Journal of Information Systems Engineering and Management
2025, 10(54s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Analysis of Cyber Security Readiness and Technology Readiness in Digital Transformation in Cooperatives in Bandung City

Mizan Nadhifah[1], Ratna Komala Putri[2], Puspita Kencana Sari[3]
[1]*Faculty of Economics and Business, Telkom University, Indonesia*
[2]*Faculty of Economics and Business, Telkom University, Indonesia*
[3]*Faculty of Economics and Business, Telkom University, Indonesia*

ARTICLE INFO

Received: 31 Dec 2024

Revised: 20 Feb 2025

Accepted: 28 Feb 2025

ABSTRACT

Digital transformation is an important need for the cooperative sector to remain competitive in the digital era. This study evaluates the readiness of technology and cybersecurity in supporting digital transformation in cooperatives in Bandung. Using a quantitative approach and SEM-PLS method, data were collected through valid online questionnaires from 263 cooperative management respondents. This study proposes 4 hypotheses, which test the relationship between technology readiness and cybersecurity readiness on the success of digital transformation, as well as its impact on tangible and intangible benefits for cooperatives. The results show that technology readiness and cybersecurity have a positive and significant effect on the success of digital transformation. This transformation provides tangible benefits, such as operational efficiency, and intangible benefits, such as increased reputation and member trust. This study contributes to the literature on cooperative readiness in facing digital transformation and provides recommendations for strengthening.

Keywords: Cybersecurity Readiness; Technology Readiness; Digital Transformasi; Tangible Benefit; Intangible Benefit.

INTRODUCTION

Digital transformation is growing rapidly in Indonesia and is a priority for many organizations in various sectors, including Cooperatives. Driven by the need for organizations to meet market expectations and face increasingly tight competition. However, behind the many opportunities offered in today's digital transformation, cybersecurity threats continue to increase, from malware to data theft that can disrupt business and reduce the organization's reputation (Berlilana et al., 2021). The National Cyber Security Operations Center reports that millions of cyber-attacks occur every year. This highlights the importance of cybersecurity readiness for organizations, as it is crucial in ensuring the sustainability of the organization in the digital era. By assessing both cybersecurity readiness and technological readinessespecially in terms of infrastructure and other technologies organizations can identify vulnerabilities in their security systems and take preventive measures before threats arise. Comprehensive cybersecurity preparation can help prevent financial losses, protect sensitive data, and safeguard the organization's reputation.In today's digital landscape, digital transformation is no longer optional; it has become a necessity. This transformation enables organizations to remain competitive in the market, as advancements in information technology have shifted organizational operations from manual processes to digital ones, thereby increasing efficiency and effectiveness in their operations (Pangandaheng et al., 2022). For cooperatives, cybersecurity readiness becomes even more vital within the digital transformation process. Cooperatives must ensure that their data is secure and that they maintain the trust of their members through a robust security infrastructure.

Journal of Information Systems Engineering and Management
2025, 10(54s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Cooperatives, as member-owned and member-managed organizations, have the fundamental goal of meeting their members' economic and social needs. The core characteristics of cooperatives include voluntary and open membership, where each member has equal voting rights in decision-making. Additionally, cooperatives emphasize shared ownership and management, where profits are distributed based on the amount of participation (services or transactions) made by the members, rather than capital investment. This structure fosters a strong sense of community and mutual support, making cooperatives an essential component in the development of local economies. In the context of urban areas like Bandung, cooperatives are seen as vital contributors to community welfare and economic stability (Santos et al., 2024). However, with the ongoing digital transformation, cooperatives face significant challenges. Despite the many opportunities digitalization offers such as increased operational efficiency, better customer service, and broader market reach cooperatives often struggle with adapting to new technologies. These challenges include limited resources, insufficient technological infrastructure, and a lack of cybersecurity preparedness. Many cooperatives are still reliant on traditional, manual systems, which not only hinder operational efficiency but also expose them to risks associated with data breaches and cyber-attacks. Moreover, there is often resistance to change, as many cooperative managers and members are not fully aware of the potential benefits of digital transformation, or they fear the complexity of technology adoption (Vinh et al., 2023). This makes the urgency of this research clear: cooperatives must develop a comprehensive understanding of both their technological readiness and cybersecurity preparedness to thrive in the digital age. The study focuses on cooperatives in Bandung, a city known for its active engagement in digitalization and technological adoption. Despite this, many cooperatives in Bandung still face challenges in securing their digital infrastructure and adapting to new technological demands. Therefore, understanding the state of cybersecurity and technological readiness in Bandung's cooperatives is essential for fostering a successful transition to the digital eraSeveral cooperatives in the Bandung area are actively engaging in digital transformation, faced with the challenge of ensuring their technological readiness and cybersecurity readiness to protect cooperative information assets including data protection, operational efficiency, and the trust of cooperative members. Therefore, measuring cybersecurity readiness and technological readiness is crucial for cooperatives to prepare for cyber attacks that can have a major and significant impact on cooperative operations such as financial losses, loss of sensitive data, and degradation of the image of cooperative member trust. Previous research shows that organizations that are not prepared for cyber attacks will experience significant losses, including the loss of sensitive data and a decrease in the reputation of the organization (Berlilana et al., 2021). This is very relevant to remember that the success of digitalization is not only determined by the adoption of technology, but also the readiness of the security infrastructure to face increasingly complex cyber threats. (Berlilana et al., 2021; Pangandaheng et al., 2022). Previous studies have examined various aspects of technology and cybersecurity readiness in various organizations in the corporate sector, highlighting the importance of cybersecurity readiness in protecting organizational assets, which directly impact organizational performance, including tangible benefits such as operational efficiency and intangible benefits such as better reputation (Berlilana et al., 2021). In the previous study, it was highlighted that digital transformation requires a strategy that is in accordance with organizational capacity, involves top management involvement, and organizational cultural support to achieve success (Pangandaheng et al., 2022). However, these studies focus on large corporate organizations or business and government sectors, while studies on technology readiness and cybersecurity in cooperatives are still limited. Therefore, the current study to filling this gap by evaluating and analyzing cybersecurity readiness and information technology readiness in implementing digital transformation in cooperatives.

