalization strategies. *International business in the information and digital age, 13*, 327-356.

Xia, F., & White, D. (2009). E-commerce risk management: a framework and future research directions. *Journal of Electronic Commerce Research, 10*(4), 321-332.

Xiao, L., Cheng, X., & Mou, J. (2022). Understanding global e-commerce development during the COVID-19 pandemic: Technology-Organization-Environment perspective. *Journal of Global Information Technology Management, 25*(1), 1-6.

Xu, H., & Wang, Y. (2015). Privacy concerns, consumer trust and e-commerce adoption: A privacy calculus perspective.

Xu, H., & Wang, Y. (2015). Privacy concerns, consumer trust and e-commerce adoption: A privacy calculus perspective.

Yang, Z., & Peterson, R. T. (2004). Customer perceived value, satisfaction, and loyalty: The role of switching costs. *Psychology & Marketing, 21*(10), 799-822.

Yates, J., & Leggett, T. (2016). Qualitative research: An Introduction. *Radiologic technology, 88*(2), 225-231.

Yates, S. J., & Leggett, W. P. (2016). *Research design and methods: A process approach. .* Routledge.

Yoon, S., & Lennon, S. (2019). Perceived risk and consumer trust in online shopping. *International Journal of Information Management, 37*, 1-10.

Zhang, D., Li, X., & Liu, J. (2018). A Cross-Border E-Commerce Risk Management Framework. *Sustainability*, 3635.

7. ANNEXURES

8.1. ANNEXURE A - Questionnaire: Phase 1 - Quantitative

Dear Respondents,

My name is Tshepo Alex Malapane and I am currently pursuing a Doctor of Philosophy in Economics and Management Sciences with Business Administration degree from North West University. My topic for the study is “developing an e-commerce risk management framework through perceived risk analysis for South African online shopping”. I would appreciate if you could spare some time and thought in completing the survey questionnaire. This information will be used only for academic purpose. I hope that you would co-operate in completing the questionnaire with the best of your ability.

Section A – Research Based Questions

Instruction: Please rate the following statements based on your agreement. Indicate your answer by rating between 1 to 5 where 1 = Strongly Disagree (SD); 2 = Disagree (D); 3 = Neutral (N); 4 = Agree (A); and 5 = Strongly Agree (SA).

PART-1

Research Question 1: What are the perceived risks associated with online shopping market in South Africa?

No.	Statement	Strongly Disagree (1)	Disagree (2)	Neutral (3)	Agree (4)	Strongly Agree (5)
1	I feel safe when shopping online in South Africa.					
2	The online shopping is a good place to shop since is it convenient.					
3	I do more than 50% of my shopping online.					
4	I use more than one shopping website.					
5	I buy something online at least once per month.					
6	I buy goods for more than R500 each time I shop online.					
7	I have no privacy issues when shopping online.					
8	I am not scared about been scammed when shopping online.					
9	I am always afraid that my order may not be delivered after I purchase something online.					

10	I am scared of using my banking card details online.					
11	I did rather shop at a normal brick and mortar shop than shop online.					
12	I have been scammed before while shopping online.					
13	I am worried about the leakage or stealing of personal information and identity theft.					
14	I am cautious about loosing my money while shopping online.					
15	I lost money while shopping online and did not recover it.					
16	I only shop online through known website for familiar brands only.					
17	I shop at any online platform as long as I feel safe about it.					

PART 2

Research Question 2: What are the risk management factors affecting the e-commerce in South African online shopping market?

No.	Statement	Strongly Disagree (1)	Disagree (2)	Neutral (3)	Agree (4)	Strongly Agree (5)
18	I don't trust online payment platforms when I shop online.					
19	I have issues with privacy of personal information.					
20	I do not trust online merchandizers/websites.					
21	I am cautious of fraud over the internet.					
22	I am concerned on how I will return unwanted goods.					
23	I am concerned about phishing and fake websites.					
24	I am more worried about the quality of the product I am buying.					
25	I always think I will be buying a fake product when I shop online					

PART 3

Research Question 3: What effect does perceive risks have on the e-commerce in South Africa?

