Journal of Economics, Business, and Accountancy Ventura Vol. 27, No. 2, August – November 2024, pages 217-233

Managing Risk in the Digital Era: A Generational Approach-Z on Personal Risk Management

Amelia Setiawan*, Samuel Wirawan, Hamfri Djajadikerta, Sandra Faninda

Parahyangan Catholic University, Bandung, Jawa Barat, Indonesia

A R T I C L E I N F O

Article history:
Received: June 27, 2023
Revised: August 30, 2024;
September 10, 2024;
September 16, 2024;
September 20, 2024
Accepted: September 23, 2024

JEL Classification:
M15, M49, D81

DOI:
10.14414/jebav.v27i2.3909

Keywords:
Personal risk management,
Generation Z,
Concern for privacy,
Perceived threat,
Internet self-efficacy

A B S T R A C T

Risk management should be applied not only at the corporate level but also on a personal level. As technology becomes increasingly integral to daily life, implementing personal risk management in digital activities warrants examination. This study explores personal risk management within the context of online shopping. It investigates factors influencing personal risk management, including privacy concerns, perceived security threats, and internet self-efficacy. The study focuses on individuals from Generation Z, the first generation to grow up in a fully digital environment. Data were collected through online questionnaires, yielding 972 responses, of which 466 were analyzed further. The data were processed using SEM-PLS. The findings indicate that privacy concerns, perceived threats, and internet self-efficacy directly impact personal risk management, which in turn directly influences purchase intentions. This research offers valuable insights for regulators in crafting digital security regulations, for individuals in evaluating and enhancing their personal risk management strategies, for online retailers in designing robust data security measures, and for researchers as a contribution to the limited literature on this topic.

A B S T R A K

Manajemen risiko seharusnya diterapkan tidak hanya pada tingkat perusahaan tetapi juga pada tingkat pribadi. Seiring dengan semakin pentingnya teknologi dalam kehidupan sehari-hari, penerapan manajemen risiko pribadi dalam aktivitas digital perlu diteliti. Studi ini mengeksplorasi manajemen risiko pribadi dalam konteks belanja online. Penelitian ini menyelidiki faktor-faktor yang mempengaruhi manajemen risiko pribadi, termasuk kekhawatiran privasi, ancaman keamanan yang dirasakan, dan efikasi diri internet. Studi ini berfokus pada individu dari Generasi Z, generasi pertama yang tumbuh dalam lingkungan yang sepenuhnya digital. Data dikumpulkan melalui kuesioner online, menghasilkan 972 tanggapan, di mana 466 di antaranya dianalisis lebih lanjut. Data diproses menggunakan SEM-PLS. Temuan menunjukkan bahwa kekhawatiran privasi, ancaman yang dirasakan, dan efikasi diri internet memiliki dampak langsung pada manajemen risiko pribadi, yang pada gilirannya secara langsung mempengaruhi niat pembelian. Penelitian ini menawarkan wawasan berharga bagi regulator dalam merancang regulasi keamanan digital, bagi individu dalam mengevaluasi dan meningkatkan strategi manajemen risiko pribadi mereka, bagi pedagang ritel online dalam merancang langkah-langkah keamanan data yang kuat, dan bagi peneliti sebagai kontribusi terhadap literatur yang terbatas pada topik ini.

1. INTRODUCTION

Industry 5.0 represents an industrial revolution characterized by the collaboration between humans and machines, aiming to enhance production efficiency with a focus on human-centric and sustainable practices (Adel, 2022; Nikiforova et al., 2022). This collaboration inherently involves the dissemination of information, including personal data, which should be carefully managed to prevent unauthorized exposure. While the benefits are significant, it is crucial to recognize the risks associated with maximizing human-machine collaboration. Often, individuals perceive risk management as a responsibility of corporations or governments, rather than a personal obligation (Kozarevi et al., 2015; Viola et al., 2023). However, risk management is a responsibility shared by individuals at personal, organizational, and macro levels.

* *Corresponding author, email address: amelias@unpar.ac.id*

Research on personal risk management is limited, typically focusing on financial or health management risks (Ajupov et al., 2019; M. A. Fox et al., 2021). There is a notable gap in studies addressing personal risk management related to data security in the context of digitalization. Digitalization has permeated various sectors due to its numerous advantages. Social media, in particular, plays a crucial role in transactions, especially for Generation Z, whose unique shopping behaviors make it a vital tool for marketing products and brands (Febrian et al., 2022; Nurhadi et al., 2022). Consumer buying patterns have shifted from traditional to online channels, facilitated by easy access to digital technology and global markets (Moon et al., 2021). Despite general awareness of data protection's importance, many individuals lack the resources to assess information security risks, implement mitigation strategies, or participate in awareness training programs (Nicolas-Rocca & Burkhard, 2019b). Numerous incidents involving personal data breaches have occurred, with over 35 billion records compromised in more than 9,000 publicly disclosed incidents (IT Governance, 2024). A survey predicts the global annual cost of cybercrime will reach $9.5 trillion USD in 2024 (Bluefin, 2024). Effective risk management begins with analyzing critical information, conducting risk assessments, evaluating alternatives, and selecting the best course of action (Dobrowolski et al., 2022).

Generational differences significantly influence behavior in digital transactions. Older generations tend to trust government measures for transaction security, while younger generations rely more on peer recommendations (Adiani et al., 2021). According to the Central Bureau of Statistics, Generation Z constitutes 27.95 percent of Indonesia's population (Fajri, 2022). This generation's distinctive e-commerce behaviors warrant further study (Mubarok, 2022). Online shopping intent is a key variable for testing risk management applications, as Generation Z frequently engages in online shopping. This study focuses on Generation Z, digital natives born between 1990 and 2005, who have grown up with the internet and are adept at online shopping. This generation is characterized as tech-savvy, empowered, prematurely mature, protected, risk-averse, and pampered (Dang et al., 2020; Dobrowolski et al., 2022; Kien Men & Noordin, 2019). The research examines the application of risk management in online shopping activities.

Few studies have explored digital self-efficacy in Generation Z (Lee, 2021). This study aims to assess Generation Z's awareness of personal risk management in digital transactions and its link to purchase intentions. Specifically, it investigates whether privacy concerns, perceived threats, and internet self-efficacy influence personal risk management, and whether personal risk management affects purchase intentions. The research contributes to raising individual awareness about the importance of protecting personal data as a form of personal risk management. Regulators should enforce existing rules to ensure effective personal data protection and regulate data collection, processing, and storage practices. This study is limited to personal risk management related to digital security, excluding financial security, due to the scarcity of research in this area, highlighting the need for increased awareness among individuals and regulators.

2. THEORETICAL FRAMEWORK AND HYPOTHESES

2.1. Theoretical Foundations

This research is grounded in three foundational theories: risk management theory (Ajupov et al., 2019), the Theory of Reasoned Action (TRA) by Fishbein and Ajzen (1975) (Maity et al., 2019; H. Setiawan & Iramani, 2023), and prospect theory (Singh et al., 2023). Internal control theory, which gained popularity in 1992, emphasizes the necessity of risk management as a component for achieving organizational goals (Mu et al., 2023). However, the application of this theory to personal risk management is not straightforward. Therefore, this study primarily relies on risk management theory, which is based on three core concepts: utility, regression, and diversification (Ajupov et al., 2019; Gilliam et al., 2010). According to this theory, the utility method informs decision-making by emphasizing the importance of considering the magnitude of different outcomes (Ajupov et al., 2019).

The TRA is used to understand motivations behind normative behavior and computer usage (A. Habib et al., 2022; Maity et al., 2019; Al-Jabri et al., 2020; Castillo-Vergara et al., 2022). TRA explains the intention to use information technology through behavioral intentions and subjective norms (Castillo-Vergara et al., 2022; A. Setiawan et al., 2021). In this study, which links personal risk management to privacy awareness, TRA is particularly relevant (Sommestad et al., 2019). Prospect theory, which contrasts with traditional theories, posits that individuals do not always utilize all available information when making decisions; instead, they are influenced by their perceptions of personal benefits (Singh et al., 2023). This theory is fre-

quently applied in research on personal risk management (Baláž, 2021; Howat-Rodrigues et al., 2019; Kuzniak et al., 2015; Nobre et al., 2016).

Risk management involves assessing and managing identified risks (Islam et al., 2017). It is not solely a corporate responsibility (Studley, 2021; Zoran, 2018) but should also be applied at the personal level. Human factors are often the weakest link in a company's security system, with 64 percent of data breaches attributed to human error and system disruptions (Kennedy, 2016). Social engineering, a common attack on corporate data, involves deceiving users into divulging confidential or sensitive information (ISACA, 2015). This underscores the importance of applying risk management to secure personal data, a valuable area of research. Individuals often mistakenly view risk management as a responsibility only at the macro level (Yang, 2022).