This research provides academic and practical contributions. On the academic side, this research enriches the existing literature on cybersecurity readiness and technological readiness in cooperatives in Bandung which are still in the process of digitalization, especially in the cooperative sector which often faces resource limitations. This research uses a holistic approach that includes technological, organizational and external environmental factors (Berlilana et al., 2021). Then, from a practical perspective, this study provides strategic guidance for cooperatives in evaluating their readiness to adapt to digital transformation safely and effectivelyThis study uses a case study approach with quantitative methods. Data were collected through a survey distributed to cooperative managers in Bandung. Data analysis was carried out using the SEM-PLS method to evaluate the relationship between technological readiness and cybersecurity readiness in the existing Digital Transformation. The practical implications of these findings are that cooperatives aiming for successful digital transformation must ensure their technological infrastructure is fully

Research Article

prepared, enhance the competencies of their human resources in both technology and cybersecurity, and foster an organizational culture that embraces change. This study will also provide strategic recommendations for cooperatives to strengthen stakeholder involvement in the digital transformation process, reinforce security policies, and offer training programs for employees to mitigate any discomfort or insecurity that may arise during the digitalization process.

LITERATURE REVIEW

2.1 Digital Transformation

Digital transformation is the basic process of entering digital technology into all aspects of a business that results in fundamental changes in the way organizations operate and provide value to users in the context of cooperatives, this digital transformation itself makes profound changes to the way cooperatives operate. The Digital Readiness Framework (World Economic Forum, 2021) also focuses heavily on the importance of technological infrastructure readiness, such as networks, hardware, and software as the main supporters of digital transformation. Vial (Vial, 2019) Strengthening Digital transformation is a process that aims to increase operational efficiency driven by technology such as Cloud Computing, Big Data Analytics, and IoT. In the context of digital transformation in cooperatives, this transformation includes the use of a combination of information technology, computers, communications and connectivity properties. This emphasizes that digital transformation is not only about adopting technology and techniques, but also about how cooperatives can take advantage of fundamental changes in the business model and culture of cooperatives by utilizing technology to create tangible benefits (Tangible Benefits) such as increasing the operational efficiency of cooperatives and intangible benefits (Intangible Benefits) such as increasing the reputation of cooperatives. The main characteristics of digital transformation are very many and of course diverse which makes digital transformation different from just digitizing or automating processes. (Subekti et al., 2024) explains in the Dynamic Capabilities Theory, that organizations that are able to adapt to environmental and technological changes will be more successful in digital transformation. Strengthened by (Subekti et al., 2024), Digital Transformation is the integration of digital technologies into all aspects of an organization's operations, which changes the way the organization operates and delivers value to customers. In addition, (Subekti et al., 2024) highlights organizational culture as an important factor in supporting the success of digital transformation, and organizations that successfully carry out digital transformation will experience an increase in operational efficiency of 40% and an increase in customer satisfaction of 35%. This shows that digital transformation is no longer an option, but a necessity to survive in a competitive market environment and how Cooperatives can prepare human resources and infrastructure to support digital transformation and effective and efficient management changes to reduce resistance from within the cooperative to innovation.

However, in this process, cooperatives certainly face various challenges in the digital transformation process. (Vial, 2019) identified that the main challenges include resistance to change, limited resources, and lack of digital skills. Especially for small organizations such as cooperatives, these challenges are increasingly complex due to limited resources and technical capabilities, therefore, to achieve the success of the cooperative's digital transformation, it is highly dependent on internal readiness to face these challenges, including cybersecurity readiness in cooperatives that can ensure that this new information system is protected from existing threats and technological readiness in cooperatives that are undergoing digital transformation to prove the level that cooperatives are ready to utilize new technologies. Cooperatives also need to adopt a holistic approach such as change management, resource training and building a culture of innovation. In this way, Digital Transformation can be successfully implemented properly and efficiently so that cooperatives will be more efficient in operations and more focused on tangible benefits and intangible benefits.

2.2 Cybersecurity Readiness: Theory and Concepts

In today's digital era, Cybersecurity has become an urgent need for cooperatives that are increasingly dependent on information technology, and protecting information systems means increasing threats to data security and digital infrastructure. Therefore, it is important for cooperatives to have cybersecurity readiness. Cybersecurity has an important role in ensuring operational stability and protecting information systems.(Neri et al., 2024) argues that cyber security covers the most basic fundamental technical and non-technical aspects, namely the CIA Triad:

Journal of Information Systems Engineering and Management
2025, 10(54s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Confidentiality, Integrity (Intelligent), Information Availability (Available) as important elements that are the main foundation in protecting the organization's digital assets from risks that disrupt the sustainability of the organization's operations. Confidentiality, according to (Neri et al., 2024) aims to protect information so that it cannot be accessed by any unauthorized or unauthorised party, with the implementation of encryption and multifactor authentication as the main steps. Integrity (Intellegent), explained by (Vinh et al., 2023) that this integrity is very important for organizations to ensure data is accurate and not changed arbitrarily without permission through unauthorized techniques such as hashing and data validation. And finally, Availability, explained by (Eliza et al., 2024) ensuring data and system accessibility whenever needed, with redundancy planning and disaster recovery as key supporting elements. In the study (Nepal et al., 2022) also explains the importance of understanding dynamic human behavior in the context of security and privacy. This shows that the cybersecurity approach must include a comprehensive strategy, starting from cooperative aspects and user behavior in data protection to ensuring the sustainability of access and integrity of information. Strengthened by (Vinh et al., 2023) which states that cyber security protection requires human readiness to face increasingly complex threats, not just at the technological level. Therefore, an approach that combines education, user awareness and advanced technology can create a solid layer of defense.

Cybersecurity threats and risks can disrupt organizational operations, there are various cybersecurity threats, namely: Phishing, Malware, DDoS (Distributed Denial of Service) and many other cybersecurity threats. What often happens is phishing, where attackers use spam emails, telephone calls, or text messages to manipulate psychology to steal sensitive information such as login credentials. In research (Neri et al., 2024)noted that phishing was successful due to a lack of user awareness. In addition to phishing, there are also other significant threats that can damage systems and steal data, namely malware, including ransomware, noted by (Vinh et al., 2023) IoT devices are increasingly vulnerable to malware attacks due to their high connectivity. DDoS is a threat attack designed to flood a system with fake traffic and cause other disruptions. (Vinh et al., 2023) strongly emphasizes the importance of conducting real-time monitoring to detect and prevent these attacks effectively. So from all the explanations of the strengthening theory above, it is very important for cooperatives that have not, are new or have carried out digital transformation to have awareness and readiness for cybersecurity in information systems.