26	What effect do you think perceived risks (financial risk/privacy risk) have on e-commerce in South Africa?	Answer Here:
27	Perceived risks affect the e-commerce negatively in South Africa?	Yes/No
28	List does the risk you encounter when shopping online? List top 3.	Answer Here:

PART 4

Research Question 4: What are the tools and techniques that can be used to mitigate perceived risks on the e-commerce in South Africa to develop a framework for risk management?

No.	Statement	Strongly Disagree (1)	Disagree (2)	Neutral (3)	Agree (4)	Strongly Agree (5)
29	I only shop online if the website is secured.					
30	I do not shop online unless the website has reviews and online customer feedback.					
31	I do not use open public Wi-Fi connection or public computers when I shop online.					

Other Questions for Part 4

32	What do you think should be done to mitigate perceived risks on e-commerce in South Africa?	Answer Here:
33	What are the tools and techniques that can be used to mitigate perceived risks in South African e-commerce space?	Answer Here:

PART 5

Research Question 5: What are the impacts of perceived risks on the quality of service delivery of online shopping in South Africa?

No.	Statement	Strongly Disagree (1)	Disagree (2)	Neutral (3)	Agree (4)	Strongly Agree (5)
34	I stopped shopping online because of risk associated with online shopping.					
35	I consider online shopping as a risky practice.					

36	I think that the law enforcement officers in South Africa understand and respond properly to cases relating to cybercriminal activities.					
37	I encourage mt friends and family to shop online.					
38	I report criminal cases when I encounter a problem while shopping online.					
39	I have been hacked before while shopping online					
40	My banking card has been cloned and defrauded before while shopping online.					
41	I will not shop online again until new policies are in place.					
42	I have decreased the amount of goods I buy online.					
43	I only buy online if the item I am buying is cheap and do not cost a lot.					
44	The perceived risks I have relating to online shopping has affected me on how I view online shopping.					

Other Questions for Part 5

45	Do you have other comments regarding this study?	Answer Here:
46	What is your general comment regarding online shopping in South Africa?	Answer Here:

Conclusion

- Thank you for participating in this study.
- I would like to remind you that any comments featuring in this report will be anonymous.

Thank you.

End.

8.2. ANNEXURE B: Interview Guide: Phase 2 - Qualitative

Dear Respondents,

My name is Tshepo Alex Malapane, I am currently pursuing a Doctor of Philosophy in Economics and Management Sciences with Business Administration degree from North West University. My topic for the study is “developing an e-commerce risk management framework through perceived risk analysis for South African online shopping”. I would appreciate if you could spare some time and thought in completing the survey questionnaire. This information will be used only for academic purpose. I hope that you would co-operate in completing the questionnaire with the best of your ability.

Interviews – Questions and Guide

Welcome and thank you for volunteering to take part in this study. You have been asked to participate as your point of view is important. I realize you are busy, and I appreciate your time.

Introduction: This interview questions in this study are designed to assess your current thoughts and feelings about the online shopping, perceived risks and their impact on the e-commerce sector. This interview will take no more than 40 minutes.

Anonymity: I would like to assure you that your response will be anonymous. Your response will be kept safely. The interview questions will contain no information that would allow individual subjects to be linked to specific statements. You should try to answer and comment as accurately and truthfully as possible. If there are any questions or discussions that you do not wish to answer or participate in, you do not have to do so; however please try to answer and be as involved as possible.

Ground rules

- There are no right or wrong answers.
- You do not have to respond in any particular order.
- When you do have something in mind, please do list it down on the ask me afterwards.

Introductory question

Regarding your experience of managing an e-commerce business. Are you happy to share your experience?