2.2. Hypotheses Development

In the early 2000s, personal risk encompassed the risk of illness or accident, unemployment, premature death, and insufficient pension funds (Charupat et al., 2012). Personal risk management emerged as a component of financial theory, linking personal financial planning with risk management, beginning with Elger's publication (Elger, 2004). Initially, personal risk management focused solely on financial planning (Charupat et al., 2012; Elger, 2004). Over time, it expanded to include insurance, covering not only life insurance but also asset protection and financial risks (Armstrong, 2017; Rejda et al., 2022). With technological advancements and increasing reliance on technology, there is a growing need for personal risk management that extends beyond financial management to encompass a broader scope (Li & van Rooij, 2022; Pedersen & Nagengast, 2008; Rosique-Blasco et al., 2018; Studley, 2021). Research conducted in Sri Lanka highlights a significant disparity between individuals with and without insurance literacy and trust in insurance products. Consequently, it is strongly recommended that the government, regulators, and decision-makers in Sri Lanka foster a culture of personal risk management through education at the school, college, and university levels. This initiative aims to raise awareness of the benefits and importance of insurance solutions, thereby enhancing the quality of life in Sri Lanka and alleviating the government's social cost burden (Weedige et al., 2019).

2.2.1. Privacy Concern and Personal Risk Management

The vast amount of information available about individuals on social media poses cyber threats, ranging from the exposure of personal data to the leakage of confidential company information (Fataliyev & Mehdiyev, 2020; A. Setiawan et al., 2021; Windiarti et al., 2020). Research in Indonesia indicates that 71 percent of Generation Z respondents have only an average level of awareness regarding these risks, highlighting a generally low awareness among smartphone users in the country (Akraman et al., 2018). As reliance on technology grows, more personal information is shared online. According to the utility concept in risk management theory, the increasing dissemination of personal data necessitates greater attention to the potential impacts of various outcomes. Previous studies support this notion. Research conducted in Hong Kong found that an individual's approach to managing personal risk influences their privacy concerns when shopping online (Hong et al., 2021). Similar findings have been reported in Europe (Gimpel et al., 2018), Taiwan (Wang, 2019), Ireland (G. Fox et al., 2022), Germany (Hoppe et al., 2021), and Slovenia (Zlatolas et al., 2019). Based on these insights, the first hypothesis of this study is:

H1. Concern for privacy affects personal risk management.

2.2.2. Perceived Threat and Personal Risk Management

Technology risk is a key component of perceived security threats (Pruss, 2006). As reliance on the internet and digitalization increases, so do technology-related risks, such as the theft of personal data for fraudulent transactions, leading to financial losses. According to the Theory of Reasoned Action (TRA), perceived risk reflects a consumer's sense of uncertainty and potential negative outcomes when engaging in online shopping. However, prospect theory suggests that individuals may not use all available information due to their perception of the benefits they expect to gain from their decisions. Despite awareness of threats and risks, people often prefer online shopping due to its flexibility, competitive pricing, and various conveniences. Thus, the perceived benefits can significantly influence decision-making. Research conducted in Korea (Jang & Kim, 2022) found that online purchase intentions are negatively affected by security threats, privacy concerns, performance risks, and social risks from malicious use. Similar findings have been reported in studies from Saudi Arabia (Mahlous, 2023), China (Tang et al., 2021; Zang et al., 2022), England (Diers-Lawson et al.,

2021), Vietnam (Nguyen et al., 2022), and Italy (Esposito et al., 2022). Based on these insights, the second hypothesis of this study is:
H2. The perceived threat affects personal risk management.

2.2.3. Internet Self-Efficacy and Personal Risk Management
According to the TRA, an individual's ability significantly influences their decision-making process. When making decisions, individuals evaluate various possibilities and consider the potential outcomes. A key concept in risk management theory is the application of regression functions. This concept suggests that individuals assess the likelihood of risks and predict the consequences of each available option. Integrating these theories, it can be inferred that an individual's capability to protect their personal data impacts their approach to personal risk management. Consumers with proficient technological skills in internet use and digital transactions tend to have greater confidence in managing risks associated with online shopping (S. Habib & Hamadneh, 2021). Those with strong technological competencies, particularly in internet self-efficacy, are better equipped to access information on cybersecurity, which influences their perception of risks, including performance, financial, and transaction risks (Kim & Lennon, 2010). Based on these premises, the third hypothesis of this study is:
H3. Internet self-efficacy affects personal risk management.

2.2.4. Personal Risk Management and Intention to Purchase
Online purchase intention refers to an individual's desire to make purchases via the internet (Moslehpour et al., 2018; Sujarwo & Indriani, 2022). People are inclined to shop from virtual stores for various reasons, including the availability of product and service catalogs, search functionalities, trust in websites, price comparison options, and online payment systems (Moslehpour et al., 2018). Research conducted in Bolivia identifies three risks that influence online purchase intentions: the risk of information misuse, the risk of not receiving the expected product benefits, and the risk of functional inefficiencies (Carvache-Franco et al., 2022). Similarly, a study in Malaysia (Kamalul Ariffin et al., 2018) highlights financial risk, product risk, security risk, and psychological risk as factors affecting online shopping intentions. Risk perception also plays a significant role in influencing online shopping behaviors, as demonstrated by studies in China (Liu et al., 2022) and India (S. Habib & Hamadneh, 2021). These findings are consistent with previous research (Gimpel et al., 2018; Wang, 2019). Based on these insights, the fourth hypothesis of this study is:
H4. Personal risk management affects the intention to purchase.

The study framework, informed by previous research and foundational theories for each variable, is illustrated in Figure 1.

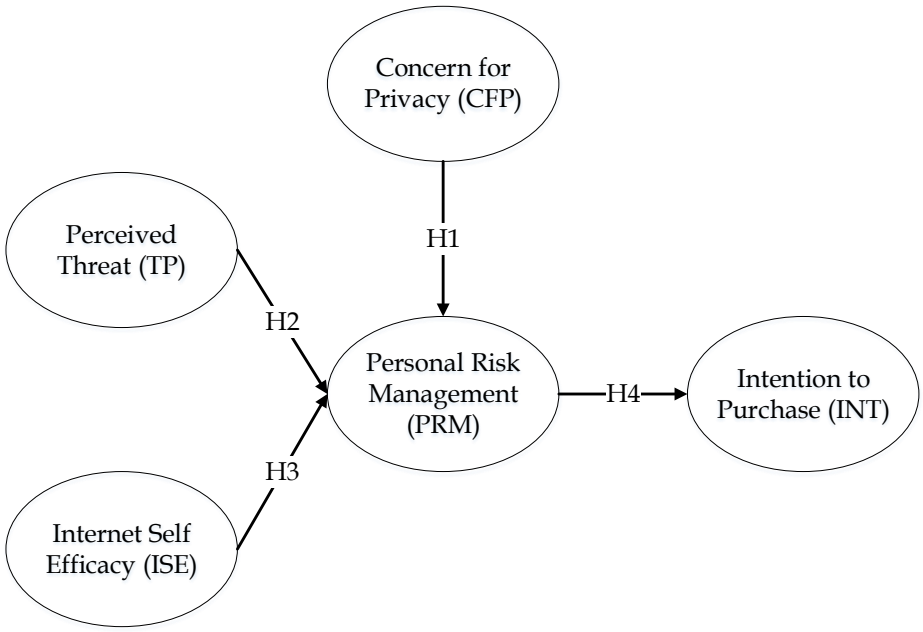

Figure 1. Research framework

3. RESEARCH METHOD

This quantitative descriptive study employed an online survey methodology. A purposive sampling method was used to select participants, focusing on individuals belonging to the Generation Z cohort, born between 1995 and 2015 (Dobrowolski et al., 2022; Goldbach et al., 2023; Iswari & Budiyono, 2024; Tri Marhendra Rahardyan et al., 2023). The study centers on personal risk management in the context of the digital era, making Generation Z, who are digital natives, the most appropriate population for this research.

The research utilized a questionnaire with items adapted from previous studies (Cromer, 2015; Dang et al., 2020; Junglas et al., 2008; Youn, 2009). The questionnaire comprised two main sections: the first gathered demographic information (gender, age, and location), and the second focused on variables pertinent to the study. Out of 972 respondents, 466 were eligible for statistical analysis, as the remainder had never shopped online or did not belong to Generation Z. The measurement of variables was based on prior research, with modifications to align with the study's objectives. Details of all variables, dimensions, and indicator statements are provided in Appendix 1.

The endogenous variables in this study are personal risk management (PRM) and purchase intention (INT). Indicators for personal risk management were adapted from previous research (A. Setiawan & Haryanto, 2024; Youn, 2009) to assess the willingness to seek knowledge for securing personal data. Indicators for purchase intention were adapted from Dang et al. (2020) to evaluate preferences and habits related to online shopping. These variables were measured using a Likert scale ranging from 1 to 5. The exogenous variables include Concern for Privacy (CFP), Perceived Threat (TP), and Internet Self-Efficacy (ISE). Concern for Privacy, adapted from Junglas et al. (2008), was measured by indicators related to privacy from mobile providers, phone location data, and awareness of personal data security. Perceived Threat, adapted from Cromer (2015), was measured by indicators of perceived threat probability and severity. Internet Self-Efficacy, also adapted from Cromer (2015), was measured by indicators of internet self-efficacy. These variables were similarly measured using a Likert scale from 1 to 5. Table 1 presents the operationalization of these variables.