2.3 Technology Readiness in Digital Transformation

Technology Readiness is a very important factor to support digital transformation. Found and developed by (Parasuraman, 2000) through the Technology Readiness Index (TRI) model by grouping the readiness of a person or organization in 4 main dimensions that reflect various attitudes and reactions that influence how technology is adopted and used, the following 4 main dimensions are: optimism, innovation, discomfort, and insecurity. This theory is the basis for measuring the readiness of cooperatives to accept new technology for digital transformation in their operations. (Chang & Chen, 2021) explains technological readiness is a concept used to measure the readiness of individuals and organizations in various sectors that adopt and carry out digital transformation including cooperatives in Bandung that are undergoing digital transformation. In the context of cooperatives in this study, these 4 dimensions have a very relevant role in analyzing the readiness of cooperatives to carry out digital transformation, optimism and innovation are dimensions that support technological readiness, while discomfort and insecurity are dimensions that can hinder technological readiness. According to(Lin & Hsieh, 2007) Organizations with higher technological optimism will adopt new technologies more quickly and experience benefits from increased operational satisfaction. Therefore, Optimism in the context of cooperatives reflects the belief that technology can provide significant benefits such as higher efficiency, better security, and increased trust of cooperative members. For example, the implementation of good information technology can help cooperatives improve the efficiency of member management, transactions, financial reports and other operations. In relation to the openness of cooperatives to change and the ability to implement new technologies, innovation is very important for cooperatives, especially for cooperatives that often face limitations in human and financial resources, these limitations require innovative solutions. In line with (Nalmpanti et al., 2024) explains that limitations in knowledge and finance can weaken an organization's ability to be open to innovation. However, in addition to the 2 dimensions that support technological readiness, discomfort and insecurity are major obstacles to technological readiness that have a major impact on slowing down the digital transformation process in cooperatives. Discomfort arises when cooperative

Journal of Information Systems Engineering and Management
2025, 10(54s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

managers feel that digital transformation is too complicated or inefficient to use.(J. Zhao et al., 2025) inconvenience and insecurity are the main inhibiting factors in technology readiness based on the Technology Readiness Index (TRI 2.0) framework which shows that negative perceptions of the use and concerns about technology risks significantly reduce the intention of individuals or organizations to carry out digital transformation. Therefore, in this situation, it is important to hold adequate training from cooperatives so that technology is used effectively by cooperative managers and does not hinder managers from being hampered by inconvenience in digital transformation. While insecurity is related to concerns about the sensitivity of data security and privacy risks.(Aljaradat et al., 2024)insecurity associated with increased cybercrime has caused users to hesitate and even withdraw from using digital technology, even though the technology offers efficiency. This phenomenon reinforces that it is true that without a solid cybersecurity system and user trust, digital transformation in cooperatives with limited resources will run slower and full of obstacles. Therefore, in this study, technological readiness will be evaluated with the aim of understanding how ready cooperatives in Bandung are to adopt new technologies and safe and effective digital transformation for cooperative operations. These 4 dimensions will be the basis for evaluating whether cooperatives in Bandung have sufficient optimism and innovation to overcome the discomfort and insecurity in technological readiness and cybersecurity readiness in facing digital transformation. And also this study is expected to provide practical guidance for cooperatives in improving their technological readiness and cybersecurity, in order to be able to manage digital transformation well and minimize cybersecurity risks

In the context of cooperatives, digital transformation has become a critical process to remain competitive and enhance operational efficiency. However, successful digital transformation requires not only the adoption of technology but also the readiness of cybersecurity measures. Research shows that cybersecurity readiness plays a significant role in ensuring the protection of sensitive data, preventing cyberattacks, and maintaining the trust of cooperative members (Berlilana et al., 2021; Pangandaheng et al., 2022). This is particularly important for cooperatives as they integrate digital technologies, which require robust security infrastructures to safeguard information assets. The relationship between cybersecurity readiness and digital transformation is rooted in the understanding that digital technologies, such as Cloud Computing and IoT, can provide substantial operational efficiency but simultaneously expose organizations to potential cybersecurity risks (Vial, 2019). Cybersecurity readiness enables organizations to prevent, detect, and respond to cyber threats, which is crucial in the digital transformation journey, especially for cooperatives with limited resources and high dependence on digital services (Neri et al., 2024). In addition, well-prepared cooperatives in terms of cybersecurity can better utilize new technologies by mitigating risks and ensuring a secure and seamless digital transition (Pangandaheng et al., 2022). Therefore, cybersecurity readiness is expected to have a direct and significant influence on the successful implementation of digital transformation in cooperatives, as it ensures the security of digital systems, the integrity of data, and the protection of cooperative members' trust. This underlines the importance of assessing both technology readiness and cybersecurity readiness as key factors for digital transformation in cooperatives. Tangible Benefits from digital transformation in cooperatives involve direct improvements in operational efficiency and cost savings. Digitalization allows cooperatives to operate more efficiently in daily activities, accelerate processes, and reduce operational costs that were previously high. Furthermore, digital transformation helps cooperatives expand their services to members and enhance transparency in management and service delivery (Minzar & Mishra, 2024). These benefits will be optimized when cooperatives have strong technology readiness and cybersecurity preparedness. On the other hand, Intangible Benefits gained by cooperatives from digital transformation include enhanced trust and reputation in the eyes of their members. Digitalization can improve the member experience through more interactive and transparent platforms, which can boost member loyalty. Members feel more connected and valued through the use of technology that facilitates communication and the management of cooperative services in a more open manner. This, in turn, contributes to strengthening the cooperative's image and enhancing members' perception of the cooperative as a modern and trustworthy organization (Al Maazmi et al., 2024; Buglea et al., 2025).Based on this, it is necessary to formulate a hypothesis where the research hypothesis is based on various factors that influence the readiness of cooperatives in Bandung in carrying out digital transformation, where in this study will evaluate the factors of cooperative readiness in carrying out digital transformation, namely cybersecurity readiness and technological readiness in cooperatives in Bandung. Therefore, the hypothesis proposed is a hypothesis that focuses on the main variables, as follows:

Journal of Information Systems Engineering and Management
2025, 10(54s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

1. **Hypothesis (H1).**The better the cooperative's cybersecurity readiness, the more ready the cooperative will be to carry out digital transformation.
2. **Hypothesis (H2).**The higher the technological readiness of cooperatives to adopt new technologies, the more ready the cooperatives are to carry out digital transformation.
3. **Hypothesis (H3).**The better the Digital Transformation in cooperatives, the greater the real benefits that cooperatives will obtain.
4. **Hypothesis (H4).**The better the Digital Transformation in cooperatives, the more it will increase the intangible benefits for cooperatives.