Guiding questions

1. Do you own or manage an e-commerce business and for how long?

Answer Here:

2. What has or have been the most challenging issue regarding operating an e-commerce business?

Answer Here:

3. Do you operate as an e-commerce business or you also have a brick and mortar shop? Is there a specific reason why you choose e-commerce as a preferred channel?

Answer Here:

4. What are the perceived risks and risk management factors do you think are affecting the e-commerce in South Africa?

Answer Here:

5. In terms of percentage, how many of your customers do you service through e-commerce?

Answer Here:

6. What do you think are the tools and techniques that can be used to mitigate perceived risk to develop a framework for risk management?

Answer Here:

7. Have you experienced e-commerce issues or challenges that needed the attention of law enforcement agents? Is so, what was your experience in dealing with law enforcement agents?

Answer Here:

8. What is your opinion regarding the applicable laws, regulations and framework that is used to combat cybercrimes?

Answer Here:

9. In your opinion, do you think that South African laws and regulations are sufficient to deal with cybercrimes?

Answer Here:

10. What advice can you give about how South African can deal with cybercrimes relating to e-commerce?

Answer Here:

11. What impact is e-commerce cybercrimes have in your business?

Answer Here:

12. Can you recommend a solution that can be used to mitigate e-commerce risk management?

Answer Here:

13. What do you think are the impacts of perceived risks on the quality of service delivery of online shopping in South Africa?

Answer Here:

Conclusion

- Thank you for participating.
- Your opinions will be a valuable asset to the study.
- I hope you have found the questions interesting.
- I would like to remind you that any comments featuring in this report will be anonymous.

Thank you.

End.

8.3. ANNEXURE C: Researchers Informed Consent Letter

To Whom It May Concern

I am writing to request your consent to conduct a research study titled "Developing an e-commerce risk management framework for online shopping in South Africa" as part of my doctoral research project at North West University. The purpose of this letter is to seek permission to access the necessary resources and participants for my study.

The primary aim of my research is to contribute to the field of e-commerce by developing a comprehensive risk management framework tailored to the specific challenges faced by online shoppers in South Africa. As the e-commerce landscape continues to evolve, it is imperative to address the unique risks and vulnerabilities that consumers encounter in this digital environment. By conducting this study, I hope to provide valuable insights that can inform the development of effective risk management strategies for both businesses and consumers alike.

The research methodology will involve a combination of qualitative and quantitative approaches, including surveys, interviews, and data analysis. Participants will be selected based on their experience and involvement in online shopping activities within South Africa. All data collected will be treated with the utmost confidentiality and used solely for research purposes.

I assure you that this study will adhere to the highest ethical standards, including obtaining informed consent from all participants and ensuring their anonymity and privacy throughout the research process. Additionally, any findings derived from this study will be presented objectively and disseminated for academic purposes only.

Sincerely,

Tshepo Alex Malapane
PhD Candidate
North West University

8.4. ANNEXURE D: Ethical Clearance Approval

Private Bag X1290, Potchefstroom
South Africa 2520

Tel: 018 299-1111/2222
Fax: 018 299-4910
Web: http://www.nwu.ac.za

Senate Committee for Research Ethics
Tel: 018 299-4849
Email: nkosinathi.machine@nwu.ac.za

21 June 2022

ETHICS APPROVAL LETTER OF STUDY

Based on approval by the **Economic and Management Sciences Research Ethics Committee (EMS-REC)** on 27/05/2022, Round Robin the Economic and Management Sciences Research Ethics Committee hereby **approves** your study as indicated below. This implies that the North-West University Senate Committee for Research Ethics (NWU-REC) grants its permission that, provided the special conditions specified below are met and pending any other authorisation that may be necessary, the study may be initiated, using the ethics number below.