Data collection involved distributing online questionnaires to the target respondents. For a large population with a 95% confidence level, a minimum sample size of 384 is required (Israel, 2003; Oribhabor & Anyanwu, 2019). This study collected data from 466 respondents. The online questionnaire was distributed from March to June 2022 using Google Forms, and the link was shared via various social networking platforms. The data were analyzed using Structural Equation Modeling (SEM), a multivariate analysis technique that integrates elements of simultaneous equation systems, path analysis, and regression analysis with factor analysis (Saluza & Sartika, 2019; Wardhani et al., 2020). The Partial Least Squares (PLS) approach was selected for this study because it accommodates both formative and reflective indicators and can be applied without stringent assumptions (Silva et al., 2019; Solimun, 2020; Wardhani et al., 2020). To assess convergent validity, the research instrument employed a Loading Factor threshold of greater than 0.7 and an Average Variance Extracted (AVE) value exceeding 0.50 (Hair, Risher, et al., 2019). Discriminant validity was evaluated using the Heterotrait-Monotrait (HTMT) ratio, ensuring that the confidence interval value does not reach 1 for any combination of constructs (Hair, Black, et al., 2019; H. Setiawan & Iramani, 2023).

Table 1. Variable operationalization

Variable	Domain	Scale
Concern for Privacy	Privacy from mobile provider	Likert
	Phone location data	
	Awareness of personal data security	
Perceived Threat	Threat of personal data theft	Likert
	Private email hacking threats	
Internet Self-Efficacy	Internet self Efficacy	Likert
Personal Risk Management	Privacy statement	Likert
	Protection of personal data	
Intention to Purchase	Preference for online shopping	Likert
	Online shopping habits	

4. DATA ANALYSIS AND DISCUSSION

Table 2 presents the demographic data, including the percentage distribution of respondents by gender, age, and location. Descriptive statistics, such as minimum, maximum, mean, and standard deviation values, are detailed in Table 3. The classification for each criterion was developed by dividing the range between the lowest and highest values by the number of categories (Syarif et al., 2023). This study uses four categories, resulting in a category range of 0.75. The category scale is defined as follows: 1.00-1.75 (very low); 1.76-2.50 (low); 2.51-3.25 (high); 3.26-4.00 (very high). The calculations for minimum, maximum, mean, and standard deviation values were performed using Microsoft Excel.

This study examines five variables: Concern for Privacy (CFP), Perceived Threat (TP), Internet Self-Efficacy (ISE), Personal Risk Management (PRM), and Purchase Intention (INT). The descriptive statistics are summarized in Table 3. CFP has a minimum value of 1 and a maximum value of 4, with a mean of 3.14 and a standard deviation of 0.68, placing it in the high category. This indicates that respondents have a high concern for privacy. TP, which evaluates respondents' perceptions of risk likelihood and severity, has a minimum value of 1 and a maximum value of 4, with a mean of 2.99 and a standard deviation of 0.76, also in the high category. This suggests that respondents perceive a high risk associated with technology-based threats.

ISE measures respondents' internet browsing and security skills, with a minimum value of 1 and a maximum value of 4, and a mean of 2.94, which is in the high category. However, this is the lowest mean among the five variables, indicating that while respondents consider their internet-related capabilities to be high, it is relatively lower compared to other variables. PRM has a minimum value of 1 and a maximum value of 4, with a mean of 3.02 and a standard deviation of 0.75, placing it in the high category. This suggests that respondents believe they have a high ability to manage risk. Lastly, INT has a minimum value of 1 and a maximum value of 4, with a mean of 3.07 and a standard deviation of 0.67, also in the high category, indicating a strong desire among respondents to shop online.

The structural model in this study incorporates three exogenous variables—concern for privacy, threat perception, and internet self-efficacy—and two endogenous variables—personal risk management and purchase intention. Evaluating the results of Partial Least Squares Structural Equation Modeling (PLS-SEM) involves three key steps: 1) examining the measurement model, 2) assessing the structural model, and 3) interpreting the PLS-SEM results. Validity testing for reflective indicators was conducted by evaluating the correlation between indicator scores and construct scores using the Smart PLS software. Reflective measurement theory was applied because all indicators selected for a construct reflect the latent construct. Each indicator is highly correlated, allowing for interchangeability and removal without altering the construct's meaning (Hair, Black, et al., 2019). Convergent validity measures the correlation of two or more indicators for a construct (Hair, Black, et al., 2019). The evaluation of the reflective measurement model consists of four stages: 1) examining the indicator loadings, 2) assessing internal consistency reliability, 3) assessing convergent validity for each construct measure, and 4) assessing discriminant validity.

The first step in evaluating the measurement model involves examining the indicator loadings. Outer loading scores above 0.70 are recommended, as they indicate that the construct explains more than 50% of the indicator's variance (Bai et al., 2022; Hair, Risher, et al., 2019). In this study, as shown in Table 3, all outer loading scores exceed 0.70, thus providing acceptable item reliability. The second step involves assessing internal consistency reliability, commonly tested using composite reliability (Hair, Risher, et al., 2019). Composite reliability is considered more accurate than Cronbach's alpha because it accounts for item weighting (Hair, Risher, et al., 2019).

Table 2. Respondent characteristics

Characteristics	Detail	Respondents	Percentage
Gender	Male	170	0.36
	Female	296	0.64
Year of birth	1990-1995	61	0.13
	1996-1999	122	0.26
	2000-2005	283	0.61
Demographic Location	Sumatera	132	0.28
	Jawa-Bali	84	0.18
	Kalimantan	242	0.52
	Sulawesi	5	0.1
	Papua	3	0.1

Values between 0.7 and 0.9 are deemed satisfactory, while values above 0.95 may indicate redundancy, reducing construct validity. In this study, as shown in Table 3, the composite reliability values range from 0.82 to 0.92, indicating satisfactory internal consistency reliability. Cronbach's alpha can serve as an alternative measure of internal consistency reliability, typically yielding lower values than composite reliability (Hair, Risher, et al., 2019). A minimum value of 0.70 is acceptable. In this study, as shown in Table 3, Cronbach's alpha values range from 0.70 to 0.89, confirming that the internal consistency reliability test meets the required standards.

The third step involves assessing convergent validity for each construct measure. Convergent validity refers to the extent to which a construct explains the variance of its items (Hair, Risher, et al., 2019). The average variance extracted (AVE) is used to evaluate a construct's convergent validity. A loading value greater than 0.5 to 0.7 indicates that the construct accounts for at least 50% of the variance in its items (Alotaibi & Alshahrani, 2022; Bai et al., 2022; Liao et al., 2022; Maswadi et al., 2022; P Panca et al., 2017; Shiau et al., 2019). In this study, as shown in Table 3, the AVE values range from 0.60 to 0.75, confirming that the convergent validity test meets the required standards. This indicates that the research instrument is valid. The fourth step in evaluating the measurement model involves assessing discriminant validity. The Heterotrait-Monotrait (HTMT) ratio is the most commonly used metric for this purpose.

Table 3. Statistic descriptive-outer mode & convergent validity test results

Construct	Indicator	Loading	CR	Cronbach's Alpha	AVE	Mean	Min	Max	Std Dev
Privacy Concern (CFP)	CFP1	0.79	0.82	0.70	0.61	3.14	1	4	0.69
	CFP2	0.78							
	CFP5	0.77							
Threat Perception (TP)	PTP1	0.85	0.92	0.89	0.69	2.99	1	4	0.76
	PTP2	0.88							
	PTP3	0.86							
	PTS1	0.77							
	PTS2	0.79							
Internet Self Efficacy	SE1	0.84	0.92	0.89	0.75	2.94	1	4	0.71
	SE2	0.88							
	SE3	0.89							
	SE4	0.83							
Personal Risk Management (PRM)	PRM1	0.88	0.88	0.80	0.72	3.02	1	4	0.75
	PRM2	0.87							
	PRM3	0.78							
Purchase Intention (INT)	Int1	0.74	0.82	0.71	0.60	3.07	1	4	0.67
	Int2	0.70							
	Int3	0.88							

Table 4. Discriminant validity (HTMT)

Variable	CFP	INT	ISE	PRM	TP
Concern for Privacy (CFP)					
Purchase Intention (INT)	0.27				
Internet Self-efficacy (ISE)	0.21	0.41			
Personal Risk Management (PRM)	0.74	0.26	0.35		
Perceived Threat (TP)	0.75	0.23	0.21	0.55	

Table 5. R-squared value

Variable	R Square	Q-squared value
Purchase Intention	0.05	0.02
Personal Risk Management	0.40	0.28

The HTMT ratio is calculated as the average value of item correlations between different constructs, divided by the geometric mean of the average correlations for items within the same construct. A reference value below 0.90 indicates adequate discriminant validity (Hair, Risher, et al., 2019). In this study, as shown in Table 4, all HTMT ratios range from 0.21 to 0.75, which is below the 0.90 threshold. Therefore, it can be concluded that each construct is empirically distinct from the others in the structural model.