This research is expected to contribute to filling the existing literature gap regarding the readiness of cooperatives in facing digital transformation, especially in terms of technological readiness and cybersecurity. In addition, this study also provides practical recommendations for cooperatives in strengthening technological infrastructure and cybersecurity policies to mitigate existing digital threats.

METHODS

This chapter will explain the process carried out during the research, starting from data collection to processing the data obtained. This study was conducted to analyze how cybersecurity readiness and technological readiness affect digital transformation in cooperatives in Bandung, as well as to understand the relationship between cybersecurity readiness, technological readiness, digital transformation, and the tangible and intangible benefits produced, this study applies a quantitative approach through empirical hypothesis testing. Data collection was carried out using a questionnaire survey method containing questions designed to measure the variables to be evaluated and items compiled based on a review of previous research literature and measured on a Likert scale of 1-7 (Strongly Disagree-Strongly Agree) to assess the level of respondent agreement and allow for more detailed measurement of the indicators of the questions given. The target respondents were cooperative administrators in Bandung, both directly and online. The criteria for selecting target respondents were carried out to ensure views on digital transformation in cooperatives and also to ensure the validity of the data to be obtained, considering the uneven distribution of special personnel in the field of cybersecurity and cooperatives in Bandung which have not yet carried out digital transformation. The data collection process took place during the period January-April 2025. In the distribution of this research questionnaire, 287 respondents were collected, but in this study 263 valid respondents were used. Some data were considered invalid because the data was incomplete or there were duplicate answers. The number of target samples was based on methodological considerations that were relevant to the analysis approach used, namely Structural Equation Modeling-Partial Least Squares (SEM_PLS).(Gefen et al., 2011)For Structural Equation Modeling in management system research, the minimum appropriate sample size is 200 participants. According to(Jhantasana, 2023)The use of rules of thumb such as the “ten-times rule” often results in sample sizes that are too small and inadequate for SEM-PLS analysis. An adequate sample size, at least 200 respondents or more, is needed to ensure adequate statistical power and avoid bias in the estimation of the structural model. Thus, the number of respondents used in this study is statistically adequate. Of the 263 respondents, 143 were male and 120 were female, and the respondents came from various age groups, education levels, positions, and work experiences.

3.1 Research Model

Next, we will describe the research model used in this study. Figure 1 below illustrates the overall research model, providing a visual representation of the relationships between the key variables in the study. This model serves as a framework for understanding how different factors—such as technological readiness, cybersecurity readiness, and digital transformation success—interact and influence one another in the context of cooperatives. Table 1 outlines the components of the research model, providing detailed descriptions of each variable and its corresponding construct. This table helps clarify how each element in the model contributes to the study’s objectives and offers a structured view of the conceptual framework guiding the research. To support the measurement of variables in the study, Table 2 presents the measurement items used in the questionnaire. A seven-point Likert scale, ranging from “Strongly Disagree” to “Strongly Agree,” was used to gauge respondents' attitudes and perceptions about various factors related to digital transformation in cooperatives. The measurement items are carefully designed to assess the constructs

Journal of Information Systems Engineering and Management
2025, 10(54s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

identified in the research model, ensuring that the data collected provides a comprehensive understanding of the cooperative's readiness for digitalization.

In addition, the demographics of respondents, including both individual respondent profiles and organizational profiles, are presented in Table 3 and Table 4. Table 3 provides an overview of the demographic characteristics of the individual respondents, such as their position, experience, and familiarity with technology, which may influence their responses. Table 4 details the organizational profiles of the cooperatives, including factors like the size of the cooperative, its level of digital engagement, and the resources available for implementing digital transformation. These tables help contextualize the study's findings by offering insight into the background and characteristics of the respondents and the organizations they represent.

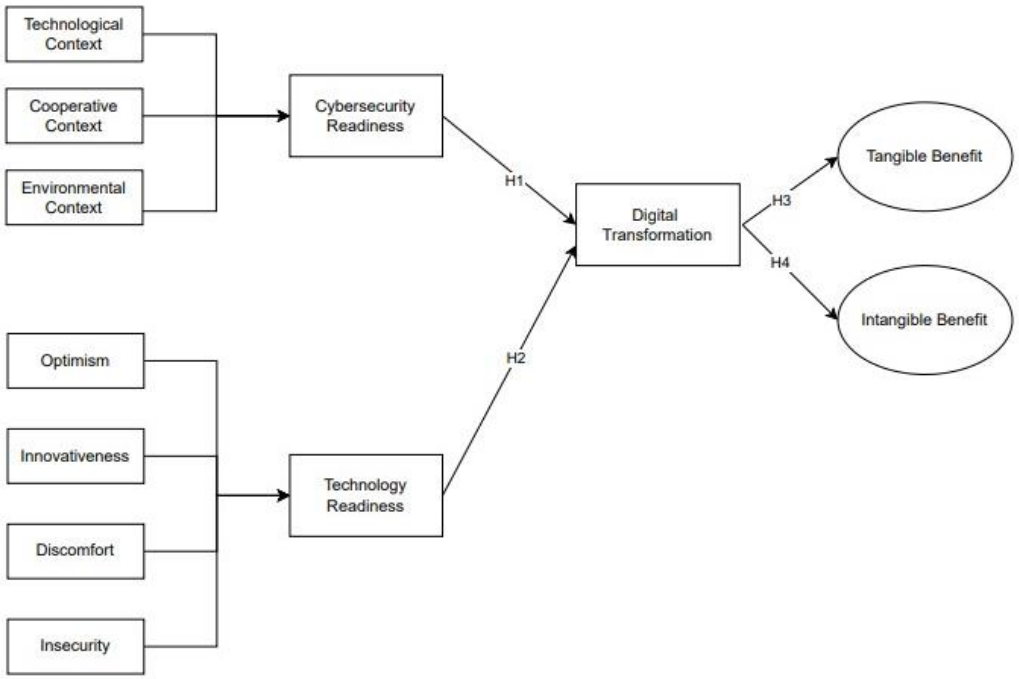

Figure 1. Research Model

Table 1. Research Model Description.