Study title: Developing an e-commerce risk management framework through perceived risk analysis for South African online shopping
Study Leader/Supervisor (Principal Investigator)/Researcher: Dr K Ndlovu – PhD in Business Administration
Student: Malapane, TA (36868957)

Ethics number: N W U - 0 0 6 6 7 - 2 2 - A 4
Institution Study Number Year Status

Status: S = Submission; R = Re-Submission; P = Provisional Authorisation; A = Authorisation

Application Type:
Commencement date: 21/06/2022 **Risk:** Low
Expiry date: 21/06/2023
Approval of the study is initially provided for a year, after which continuation of the study is dependent on receipt and review of the annual (or as otherwise stipulated) monitoring report and the concomitant issuing of a letter of continuation.

Special in process conditions of the research for approval (if applicable):

•

General conditions:

While this ethics approval is subject to all declarations, undertakings and agreements incorporated and signed in the application form, the following general terms and conditions will apply:

- *The study leader/supervisor (principle investigator)/researcher must report in the prescribed format to the EMS-REC:*
  - *annually (or as otherwise requested) on the monitoring of the study, whereby a letter of continuation will be provided, and upon completion of the study; and*
  - *without any delay in case of any adverse event or incident (or any matter that interrupts sound ethical principles) during the course of the study.*
- *The approval applies strictly to the proposal as stipulated in the application form. Should any amendments to the proposal be deemed necessary during the course of the study, the study leader/researcher must apply for approval of these amendments at the EMS-REC, prior to implementation. Should there be any deviations from the study proposal without the necessary approval of such amendments, the ethics approval is immediately and automatically forfeited.*
- *Annually a number of studies may be randomly selected for an external audit.*
- *The date of approval indicates the first date that the study may be started.*

n the interest of ethical responsibility, the NWU-SCRE and EMS-REC reserves the right to:

- *request access to any information or data at any time during the course or after completion of the study;*
- *to ask further questions, seek additional information, require further modification or monitor the conduct of your research or the informed consent process;*
- *withdraw or postpone approval if:*
  - *any unethical principles or practices of the study are revealed or suspected;*
  - *it becomes apparent that any relevant information was withheld from the EMS-REC or that information has been false or misrepresented;*
  - *submission of the annual (or otherwise stipulated) monitoring report, the required amendments, or reporting of adverse events or incidents was not done in a timely manner and accurately; and / or*
  - *new institutional rules, national legislation or international conventions deem it necessary.*
- *Please note that the ethics approval of this application is subject to the Covid-19 protocols.*

The EMS-REC would like to remain at your service as scientist and researcher, and wishes you well with your study. Please do not hesitate to contact the EMS-REC or the NWU-SCRE for any further enquiries or requests for assistance.

Yours sincerely,

Mark Rathbone

Digitally signed by Mark Rathbone
DN: cn=Mark Rathbone, o=North-West University, ou=Business management, email=mark.rathbone@nwu.ac.za, c=ZA
Date: 2022.06.22 14:26:32 +02'00'

Prof Mark Rathbone
Chairperson: NWU Economic and Management Sciences Research Ethics Committee

8.5. ANNEXURE E: Editor's Letter

Dr Angela L Mabena
Professional Translation & Editing Services
16 Landsdowne Place,
Richmond Hill,
Port Elizabeth
c/o Department of Language and Social Sciences Education
NMU
Email: thelanguageeditor@yahoo.com
Cell: +27 65 632 5246

15/01/2024

To Whom It May Concern

This is to confirm that I have read and edited the thesis titled ***"Developing an e-commerce risk management framework for online shopping in South Africa*** "by Tshepo Alex Malapane, student number (36868957) under the supervision of Dr Kaizer Ndlovu. I have looked at the following aspects:

- Referencing
- Corrected spelling, grammatical and punctuation errors
- Checked for problems in parallelisms, tense and conjugations.
- Eliminated improper language and poor word choice.
- Ensured consistency in page numbering.

Do not hesitate to contact me if the need arises.

Many thanks and regards,

Dr. A Mabena (PR: 7664434)

Member: English Academy of Southern Africa (Council member, 2016-)
Research Fellow: School of Languages and Communication Studies, University of Limpopo (2017)