After confirming the measurement model's adequacy, the next step in evaluating PLS-SEM results is to assess the structural model. This assessment involves several standard criteria, including the coefficient of determination (R^2), the cross-validated redundancy measure (Q^2) obtained through blindfolding, and the statistical significance and relevance of the path coefficients. The R-squared value (R^2) measures the extent to which an independent latent variable influences a dependent latent variable. R^2 values range from 0 to 1, with higher values indicating greater explanatory power. Generally, R^2 values of 0.75, 0.50, and 0.25 are considered substantial, moderate, and weak, respectively. However, acceptable R^2 values can vary by context; in some fields, such as predicting stock returns, an R^2 as low as 0.10 may be deemed satisfactory (Hair, Risher, et al., 2019).

The R^2 values for the endogenous variables in this study are presented in Table 5. As shown, the R^2 value for purchase intention is 0.05, while for personal risk management, it is 0.40. This indicates that personal risk management accounts for only 5% of the variance in purchase intention, suggesting it is not a primary factor influencing respondents' decisions to make online purchases. Conversely, the R^2 value of 0.40 for personal risk management suggests that 40% of its variance is explained by concern for privacy, perceived threat, and internet self-efficacy. Therefore, it can be concluded that the model has a low goodness of fit for explaining purchase intention and a moderate goodness of fit for explaining personal risk management.

Another method to evaluate the predictive accuracy of the PLS path model is by calculating the Q-square value (Q^2). This metric is obtained through the blindfolding procedure, which involves systematically omitting data points, replacing them with the mean, and then estimating the model parameters. A Q^2 value greater than zero for a specific endogenous construct suggests that the structural model has predictive accuracy for that construct, indicating a better fit between the model and the data (Hair, Risher, et al., 2019; Syarif et al., 2023). Q^2 values above 0, 0.25, and 0.50 represent small, medium, and large predictive relevance, respectively, of the PLS path model (Hair, Risher, et al., 2019). In this study, as shown in Table 5, the Q^2 value for purchase intention is 0.02, while for personal risk management, it is 0.28. These values indicate that the model has only small predictive relevance for purchase intention, whereas it has medium predictive relevance for personal risk management. After evaluating the model's explanatory and predictive power, the final step in assessing the structural model is to examine the statistical significance and relevance of the path coefficients. The results of the PLS algorithm processing and bootstrapping, which assess the significance of the path coefficients, are presented in Figure 2 and Table 6.

A research hypothesis is considered valid if the p-value is less than 0.05. The detailed results, presented in Table 6, are based on bootstrapping estimation, indicating that all the hypotheses in this study are valid. Bootstrapping estimation also provides a robustness check. Recent research has introduced additional methods for evaluating the robustness of PLS-SEM results (Hair, Risher, et al., 2019). These methods focus on either the measurement model or the structural model. One robustness check involves assessing the linearity of the relationship between exogenous and endogenous variables by evaluating the p-value of the squared term for the exogenous variables. If the p-value for the squared term is not significant, it suggests that the relationship between the variables is linear (Sudaryono et al., 2024). This confirms the validity of all the hypotheses in this research. Additionally, bootstrapping estimation provides a robustness check.

The intersection of personal risk management and technological advancements, particularly the extensive use of digitalization, is intricately linked to privacy concerns. In this study, privacy concerns were evaluated by assessing respondents' comfort levels with cellular providers storing personal data, continuously monitoring their location, or sharing location data with third parties.

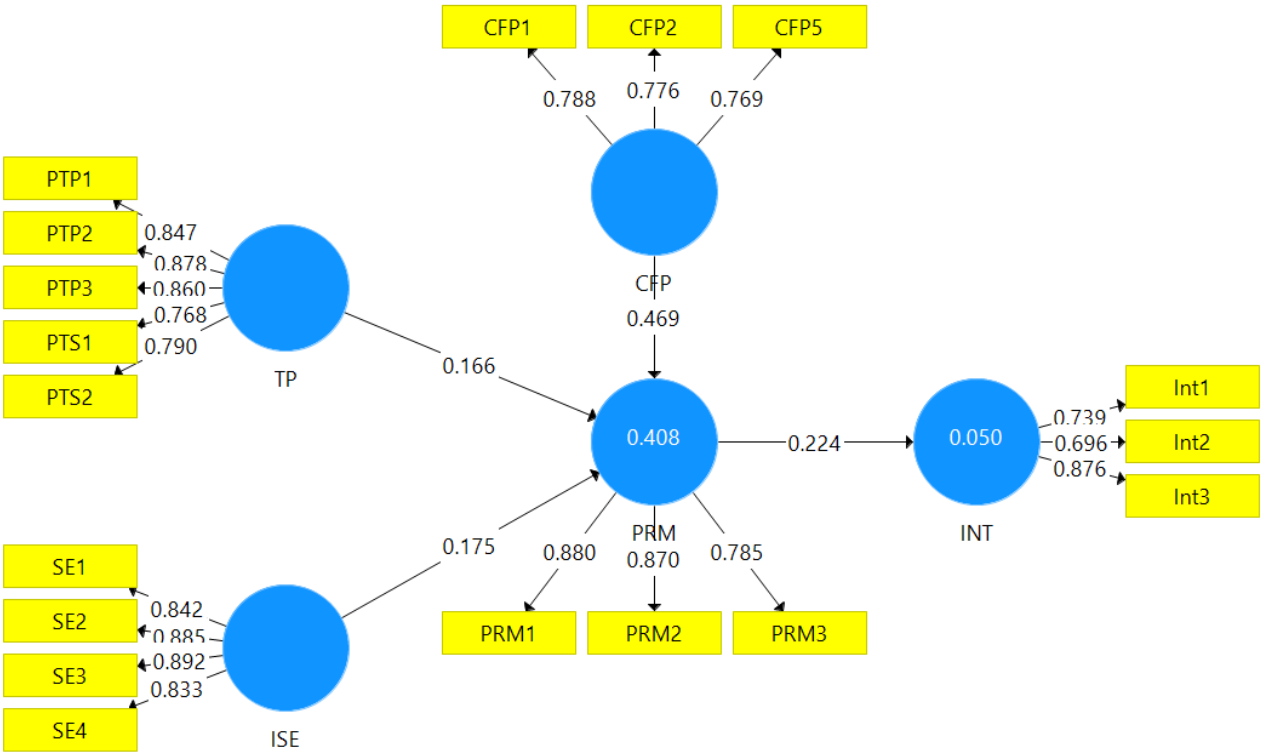

Figure 2. Structural model

Table 6. Bootstrapping estimation

Hypotheses	Variable	Original Sample	T-Statistics	P-Values
H1	Concern for Privacy → Personal Risk Management	0.469	10.513	0
H2	Internet Self-efficacy → Personal Risk Management	0.175	4.41	0
H3	Personal Risk Management → Purchase Intention	0.224	5.575	0
H4	Perceived Threat → Personal Risk Management	0.166	3.329	0.001

Additionally, respondents were evaluated on their proactive efforts to seek information about safeguarding data privacy. Identifying the risks one faces is the initial step in risk management. An individual who is uncomfortable with mobile operators continuously collecting location data demonstrates a significant concern for privacy. For instance, when passing through certain locations, individuals may receive unsolicited promotions or advertisements on their mobile phones, a direct consequence of continuous location monitoring by mobile operators. As illustrated in Figure 2 and Table 6, this study confirms that privacy concerns positively influence personal risk management. These findings align with previous research conducted in Europe (Gimpel et al., 2018; Hong et al., 2021), Taiwan (Wang, 2019), Ireland (Hoppe et al., 2021), and Slovenia (Zlatolas et al., 2019). The study also supports prospect theory, suggesting that individuals may overlook some information due to their focus on future prospects. Consequently, while privacy concerns and other factors moderately explain personal risk management, they have a weak indirect influence on purchase intentions. According to prospect theory, despite privacy concerns and personal risk management, the potential benefits of online purchasing may encourage continued online shopping.

Threats are factors that actively hinder an organization's goal achievement. When an organization has vulnerabilities that can be exploited by these threats, risks emerge. This study examines how individuals perceive threats, particularly regarding personal data theft, account hijacking, or data monitoring. If individuals perceive a threat, it is assumed they are more aware of the risk and manage it accordingly. The study's findings indicate that perceived threats significantly impact personal risk management, consistent with previous research in Saudi Arabia (Mahlous, 2023), China (Tang et al., 2021; Zang et al., 2022), Great Britain

(Diers-Lawson et al., 2021), Vietnam (Nguyen et al., 2022), and Italy (Esposito et al., 2022). Like privacy concerns, perceived threats also support prospect theory.

Individuals with strong internet skills generally understand the risks associated with accessing websites and know how to mitigate these threats. Higher internet self-efficacy correlates with better personal data security and effective personal risk management. This study confirms that internet self-efficacy influences personal risk management, aligning with previous research in China (Liu et al., 2022) and India (S. Habib & Hamadneh, 2021). Similar to privacy concerns, internet self-efficacy supports prospect theory.

Although this study did not focus on purchase intentions, it used them as a practical example to help respondents envision the application of personal risk management in daily life. With a weak explanatory power of 0.02, the influence of personal risk management on purchase intention is relatively low, as respondents generally have not recognized the importance of personal risk management in all life aspects, including online shopping. This study also supports the theory of reasoned action, where various factors influence a person's intention to act. In this context, personal risk management is the direct influence, while privacy concerns, perceived threats, and internet self-efficacy are indirect influences.