Build	Definition
Technology context (Berlilana et al., 2021; Hasan et al., 2021)	The characteristics and capabilities of information technology systems to support cybersecurity in an organization can influence organizational decisions in adopting technological innovations.
Organizational context (Hasan et al., 2021; Neri et al., 2024)	internal characteristics of the organization such as top management support, organizational culture, and skilled employee skills in managing operations within the organization.
Environmental context (Al-Sharhan et al., 2024; Berlilana et al., 2021; Hasan et al., 2021)	External factors that influence an organization's technology decisions, such as government regulations and industry standards that impact an organization's security readiness and technology readiness.
Cyber Security Readiness (Berlilana et al., 2021; Hasan et al., 2021)	The level of awareness, readiness, and commitment of the organization in preventing, responding to cyber attacks, and protecting organizational assets.
Optimism (Minzar & Mishra, 2024)	In the context of Technology Readiness reflects the belief that technology will provide significant benefits, such as improved operational efficiency, better

Research Article

	security, and enhanced member trust in cooperatives. This belief drives organizations to be more open to adopting digital technologies and improving their operational processes.
Innovative (Chang & Chen, 2021)	Innovative in technology readiness refers to the willingness and ability to adopt new technologies to improve operations and provide creative solutions to challenges.
Discomfort (J. Zhao et al., 2025)	Discomfort arises when individuals or organizations experience unease about using or adopting new technologies. It can be caused by perceived complexity or inefficiency of new systems.
Insecurity (Aljaradat et al., 2024)	Insecurity refers to concerns about data security and privacy risks when adopting new technologies. In a cooperative context, it relates to the fear of cyberattacks, data breaches, and the potential loss of trust.
Technology readiness (Chang & Chen, 2021; Parasuraman, 2000)	The maturity of the organization in terms of digital transformation of technology, user skills, and the ability to accept and use new technologies to support organizational goals.
Digital Transformation (Pangandaheng et al., 2022)	A process of change that involves the application of digital technologies to create new value.
Real benefits (Buglea et al., 2025; Minzar & Mishra, 2024; N. Zhao et al., 2023)	The benefits obtained by the organization and can be directly measured such as increased operational efficiency, cooperative transparency, income, cost savings and expansion of cooperative services.

Next Measurement Items in the Questionnaire, The following table presents the measurement items used in the questionnaire, designed to assess various factors related to the study. A seven-point Likert scale, ranging from "Strongly Disagree" to "Strongly Agree," was employed to evaluate respondents' perceptions and attitudes. This scale allows for a nuanced understanding of participants' views, providing a clear indication of the degree to which they agree or disagree with each statement. The use of this scale ensures that the data collected captures a spectrum of opinions, enhancing the reliability and depth of the analysis. The measurement items cover key constructs relevant to the study, and respondents were asked to rate their level of agreement with each item, contributing valuable insights into the readiness of cooperatives for digital transformation.

Table 2. Measurement Items in the Questionnaire.

Code	Cyber Security Readiness-Technology Context (TC)
TC1	The cooperative has adequate and competent experts in the field of information technology in managing cyber security.
TC2	The cooperative has adequate infrastructure to manage cyber security.
TC3	The technological equipment owned by the Cooperative to ensure cyber security is adequate.
	Cybersecurity Readiness-Cooperative Context (CC)
CC1	The cooperative has employees who are skilled in managing cyber security.
CC2	The cooperative organizes training to improve staff capabilities in cyber security.
CC3	Cooperatives provide resources to manage cybersecurity.
	Cyber Security Readiness-Environmental Context (EC)
EC1	Cooperatives always try to establish communication with related parties to maintain cyber security.
EC2	The cooperative continues to improve cyber security with related parties.
EC3	Cooperatives learn from experience to address cybersecurity issues quickly and accurately.
	Optimism for Technology Readiness (OPT)
OPT1	I feel that digital technology can improve the operational efficiency of cooperatives.
OPT2	With Digital Transformation in Cooperatives, I am sure that cooperatives can provide better services to cooperative members.
OPT3	I believe the use of digital technology will provide benefits for cooperatives.

Journal of Information Systems Engineering and Management
2025, 10(54s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

	Innovative Technology Readiness (INV)
INV1	Our cooperative actively seeks out the latest innovations to leverage technology to improve operational performance.
INV2	Cooperatives encourage the use of digital technology to create more innovative services for cooperative members.
INV3	I feel that with the development of innovation and renewal of cooperative technology, cyber security is always being updated by cooperatives.
	Technology Readiness-Technology Discomfort (DCT)
DCT1	If the co-op uses new technology, I find it very difficult to learn how to use it amidst my busy schedule.
DCT2	Using new technology often slows down my work compared to using manual (traditional) methods.
DCT3	Having to rely on technology makes me uncomfortable in completing my tasks.
	Technology Readiness-Technology Insecurity (INC)
INC1	I am concerned that personal data and confidential cooperative information can be misused through digital technology.
INC2	I have doubts about the security of the cooperative technology system.
INC3	I feel the co-op does not have procedures in place to address potential technology security issues.
	Digital Transformation (TDSI)
TDS1	Cooperatives have adequate technological infrastructure to support digital transformation.
TDSI2	Cooperatives have adopted digital technology; comprehensively to support cooperative operations and management.
TDSI3	Cooperatives are very open to innovation and the application of new technologies to improve operational efficiency.
	Real Benefits (TB)
TBC1	The use of digital technology has the potential to save our cooperative's operational costs.
TB2	Digital technology can speed up the completion of work processes.
TBC3	By starting to use technology, our cooperative can expand access to services to members.
	Intangible Benefits (IB)
IB1	The use of digital technology can increase member trust in cooperatives.
IB2	We believe that digital technology can create better experiences and loyalty for cooperative members.
IB3	Cooperative employees feel more motivated to work when using digital technology.

Table 3. Sample Demographics.

Demographic Variables	Category	Frequency	Percentage (%)
Gender	Man	143	54.4%
	Woman	120	45.6%
Age	<24 Years	37	14.1%
	25-39 Years	126	47.9%
	40-50 Years	100	38%
Level of education	Diploma	47	17.9%
	Bachelor	169	64.3%
	Control	47	17.9%
Duration of Respondents Management in Cooperatives	1-5 Years	181	70.4%
	6-10 Years	82	29.6%

Journal of Information Systems Engineering and Management
2025, 10(54s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Table 4. Organizational Profile.

Organizational Variables	Category	Frequency	Percentage (%)
Type of Business Field	Saving and loan cooperative	148	56.3%
	Production Business Cooperative	18	6.8%
	Consumer Business Cooperative	97	36.9%
Numbers of Workers	1-5 People	181	68.8%
	6-8 People	82	31.2%
Adopting information system in Cooperative	Yes	182	69.2%
	NO	81	30.8%
Adopting Anti-Virus Software in Cooperative	Yes	152	57.8%
	NO	111	111%
Adopting Services for Email Spam Filtering in Cooperatives	Yes	144	54.8%
	NO	119	45.2%
Adopting Virtual Private Network (VPN) Services for Cooperative Network Security	Yes	81	30.8%
	NO	182	69.2%
Adopting Services for the Use of Cyber Security Threat Detection Systems	Yes	94	35.7%
	NO	169	64.3%

RESULTS

In the results and discussion chapter, the author will explain and present the results of data processing and model analysis using the Structural Equation Modeling method with the Partial Least Squares (SEM-PLS) approach. The analysis was conducted to evaluate the measurement model and structural model to test the relationship between variables that have been formulated in the hypothesis. This evaluation is conducted to ensure the validity, reliability and predictive power of the model used (Zhai et al., 2022). This process is in line with the approach widely used in digital transformation studies in small and medium-sized organizations.

3.1 Validity and Reliability of Measurement Model

Initial analysis of the measurement model shows that all indicators have loading factor values above 0.70 which indicates good convergent validity. The Average Extracted (AVE) value for each construct also exceeds 0.50 meeting the criteria suggested by (January et al., nd). In addition, the composite Reliability (CR) and Cronbach's Alpha values for all constructs are above 0.70, indicating adequate internal reliability. The table below will describe the data processing process generated and carried out using SEM-PLS 4.1.1.2.

A. Convergent Validity

Testing is done by looking at each construct indicator. An indicator is declared valid if its value is greater than 0.70, while the loading factor value above 0.50 to 0.60 can be considered sufficient, and (January et al., nd) states that if all AVE values >0.5, it indicates that the indicators are valid in measuring their respective constructs and meet the convergent validity criteria.

Journal of Information Systems Engineering and Management
2025, 10(54s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

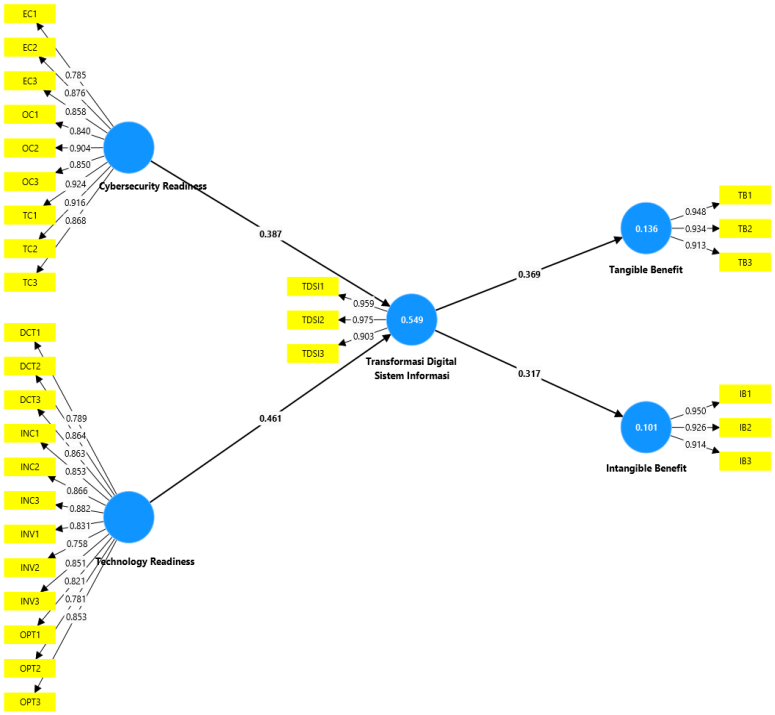

Figure 2. Smart-PLS 4.0 Algorithm Results

Table 5. Results of the smart-PLS 4.0 algorithm.

Variables	Indicator	Factor Loading
Cybersecurity Readiness	TC1	0.924
	TC2	0.916
	TC3	0.868
	CC1	0.840
	CC2	0.904
	CC3	0.850
	EC1	0.785
	EC2	0.876
	EC3	0.858
Technology Readiness	OPT1	0.821
	OPT2	0.781
	OPT3	0.853
	INV1	0.831
	INV2	0.758
	INV3	0.851
	DCT1	0.789
	DCT2	0.864
	DCT3	0.863
	INC1	0.853
	INC2	0.866
	INC3	0.882
Digital Transformation	TDSI1	0.959
	TDSI2	0.975
	TDSI3	0.903
Tangible Benefits	TB1	0.948

Journal of Information Systems Engineering and Management
2025, 10(54s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

	TB2	0.934
	TB3	0.913
Intangible Benefits	IB1	0.950
	IB2	0.926
	IB3	0.914

B. Internal Reliability

Furthermore, to ensure that there are no measurement-related problems, the author needs to test the reliability of the model. Reliability testing is carried out by looking at the Cronbach's Alpha and Composite Reliability values, which aim to test the reliability of the instrument in an instrument in the research model. (Marar et al., 2023) If all latent variable values have a Cronbach's Alpha value≥ 0.70 means that the construct has good reliability or the questionnaire used as a tool in this study has been consistent. In this study, it can be seen that the Cronbach's Alpha value shows satisfactory results, namely > 0.70.

Table 6. Composite Reliability and Conbach's Alpha Test Results.