Future research could involve practical experiments in online investment, digital payments, or other digital activities involving privacy data. The study's findings are consistent with previous research (Gimpel et al., 2018; S. Habib & Hamadneh, 2021; Kamalul Ariffin et al., 2018; Wang, 2019). Research in Lithuania found that financial literacy significantly impacts personal finance management for Generation Z (Navickas et al., 2014).

To enhance personal data security at both individual and regulatory levels, education or training programs are essential. These programs will increase awareness of data privacy threats, emphasizing the necessity of personal risk management. Such education is particularly crucial for Generation Z (Nicolas-Rocca & Burkhard, 2019a). In this study, privacy concerns, perceived threats, and internet self-efficacy account for 40% of the variance, with other factors influenced by personality traits (Chen et al., 2023; Lissitsa & Kol, 2021; Twumasi Baffour et al., 2019), effective decision-making, self-control, conscientiousness, neuroticism (Ganbat et al., 2021), perceived relevance (availability, accessibility, acceptability, and adaptability), informativeness, perceived expectancy (Mohd Thas Thaker et al., 2021), consumer adaptation to technology, perceived risk in online transactions, consumer trust in online technologies (S. Habib & Hamadneh, 2021), financial, product, security, and psychological risks (Kamalul Ariffin et al., 2018), information (Kim & Lennon, 2010), satisfaction (Kim & Lennon, 2010), risk perception, education (Shin & Park, 2017), and gender (Twumasi Baffour et al., 2019).

5. CONCLUSION, IMPLICATION, SUGGESTION, AND LIMITATIONS

This study examines the relationship between privacy concerns, perceived threats, and internet self-efficacy in the context of personal risk management. To illustrate these relationships in everyday life, the study also considers their impact on online shopping intentions. The findings reveal that privacy concerns, perceived threats, and internet self-efficacy significantly and positively influence personal risk management.

Personal risk management, particularly in the era of technological advancements and widespread digitalization, is closely linked to privacy concerns. The study's results indicate that privacy concerns enhance personal risk management, supporting prospect theory, which suggests that individuals may overlook certain information in favor of potential gains. Consequently, while privacy concerns and other factors provide moderate explanatory power, their effect on purchase intentions is weak and indirect. Thus, despite concerns about privacy and personal risk management, the potential benefits of online shopping encourage individuals to continue making purchases.

A threat is defined as any person or thing that poses a risk of harm or danger. In this study, threat perception is associated with concerns about personal data theft, account hijacking, or monitoring of personal information. As individuals perceive greater threats, they are likely to improve their personal risk management. The findings show that perceived threats influence personal risk management. Like privacy concerns, perceived threats align with prospect theory, offering moderate explanatory power and a weak indirect effect on purchase intentions. This is because individuals often prioritize the benefits of online shopping over perceived threats.

Similarly, an individual's internet self-efficacy affects their personal risk management practices. Higher internet self-efficacy correlates with greater efforts in personal risk management. The study indicates that internet self-efficacy influences personal risk management and aligns with prospect theory, providing

moderate explanatory power and a weak indirect effect on purchase intentions.

The practical implications of privacy concerns, perceived threats, and internet self-efficacy on personal risk management in online shopping are significant for individuals, regulators, and companies. For individuals, understanding and managing privacy concerns and enhancing self-efficacy can lead to safer online transactions. Regulators should develop policies to protect consumer data and raise awareness about digital threats, creating a safer shopping environment. Companies should focus on transparency, data security, and educating consumers about potential risks. By doing so, all parties can strengthen personal risk management and increase trust in online shopping. This research can guide regulators in designing digital security regulations, help individuals assess personal risk management, assist online retailers in enhancing data security, and serve as supporting literature for researchers in this underexplored area.

This study contributes to the existing literature on personal risk management by identifying the influence of privacy concerns, perceived threats, and internet self-efficacy. There is still limited research on personal risk management theories. The findings also support related theories, including risk management theory, the theory of reasoned action, and prospect theory. This research aligns with prospect theory, which posits that individuals may ignore certain information in favor of potential gains. As a result, while privacy concerns and other factors offer moderate explanatory power, their effect on purchase intentions remains weak and indirect. Thus, following prospect theory, despite concerns about privacy and personal risk management, the potential profit from online shopping motivates individuals to continue making purchases. Furthermore, this study supports the utility method as a key concept in risk management, emphasizing the importance of considering the magnitude of different outcomes in decision-making processes.

The factors examined in this study are primarily internal to individuals (privacy concerns, perceived threats, and internet self-efficacy). Future research could incorporate external factors such as economic benefits, perceived value (Kim & Lennon, 2010), perceived usefulness (Sutarso, 2021), government regulation (Adiani et al., 2021), modified cybersecurity risk assessment (Alamri et al., 2023), internal communication through digital channels to reduce risk (Kovaitė et al., 2020), individual risk tolerance (Sheedy & Lubojanski, 2018), customer trust, data security, user interface (Stewart & Jürjens, 2017), data transmission to third parties, and privacy-sensitive data analysis (Chatfield et al., 2017).

Consistent with previous research (Mubarok, 2022), the government's role is crucial in formulating policies that prevent digital transaction incidents and support consumer protection. In this study, online purchase intention was chosen to test the application of risk management, as Generation Z is prevalent in online shopping activities. Another testing alternative could be digital investment or banking.

There are several limitations to this research. First, the focus on a specific sample of Generation Z limits the generalizability of the findings. While this age group was selected for its relevance, it restricts the applicability of the results to populations with diverse socio-demographic backgrounds. Future research should aim for more varied samples across different locations and age groups. Second, the study's parameters, particularly regarding online shopping, pose another limitation. The influence of personal risk management on online shopping intention is categorized as weak, possibly because online shoppers prioritize shopping activities over risk factors. Future studies might consider using other online activities, such as online investment intentions, as experimental tools. Additionally, the three factors selected for this research—privacy concerns, perceived threats, and internet self-efficacy—explain only 40% of personal risk management. Although the model test meets the criteria for model fit, indicating that the factors identified are appropriate for making predictions, the R-square of 40% suggests that the structural model is moderate. Subsequent research could explore other factors such as personality, effective decision-making, self-control, conscientiousness, neuroticism, perceived relevance, informativeness, perceived expectancy, consumer adaptation to technology, perceived risk associated with online transactions, consumer trust in online technologies, financial risk, security risk, psychological risk, satisfaction, risk perception, education, and gender.

REFERENCES

Adel, A. (2022). Future of Industry 5.0 in Society: Human-centric Solutions, Challenges and Prospective Research Areas. *Journal of Cloud Computing*, *11*(1). https://doi.org/10.1186/s13677-022-00314-5

Adiani, W., Aprianingsih, A., & Purwanegara, M. S. (2021). Cashless Society in Progress: Capturing Different Generations' Perspectives toward External Influence in E-Wallet Usage. *Journal of Economics, Business, & Accountancy Ventura*, *24*(2), 205. https://doi.org/10.14414/jebav.v24i2.2677

Ajupov, A., Sherstobitova, A., Syrotiuk, S., & Karataev, A. (2019). The Risk-Management Theory in Modern Economic Conditions. *E3S Web of Conferences*, *110*. https://doi.org/10.1051/e3sconf/201911002040

Akraman, R., Candiwan, C., & Priyadi, Y. (2018). Pengukuran Kesadaran Keamanan Informasi Dan Privasi Pada Pengguna Smartphone Android Di Indonesia. *Jurnal Sistem Informasi Bisnis*, *8*(2), 115. https://doi.org/10.21456/vol8iss2pp115-122

Al-Jabri, I. M., Eid, M. I., & Abed, A. (2020). The Willingness to Disclose Personal Information: Trade-off between Privacy Concerns and Benefits. *Information and Computer Security*, *28*(2), 161–181. https://doi.org/10.1108/ICS-01-2018-0012

Alamri, B., Crowley, K., & Richardson, I. (2023). Cybersecurity Risk Management Framework for Blockchain Identity Management Systems in Health IoT. *Sensors*, *23*(1), 1–39. https://doi.org/10.3390/s23010218

Alotaibi, R. S., & Alshahrani, S. M. (2022). An Extended DeLone and McLean's Model to Determine The Success Factors of E-learning Platform. *PeerJ Computer Science*, *8*, 1–27. https://doi.org/10.7717/peerj-cs.876

Armstrong, A. (2017). Personal Risk Management. *Better Investing*, *January/Fe*, 12–14.

Bai, P., Suresh, S., Ansari, J., & Ahmed, S. (2022). Why Employees are not loyal to their Workplace in Private Sector? *Global Management Journal for Academic & Corporate Studies*, *12*(1), 82–98.

Baláž, V. (2021). Attitudes towards Financial Risks and Portfolio Allocations: Evidence from Large-Scale Surveys1. *Ekonomicky Casopis*, *69*(2), 113–134. https://doi.org/10.31577/ekoncas.2021.02.01

Bluefin. (2024). *The Biggest Data Breaches of the Year (2024)*. Bluefin. https://www.bluefin.com/bluefin-news/biggest-data-breaches-year-2024/

Carvache-Franco, O., Loaiza-Torres, J., Soto-Montenegro, C., Carvache-Franco, M., & Carvache-Franco, W. (2022). The Risks Perceived by The Consumer in the Acceptance of Electronic Commerce. A Study of Bolivia. *PloS One*, *17*(11), e0276853. https://doi.org/10.1371/journal.pone.0276853

Castillo-Vergara, M., Álvarez-Marín, A., Villavicencio Pinto, E., & Valdez-Juárez, L. E. (2022). Technological Acceptance of Industry 4.0 by Students from Rural Areas. *Electronics*, *11*(14), 2109. https://doi.org/10.3390/electronics11142109

Charupat, N., Huang, H., & Milevsky, M. A. (2012). Strategic Financial Planning over The Lifecycle: A Conceptual Approach to Personal Risk Management. In *Strategic Financial Planning Over the Lifecycle: A Conceptual Approach to Personal Risk Management*. https://doi.org/10.1017/CBO9780511807336

Chatfield, K., Borsella, E., Mantovani, E., Porcari, A., & Stahl, B. C. (2017). An Investigation into Risk Perception in The ICT Industry as A Core Component of Responsible Research and Innovation. *Sustainability (Switzerland)*, *9*(8). https://doi.org/10.3390/su9081424

Chen, Y.-H., Wang, K.-J., & Liu, S.-H. (2023). How Personality Traits and Professional Skepticism Affect Auditor Quality? A Quantitative Model. *Sustainability*, *15*(2), 1547. https://doi.org/10.3390/su15021547

Cromer, C. T. (2015). Consumer E-Commerce Dissonance: Innovating without Alienating Before Information Overload. *Proceedings of the 2010 Academy of Marketing Science (AMS) Annual Conference*, *5*(4), 262–262. https://doi.org/10.1007/978-3-319-11797-3_149

Dang, V. T., Wang, J., & Vu, T. T. (2020). An Integrated Model of the Younger Generation's Online Shopping Behavior Based on Empirical Evidence Gathered from an Emerging Economy. *PLoS ONE*, *15*(5), 1–20. https://doi.org/10.1371/journal.pone.0232213

Diers-Lawson, A., Symons, A., & Zeng, C. (2021). Building Crisis Capacity with Data Breaches: The Role of Stakeholder Relationship Management and Strategic Communication. *Corporate Communications*, *26*(4), 675–699. https://doi.org/10.1108/CCIJ-02-2021-0024

Dobrowolski, Z., Drozdowski, G., & Panait, M. (2022). Understanding the Impact of Generation Z on Risk Management — A Preliminary Views on Values, Competencies, and Ethics of the Generation Z in Public Administration. *International Journal of Environmental Research and Public Health*, *19*(7). https://doi.org/10.3390/ijerph19073868

Elger, J. F. (2004). Personal Financial Planning As Personal Risk Management. *Journal of Financial Service Professionals*, *58*(1), 38–39. http://search.ebscohost.com/login.aspx?direct=true&db=bsh&AN=11775083&site=ehost-live

Esposito, B., Sessa, M. R., Sica, D., & Malandrino, O. (2022). Service Innovation in The Restaurant Sector During COVID-19: Digital Technologies to Reduce Customers' Risk Perception. In *TQM Journal* (Vol. 34, Issue 7). https://doi.org/10.1108/TQM-01-2022-0016

Fajri, C. (2022). *Memastikan Penerapan Industri 5.0 Hadir Merata di Seluruh Indonesia*. Antara News. https://www.antaranews.com/berita/3018049/memastikan-penerapan-industri-50-hadir-merata-di-seluruh-indonesia

Fataliyev, T., & Mehdiyev, S. (2020). Industry 4.0: The Oil and Gas Sector Security and Personal Data Protection. *International Journal of Engineering and Manufacturing*, *10*(2), 1–14. https://doi.org/10.5815/ijem.2020.02.01

Febrian, A., Nani, D. A., Lina, L. F., & Husna, N. (2022). The Role of Social Media Activities to Enhance Brand Equity. *Journal of Economics, Business, & Accountancy Ventura*, *25*(1), 20. https://doi.org/10.14414/jebav.v25i1.2881

Fox, G., Lynn, T., & Rosati, P. (2022). Enhancing Consumer Perceptions of Privacy and Trust: a GDPR Label Perspective. *Information Technology and People*, *35*(8), 181–204. https://doi.org/10.1108/ITP-09-2021-0706

Fox, M. A., Niemeier, R. T., Hudson, N., Siegel, M. R., & Dotson, G. S. (2021). Cumulative risks from stressor exposures and personal risk factors in the workplace: examples from a scoping review. *International Journal of Environmental Research and Public Health*, *18*(11). https://doi.org/10.3390/ijerph18115850

Ganbat, M., Batbaatar, E., Bazarragchaa, G., Ider, T., Gantumur, E., Dashkhorol, L., Altantsatsralt, K., Nemekh, M., Dashdondog, E., & Namsrai, O. E. (2021). Effect of psychological factors on credit risk: A case study of the microlending service in Mongolia. *Behavioral Sciences*, *11*(4). https://doi.org/10.3390/bs11040047

Gilliam, J., Chatterjee, S., & Grable, J. (2010). *Evolución De Los Cuestionarios De Tolerancia Al Riesgo*. *770*.

Gimpel, H., Kleindienst, D., Nüske, N., Rau, D., & Schmied, F. (2018). The Upside of Data Privacy – Delighting Customers by Implementing Data Privacy Measures. *Electronic Markets*, *28*(4), 437–452. https://doi.org/10.1007/s12525-018-0296-3

Goldbach, D., Tayauova, G., & Zhumabekovna, A. T. (2023). Motivation at Work for Generation Z. *FAIMA Business & Management Journal*, *11*(3), 68–74.

Habib, A., Irfan, M., & Shahzad, M. (2022). Modeling the Enablers of Online Consumer Engagement and Platform Preference in Online Food Delivery Platforms during COVID-19. *Future Business Journal*, *8*(1). https://doi.org/10.1186/s43093-022-00119-7

Habib, S., & Hamadneh, N. N. (2021). Impact of perceived risk on consumers technology acceptance in online grocery adoption amid COVID-19 pandemic. *Sustainability (Switzerland)*, *13*(18), 1–16. https://doi.org/10.3390/su131810221

Hair, J. F., Black, W. C., Babin, B. J., & Anderson, R. E. (2019). *Multivariate Data Analysis* (8th ed.). Cengage Learning EMEA.

Hair, J. F., Risher, J. J., Sarstedt, M., & Ringle, C. M. (2019). When to Use and How to Report The Results of PLS-SEM. *European Business Review*, *31*(1), 2–24. https://doi.org/10.1108/EBR-11-2018-0203

Hong, W., Chan, F. K. Y., & Thong, J. Y. L. (2021). Drivers and Inhibitors of Internet Privacy Concern: A Multidimensional Development Theory Perspective. *Journal of Business Ethics*, *168*(3), 539–564. https://doi.org/10.1007/s10551-019-04237-1

Hoppe, F., Gatzert, N., & Gruner, P. (2021). Cyber Risk Management in SMEs: Insights from Industry Surveys. *Journal of Risk Finance*, *22*(3–4), 240–260. https://doi.org/10.1108/JRF-02-2020-0024

Howat-Rodrigues, A. B. C., Ferreira, J. H. B. P., & Laks, J. (2019). Brazilian Portuguese Version of Financial Risk-taking and Tolerance Scales: Validity Evidence Within and Between Measures. *Trends in Psychiatry and Psychotherapy*, *41*(4), 318–326. https://doi.org/10.1590/2237-6089-2018-0066

ISACA. (2015). Cybersecurity Fundamental. In *ISACA* (pp. 1–196). Elsevier. https://doi.org/10.1016/B978-0-08-026495-0.50007-7

Islam, S., Fenz, S., Weippl, E., & Mouratidis, H. (2017). A Risk Management Framework for Cloud Migration Decision Support. *Journal of Risk and Financial Management*, *10*(4), 10. https://doi.org/10.3390/jrfm10020010

Israel, G. D. (2003). *Using Published Tables Using Formulas To Calculate A Sample Size Using A Census For Small Populations*.

Iswari, T. I., & Budiyono, E. F. C. S. (2024). Preference by Gender among Z Generation on Risky Decision: A Survey on Business and Economics Students. *Review of Integrative Business and Economics Research*, *13*(3), 272–290.