Variables	Cronbach's Alpha	Composite Reliability	AVE
Cybersecurity Readiness	0.960	0.965	0.757
Technology Readiness	0.961	0.965	0.698
Digital Transformation of Information Systems	0.941	0.962	0.895
Tangible Benefits	0.924	0.952	0.868
Intangible Benefits	0.923	0.951	0.865

C. Discriminant Validity (Fornell-Larcker Criterion)

The next step is to compare the correlation between variables with the AVE root.($\sqrt{\boldsymbol{AVE}}$). The measurement model has good discriminant validity if$\sqrt{\boldsymbol{AVE}}$ each variable is greater than the correlation between the variables. The value$\sqrt{\boldsymbol{AVE}}$ can be seen from the Fornell Larcker Criterion Smart-PLS 4.0 output.

Table 7. Results of Discriminant Validity Test (Fornell Larcker Criterion).

Construct	Cybersecurity Readiness	Intangible Benefits	Tangible Benefits	Technology Readiness	Digital Transformation
Cybersecurity Readiness	**0.870**	0.336	0.289	0.523	0.628
Intangible Benefits		**0.930**	0.759	0.209	0.317
Tangible Benefits			**0.932**	0.197	0.369
Technology Readiness				**0.835**	0.664
Digital Transformation					**0.946**

Journal of Information Systems Engineering and Management
2025, 10(54s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

From**table 8**above, it can be concluded that for each construct is greater than the correlation between one construct and another construct in the model. The value based on the statement above, then the construct in the estimated model meets the criteria of discriminant validity.$\sqrt{AVE}$

3.2 Hypothesis Testing Results

The estimation result for the influence in the structural model must be significant. This significant value can be obtained by the bootstrapping procedure. Seeing the significance of the hypothesis by looking at the parameter coefficient value and the significant value of the t-statistic in the bootstrapping report algorithm. It can be known whether it is significant or not significant from the t-table at alpha 0.05 (5%) = 1.96. Then the t-table is compared with the t-count (t-statistic).

Table 8. Hypothesis Testing Results.

Hypothesis	Relationship Between Variables	Path Coefficient (β)	T statistics	P-Value	Information
H1	Cybersecurity Readiness -> Digital Transformation	0.387	4,938	0,000	ACCEPTED
H2	Technology Readiness -> Digital Transformation	0.461	7,551	0,000	ACCEPTED
H3	Digital Transformation -> Intangible Benefits	0.317	4,580	0,000	ACCEPTED
H4	Digital Transformation -> Tangible Benefit	0.369	5,418	0,000	ACCEPTED

Discussion of the results of hypothesis testing on the structural model:

1. The Impact of Cybersecurity Readiness on Digital Transformation:The results show that the path coefficient value is 0.387 with a t-statistic value of 4.938. Because the t-statistic value is greater than the t-table (1.96) and the P-Value value (0.000) is smaller than the significance level of 0.05, thenHypothesis accepted (Cybersecurity Readiness has a positive and significant influence on Digital Transformation).
2. The Influence of Technology Readiness on Digital Transformation:This hypothesis test produces a path coefficient value of 0.461 and a t-statistic value of 7.551. The t-statistic value which is greater than the t-table (1.96) and the P-Value (0.000) which is less than 0.05 indicate thathypothesis accepted (Technology Readiness has a positive and significant effect on Digital Transformation).
3. The Impact of Digital Transformation on Intangible Benefits:for this path, the path coefficient is 0.317 with a t-statistic of 4.580. Because the t-statistic is greater than the t-table (1.96) and the P-Value (0.000) is less than 0.05,Hypothesis is accepted (Digital Transformation has a positive and significant influence on Intangible Benefits).
4. The Impact of Digital Transformation on Tangible Benefits:The results show a path coefficient of 0.369 and a t-statistic of 5.418. The t-statistic value is greater than the t-table (1.96) and the P-Value (0.000) is less than 0.05, it is consideredHypothesis accepted (Digital Transformation has a positive and significant effect on tangible benefits).

DISCUSSION

Digital transformation in the cooperative sector has become one of the key elements in driving modernization and operational efficiency. Based on the results of the study, it was found that technological readiness and cybersecurity play an important role in determining the success of digital transformation of cooperatives in Bandung. Technological readiness that includes adequate digital infrastructure and optimal application of information technology can drive

Journal of Information Systems Engineering and Management
2025, 10(54s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

more effective and efficient digitalization of work processes. The success of this digitalization cannot be separated from the readiness of cybersecurity which is an important foundation in protecting data and digital transactions from cyber threats that continue to grow. In line with that, strengthening human resources (HR) in operating digital technology is a strategic step to ensure that the adopted technology can be implemented optimally. Research by (Sari et al., 2022) shows that the implementation of good information security practices in digital systems requires active involvement and awareness from all human resources in the organization. Strong management support and ongoing training can improve technological readiness and prevent risks caused by human error in operating digital technology. This confirms that investment in improving HR competency will encourage active involvement in the change process, as well as minimize resistance to new technologies. In addition, digitalization in cooperatives has also been shown to increase member participation and expand market access. (Minzar & Mishra, 2024) revealed that digitalization allows cooperatives to optimize member engagement through interactive digital platforms, so that communication and decision-making can be carried out more transparently and accountably. Digitalization also opens up opportunities for cooperatives to expand business networks and optimize services to members in real-time. To achieve the goal of effective and sustainable digital transformation, several strategic steps can be implemented by cooperatives. First, cooperatives need to improve cybersecurity readiness by strengthening data protection policies and access authentication systems. This step needs to be supported by regular cyber threat awareness training for cooperative administrators and members. Second, improving technological readiness is a top priority through modernizing hardware and software that supports digitalization. This readiness needs to be balanced with improving HR skills so that they can operate technology optimally. The next strategic step is to focus on human resource development. Investment in training and development of digital competencies not only improves HR capabilities in adapting but also builds a culture of innovation that supports change. Research (Sari et al., 2022) emphasized that management support, cues to action, and a strong organizational culture play a significant role in building HR involvement in digital transformation. This support not only increases HR readiness in adopting new technologies but also encourages better collaboration and innovation in the cooperative environment. Finally, regular evaluation and monitoring of technology readiness and cybersecurity policies need to be carried out consistently. This is important to identify security gaps and ensure that the technology used remains relevant and safe from new threats. Continuous monitoring also helps cooperatives adjust their digital strategies according to dynamic technological developments. By implementing these strategic steps, it is hoped that cooperatives will be able to maximize the potential of digitalization, strengthen competitiveness, and create added value for their members in the increasingly competitive era of digital transformation.