IT Governance. (2024). *Global Data Breaches and Cyber Attacks in 2024*. IT Governance. https://www.itgovernance.co.uk/blog/global-data-breaches-and-cyber-attacks-in-2024

Jang, J., & Kim, B. (2022). The Impact of Potential Risks on the Use of Exploitable Online Communities: The Case of South Korean Cyber-Security Communities. *Sustainability (Switzerland)*, *14*(8). https://doi.org/10.3390/su14084828

Junglas, I. A., Johnson, N. A., & Spitzmüller, C. (2008). Personality Traits and Concern for Privacy: An Empirical Study in The Context of Location-based Services. *European Journal of Information Systems*, *17*(4), 387–402. https://doi.org/10.1057/ejis.2008.29

Kamalul Ariffin, S., Mohan, T., & Goh, Y. N. (2018). Influence of consumers' perceived risk on consumers' online purchase intention. *Journal of Research in Interactive Marketing*, *12*(3), 309–327. https://doi.org/10.1108/JRIM-11-2017-0100

Kennedy, S. E. (2016). The Pathway to Security – Mitigating User Negligence. *Information & Computer Security*, *24*(3), 255–264. https://doi.org/10.1108/ICS-10-2014-0065

Kien Men, L., & Noordin, N. (2019). Senior Meets Junior Digital Natives: TESLians Integrating Technology in their Teaching Practice. *International Journal of Education and Literacy Studies*, *7*(4), 150. https://doi.org/10.7575/aiac.ijels.v.7n.4p.150

Kim, J. H., & Lennon, S. J. (2010). Information Available on A Website: Effects on Consumers' Shopping Outcomes. *Journal of Fashion Marketing and Management*, *14*(2), 247–262. https://doi.org/10.1108/13612021011046093

Kovaitė, K., Šūmakaris, P., & Stankevičienė, J. (2020). Digital communication channels in industry 4.0 implementation: The role of internal communication. *Management (Croatia)*, *25*(1), 171–191. https://doi.org/10.30924/mjcmi.25.1.10

Kozarevi, S., Faculty, T., Univerzitetska, E., Be, N., Telecom, B. H., Aleja, T., & Izetbegovi, A. (2015). *Risk Management in Telecommunications Services*.

Kuzniak, S., Rabbani, A., Heo, W., Ruiz-Menjivar, J., & Grable, J. (2015). The Grable and Lytton Risk-Tolerance Scale. *Financial Services Review*, *24*(2), 177–192. https://doi.org/10.61190/fsr.v24i2.3240

Lee, Y. K. (2021). Impacts of Digital Technostress and Digital Technology Self-efficacy on Fintech Usage Intention of Chinese Gen Z Consumers. *Sustainability (Switzerland)*, *13*(9). https://doi.org/10.3390/su13095077

Li, N., & van Rooij, B. (2022). Law Lost, Compliance Found: A Frontline Understanding of the Non-linear Nature of Business and Employee Responses to Law. *Journal of Business Ethics*, *178*(3), 715–734.

https://doi.org/10.1007/s10551-021-04751-1
Liao, Y. K., Wu, W. Y., Le, T. Q., & Phung, T. T. T. (2022). The Integration of the Technology Acceptance Model and Value-Based Adoption Model to Study the Adoption of E-Learning: The Moderating Role of e-WOM. *Sustainability (Switzerland)*, *14*(2). https://doi.org/10.3390/su14020815
Lissitsa, S., & Kol, O. (2021). Four Generational Cohorts and Hedonic M-shopping: Association between Personality Traits and Purchase Intention. *Electronic Commerce Research*, *21*(2), 545–570. https://doi.org/10.1007/s10660-019-09381-4
Liu, Y., Li, Q., Edu, T., Negricea, C., Fam, K. S., & Zaharia, R. (2022). Modelling E-commerce Customer Reactions. Exploring Online Shopping Carnivals in China. *Economic Research-Ekonomska Istrazivanja*, *35*(1), 3060–3082. https://doi.org/10.1080/1331677X.2021.1985576
Mahlous, A. R. (2023). Threat Model and Risk Management for a Smart Home IoT System. *Informatica (Slovenia)*, *47*(1), 51–64. https://doi.org/10.31449/INF.V47I1.4526
Maity, M., Bagchi, K., Shah, A., & Misra, A. (2019). Explaining Normative Behavior in Information Technology Use. *Information Technology and People*, *32*(1), 94–117. https://doi.org/10.1108/ITP-11-2017-0384
Maswadi, K., Ghani, N. A., & Hamid, S. (2022). Factors Influencing The Elderly's Behavioural Intention to Use Smart Home Technologies in Saudi Arabia. In *PLoS ONE* (Vol. 17, Issue 8 August). https://doi.org/10.1371/journal.pone.0272525
Mohd Thas Thaker, H., Khaliq, A., Ah Mand, A., Iqbal Hussain, H., Mohd Thas Thaker, M. A. Bin, & Allah Pitchay, A. Bin. (2021). Exploring The Drivers of Social Media Marketing in Malaysian Islamic banks. *Journal of Islamic Marketing*, *12*(1), 145–165. https://doi.org/10.1108/JIMA-05-2019-0095
Moon, J., Choe, Y., & Song, H. (2021). Determinants of Consumers' Online/Offline Shopping Behaviours During The COVID-19 Pandemic. *International Journal of Environmental Research and Public Health*, *18*(4), 1–17. https://doi.org/10.3390/ijerph18041593
Moslehpour, M., Pham, V. K., Wong, W. K., & Bilgiçli, I. (2018). E-Purchase Intention of Taiwanese Consumers: Sustainable Mediation of Perceived Usefulness and Perceived Ease of Use. *Sustainability (Switzerland)*, *10*(1). https://doi.org/10.3390/su10010234
Mu, H., Meng, S., Wang, M., & Zhang, S. (2023). Research on A Mining Area Risk Management System Based on Internal Control Theory. *Gospodarka Surowcami Mineralnymi / Mineral Resources Management*, *39*(4), 49–66. https://doi.org/10.24425/gsm.2023.148161
Mubarok, M. M. (2022). The Mapping of Electronic Commerce Issues and Consumer Protection Policy in Indonesia. *Journal of Economics, Business, & Accountancy Ventura*, *24*(3), 431. https://doi.org/10.14414/jebav.v24i2.2690
Navickas, M., Gudaitis, T., & Krajnakova, E. (2014). Influence of Financial Literacy on Management of Personal Finances in A Young Household. *Business: Theory and Practice*, *15*(1), 32–40. https://doi.org/10.3846/btp.2014.04
Nguyen, D. T., Tran, V. D., & Ghafoor, A. (2022). The Impact of Covid-19 Lockdown on Intention to Follow Preventive Measures in Vietnam: Integrated Protection Motivation Theory and Theory Planned Behavior. *Cogent Business & Management*, *9*(1), 1–20. https://doi.org/10.1080/23311975.2022.2054502
Nicolas-Rocca, T. S., & Burkhard, R. J. (2019a). Information security in libraries: Examining the effects of knowledge transfer. *Information Technology and Libraries*, *38*(2), 58–71. https://doi.org/10.6017/ital.v38i2.10973
Nicolas-Rocca, T. S., & Burkhard, R. J. (2019b). Information Security in Libraries: Examining the Effects of Knowledge Transfer. *Information Technology and Libraries*, *38*(2), 58–71. https://doi.org/10.6017/ital.v38i2.10973
Nikiforova, A., Alor, M. A., & Lytras, M. D. (2022). The Role of Open Data in Transforming The Society to Society 5.0: A Resource or A Tool for SDG-compliant Smart Living? *Computers and Society*, *0*.
Nobre, L. H. N., Grable, J. E., Da Silva, W. V., & Da Veiga, C. P. (2016). A Cross Cultural Test of Financial Risk Tolerance Attitudes: Brazilian and American Similarities and Differences. *International Journal of Economics and Financial Issues*, *6*(1), 314–322.
Nurhadi, M., Suryani, T., & Fauzi, A. A. (2022). The Power of Website and Social Media for Strengthening Brand Image, E-WoM, and Purchase Decision. *Journal of Economic, Business, & Accounting*, *25*(3), 320–331. https://doi.org/10.14414/jebav.v25i3.3093.ABSTRACT
Oribhabor, C. B., & Anyanwu, C. A. (2019). Research Sampling and Sample Size Determination: A practical Application. *Federal University Dutsin-Ma Journal of Educational Research (Fudjer)*, *2*(1), 47–56.
P Panca, W. A., Jamin Ariana, I. N., & Arismayanti, N. K. (2017). Pengaruh Kualitas Pelayanan Terhadap Loyalitas Wisatawan dan Citra Hotel Melati di Kelurahan Seminyak Kabupaten Badung Bali. *Jurnal Kepariwisataan Dan Hospitalitas*, *1*(1), 65–72.
Pedersen, C., & Nagengast, J. (2008). The Virtues of The Virtual Organization. *Strategic HR Review*, *7*(3), 19–25. https://doi.org/10.1108/14754390810865775
Pruss, E. (2006). Managing Personal Risk in an Era of Rising Wealth and Proliferating Threats. *The Journal of Wealth Management*, *9*(3), 7–23. https://doi.org/10.3905/jwm.2006.661428
Rejda, G. E., McNamara, M. J., & Rabel, W. H. (2022). *Principles of Risk Management and Insurance* (14th ed.). Pearson Education Limited.
Rosique-Blasco, M., Madrid-Guijarro, A., & García-Pérez-de-Lema, D. (2018). The effects of personal abilities and self-efficacy on entrepreneurial intentions. *International Entrepreneurship and Management Journal*, *14*(4), 1025–1052.

https://doi.org/10.1007/s11365-017-0469-0
Salahdine, F., & Kaabouch, N. (2019). Social Engineering Attacks: A Survey. *Future Internet*, *11*(4). https://doi.org/10.3390/FI11040089
Saluza, I., & Sartika, D. (2019). Pengembangan Model Keberlanjutan e-filing di Palembang Menggunakan Partial Least Square Structural Equation Models (PLS-SEM). *Jurnal Sistem Informasi Bisnis*, *9*(1), 94. https://doi.org/10.21456/vol9iss1pp94-102
Setiawan, A., Djajadikerta, H., Haryanto, H., & Wirawan, S. (2021). Theory of Reasoned Action dan Literasi Teknologi terhadap Adaptasi Perubahan Teknologi. *Jurnal Sistem Informasi Bisnis*, *11*(1), 51–61. https://doi.org/10.21456/vol11iss1pp51-61
Setiawan, A., & Haryanto, H. (2024). *Exploring the Perspective of Generation Z on Personal Risk Management*. *4*(02), 60–73.
Setiawan, H., & Iramani, R. (2023). Financial Well-Being Model for Bank Employees: the Role of Financial Behavior as a Mediator. *Journal of Economics, Business, & Accountancy Ventura*, *26*(2), 205–219. https://doi.org/10.14414/jebav.v26i2.3948
Sheedy, E., & Lubojanski, M. (2018). Risk management behaviour in banking. *Managerial Finance*, *44*(7), 902–918. https://doi.org/10.1108/MF-11-2017-0465
Shiau, W. L., Sarstedt, M., & Hair, J. F. (2019). Internet Research Using Partial Least Squares Structural Equation Modeling (PLS-SEM). *Internet Research*, *29*(3), 398–406. https://doi.org/10.1108/IntR-10-2018-0447
Shin, I., & Park, S. (2017). Integration of Enterprise Risk Management and Management Control System: Based on A Case Study. *Investment Management and Financial Innovations*, *14*(1), 19–26. https://doi.org/10.21511/imfi.14(1).2017.02
Silva, J., Pinho, J. C., Soares, A., & Sá, E. (2019). Antecedents of Online Purchase Intention And Behaviour: Uncovering Unobserved Heterogeneity. *Journal of Business Economics and Management*, *20*(1), 131–148. https://doi.org/10.3846/jbem.2019.7060
Singh, Y., Adil, M., & Haque, S. M. I. (2023). Personality Traits and Behaviour Biases: The Moderating Role of Risk-Tolerance. *Quality and Quantity*, *57*(4), 3549–3573. https://doi.org/10.1007/s11135-022-01516-4
Solimun. (2020). Warppls Analysis Application for Effects of Personality and Commitment on The Engagement of Ngrebeg Mekotek Traditional Actors in Munggu Village, Bali. *International Journal of Advanced Science and Technology*, *29*(4), 2025–2044.
Sommestad, T., Karlzén, H., & Hallberg, J. (2019). The Theory of Planned Behavior and Information Security Policy Compliance. *Journal of Computer Information Systems*, *59*(4), 344–353. https://doi.org/10.1080/08874417.2017.1368421
Stewart, H., & Jürjens, J. (2017). Information Security Management and The Human Aspect in Organizations. *Information and Computer Security*, *25*(5), 494–534. https://doi.org/10.1108/ICS-07-2016-0054
Studley, M. (2021). *Assessing D & O Risk When a Company Goes Public*. *September*, 18–20.
Sudaryono, S., Sunarya, P. A., & Dayanti, M. T. (2024). Model Pengukuran Soft Competencies Era Industri 4.0 Pendekatan PLS-SEM (Partial Least Squares Structural Equation Modeling). *ICIT Journal*, *10*(1), 113–127. https://doi.org/10.33050/icit.v10i1.3058
Sujarwo, M., & Indriani, F. (2022). Shopping Value Resonance of Household Appliance and Purchase Intentions in E-Commerce. *Journal of Economics, Business, & Accountancy Ventura*, *24*(3), 339. https://doi.org/10.14414/jebav.v24i3.2894
Sutarso, Y. (2021). Essential Drivers of Payment Gateway Continuance Intention: The Moderating Role of Usage Rate. *Journal of Economics, Business, & Accountancy Ventura*, *24*(2), 271. https://doi.org/10.14414/jebav.v24i2.2631
Syarif, A., Parno, P., Komariah, K., & Yuliani, I. (2023). Customer Loyalty in Islamic Bank during the COVID-19 Outbreak: The Mediating Role of Trust and Satisfaction. *Journal of Economics, Business, & Accountancy Ventura*, *26*(2), 236–248. https://doi.org/10.14414/jebav.v26i2.3145
Tang, J., Zhang, B., & Akram, U. (2021). What Drives Authorization in Mobile Applications? A Perspective of Privacy Boundary Management. *Information (Switzerland)*, *12*(8), 1–21. https://doi.org/10.3390/info12080311
Tri Marhendra Rahardyan, Bakri, M. R., & Anastasya Utami. (2023). Generation gap in fraud prevention: Study on generation Z, generation X, millennials, and boomers. *International Journal of Research in Business and Social Science (2147- 4478)*, *12*(3), 361–375. https://doi.org/10.20525/ijrbs.v12i3.2566
Twumasi Baffour, P., Mohammed, I., & Abdul Rahaman, W. (2019). Personality and gender differences in revealed risk preference: evidence from Ghana. *International Journal of Social Economics*, *46*(5), 631–647. https://doi.org/10.1108/IJSE-07-2018-0346
Viola, B., Aryanto, J., Marsetio, N. C., & Yuliati, R. (2023). *The Impacts of Board Characteristics and Size on Risk Disclosure : Evidence from Indonesian Mining Firms*. *25*(3), 255–272. https://doi.org/10.14414/jebav.v25i3.3435.ABSTRACT
Wang, E. S.-T. (2019). Role of Privacy Legislations and Online Business Brand Image in Consumer Perceptions of Online Privacy Risk. *Journal of Theoretical and Applied Electronic Commerce Research*, *14*(2), 0–0. https://doi.org/10.4067/s0718-18762019000200106
Wardhani, N. W. S., Nugroho, W. H., Fernandes, A. A. R., & Solimun, S. (2020). Structural Equation Modeling (SEM) Analysis with Warppls Approach Based on Theory of Planned Behavior (TPB). *Mathematics and Statistics*, *8*(3), 311–322. https://doi.org/10.13189/ms.2020.080310

Weedige, S. S., Ouyang, H., Gao, Y., & Liu, Y. (2019). Decision Making in Personal Insurance: Impact of insurance Literacy. *Sustainability (Switzerland)*, *11*(23), 1–25. https://doi.org/10.3390/su11236795

Windiarti, S., Djajadikerta, H., & Setiawan, A. (2020). *The Effect of Information Privacy Concern , Privacy Policy on Online Purchase Intention on Students in Bandung*. *57*, 5140–5145.

Yang, M. (2022). Information Security Risk Management Model for Big Data. *Advances in Multimedia*, *2022*. https://doi.org/10.1155/2022/3383251

Youn, S. (2009). Determinants of Online Privacy Concern and Its Influence on Privacy Protection Behaviors among Young Adolescents. *Journal of Consumer Affairs*, *43*(3), 389–418. https://doi.org/10.1111/j.1745-6606.2009.01146.x

Zang, W., Qian, Y., & Song, H. (2022). The Effect of Perceived Value on Consumers' Repurchase Intention of Commercial Ice Stadium: The Mediating Role of Community Interactions. *International Journal of Environmental Research and Public Health*, *19*(5). https://doi.org/10.3390/ijerph19053043

Zlatolas, L. N., Welzer, T., Hölbl, M., Heričko, M., & Kamišalić, A. (2019). A Model of Perception of Privacy, Trust, and Self- disclosure on Online Social Networks. *Entropy*, *21*(8). https://doi.org/10.3390/e21080772

Zoran, T. (2018). Fintech Firm Opportunity or Threat for Banks? *International Journal of Information, Business and Management*, *10*(1), 137–143.

Appendix 1. Research instrument

Variable	Domain	Indicator Statement	Code
Intention to purchase	Preference for online shopping	I prefer shopping online rather than shopping in physical stores.	INT1
		I will continue to shop online.	INT2
	Online shopping habits	I plan to shop online regularly in the future.	INT3
Concern for privacy	Privacy of mobile provider	It is a problem for me if my cellular provider stores my location data.	CFP1
	Phone location data	I am uncomfortable if my cellular provider can track my location anytime.	CFP2
		I expect my location data to be accurate.	CFP3
	Awareness of personal data security	My cellular provider should not share my location data with unauthorized parties.	CFP4
		My cellular provider should not share my location data without my permission.	CFP5
Self-efficacy	Internet self-efficacy	I understand terms related to the internet.	SE1
		I am able to explain the functions of internet devices.	SE2
		I am able to troubleshoot issues with my internet.	SE3
		I am able to use the internet to search for the data I need.	SE4
Threats	Perceived threat probability	In my opinion, the likelihood of someone's personal data being stolen while online is:	PTP1
		In my opinion, the likelihood of personal email being intercepted while online is:	PTP2
		In my opinion, the likelihood of privacy invasion of someone's data is:	PTP3
	Perceived threat severity	I am worried that my personal data might be stolen when I am online.	PTS1
		I am worried that my personal email might be intercepted when I am online.	PTS2
Risk	Personal risk management	I ask more knowledgeable people about how to protect personal data.	PRM1
		I read the privacy statements provided on the websites.	PRM2
		I look for guides or tutorials on personal data protection on the internet.	PRM3