This study has several limitations that should be taken into account. First, the research was conducted on cooperatives in Bandung, which may not fully represent cooperatives in other regions or countries. Differences in access to technology, cybersecurity infrastructure, and digital literacy may vary across regions, potentially influencing the findings. Future research could expand the scope by including cooperatives from diverse geographical areas to compare regional differences and their impact on digital readiness and transformation. Additionally, while this study involved a substantial number of cooperative managers, the sample size and composition may not fully capture the diversity of cooperative types and sectors. To improve the generalizability of the findings, future research could consider investigating cooperatives from different industries, such as agricultural, financial, or service cooperatives. Moreover, this study employed a cross-sectional design, offering insights at a single point in time. Although this provides valuable data on the current state of digital readiness in cooperatives, it does not account for the dynamic nature of digital transformation over time. Longitudinal studies would be beneficial to track the progress of digital transformation in cooperatives over several years, providing a deeper understanding of the long-term effects of technology adoption and cybersecurity practices. Another limitation of the study is its focus on technological readiness and cybersecurity readiness, while other factors such as organizational culture, leadership support, and financial resources may also play significant roles in the success of digital transformation. Future research could address these additional factors, offering a more comprehensive view of the enablers and barriers to digital transformation in cooperatives.

For future research, it would be valuable to conduct comparative studies across different regions to understand how external factors, such as technological infrastructure, regulatory support, and cultural attitudes toward technology, affect digital transformation in cooperatives. Longitudinal research could also be explored to examine the continuous

progress and long-term impact of digital adoption in cooperatives. Additionally, research could delve into the role of organizational culture and leadership in supporting or hindering digital transformation. Understanding how these elements interact with technology readiness and cybersecurity readiness could provide a more holistic framework for cooperatives to succeed in their digital transformation efforts. Finally, future research could examine the direct impact of digital transformation on the financial performance, member engagement, and service delivery of cooperatives, helping to identify measurable outcomes of digital adoption..

REFRENCE

[1] Al Maazmi, A., Piya, S., & Araci, Z. C. (2024). Exploring the Critical Success Factors Influencing the Outcome of Digital Transformation Initiatives in Government Organizations. In *Systems* (Vol. 12, Issue 12). Multidisciplinary Digital Publishing Institute (MDPI). https://doi.org/10.3390/systems12120524

[2] Aljaradat, A., Sarkar, G., & Shukla, S. K. (2024). Modelling cybersecurity impacts on digital payment adoption: A game theoretic approach. *Journal of Economic Criminology*, *5*, 100089. https://doi.org/10.1016/j.jeconc.2024.100089

[3] Al-Sharhan, A., Alsaber, A., Al Khasham, Y., Al Kandari, A., Nafea, R., & Setiya, P. (2024). The Influence of Governmental Support on Cyber-Security Adoption and Performance: The Mediation of Cyber Security and Technological Readiness. *International Journal of Business Data Communications and Networking*, *19*(1). https://doi.org/10.4018/IJBDCN.341264

[4] Berlilana, Noparumpa, T., Ruangkanjanases, A., Hariguna, T., & Sarmini. (2021). Organization benefit as an outcome of organizational security adoption: The role of cyber security readiness and technology readiness. *Sustainability (Switzerland)*, *13*(24). https://doi.org/10.3390/su132413761

[5] Buglea, A., Cişmaşu, I. D., Gligor, D. A. G., & Jurcuţ, C. N. (2025). Exploring the Impact of Digital Transformation on Non-Financial Performance in Central and Eastern European Countries. *Electronics (Switzerland)*, *14*(6). https://doi.org/10.3390/electronics14061226

[6] Chang, Y. W., & Chen, J. (2021). What motivates customers to shop in smart shops? The impacts of smart technology and technology readiness. *Journal of Retailing and Consumer Services*, *58*. https://doi.org/10.1016/j.jretconser.2020.102325

[7] Eliza, F., Fadli, R., Ramadhan, M. A., Sutrisno, V. L. P., Hidayah, Y., Hakiki, M., & Dermawan, D. D. (2024). Assessing student readiness for mobile learning from a cybersecurity perspective. *Online Journal of Communication and Media Technologies*, *14*(4), e202452. https://doi.org/10.30935/ojcmt/15017

[8] Farfán Chilicaus, G. C., Licapa-Redolfo, G. S., Arbulú Ballesteros, M. A., Corrales Otazú, C. D., Apaza Miranda, S. J., Flores Castillo, M. M., Castro Ijiri, G. L., Guzmán Valle, M. D. los Á., & Arbulú Castillo, J. C. (2025). Digital Transformation and Sustainability in Post-Pandemic Supply Chains: A Global Bibliometric Analysis of Technological Evolution and Research Patterns (2020–2024). *Sustainability*, *17*(7), 3009. https://doi.org/10.3390/su17073009

[9] Gefen, D., Rigdon, E. E., & Straub, D. (2011). An update and extension to SEM guidelines for administrative and social science research. In *MIS Quarterly: Management Information Systems* (Vol. 35, Issue 2). University of Minnesota. https://doi.org/10.2307/23044042

[10] Hasan, S., Ali, M., Kurnia, S., & Thurasamy, R. (2021). Evaluating the cyber security readiness of organizations and its influence on performance. *Journal of Information Security and Applications*, *58*. https://doi.org/10.1016/j.jisa.2020.102726

[11] January, B. ·, Hair, J. F., Tomas, G., Hult, M., Ringle, C. M., & Sarstedt, M. (n.d.). *A Primer on Partial Least Squares Structural Equation Modeling (PLS-SEM)*. https://www.researchgate.net/publication/354331182

[12] Jhantasana, C. (2023). Should A Rule of Thumb be used to Calculate PLS-SEM Sample Size. *Asia Social Issues*, *16*(5), e254658. https://doi.org/10.48048/asi.2023.254658

[13] Lin, J. S. C., & Hsieh, P. L. (2007). The influence of technology readiness on satisfaction and behavioral intentions toward self-service technologies. *Computers in Human Behavior*, *23*(3), 1597–1615. https://doi.org/10.1016/j.chb.2005.07.006

[14] Luigi Core, G., Antonucci, G., & Venditti, M. (n.d.). Digital Transformation and Sustainability in Cooperatives Enterprises: A Literature Review. *Antonio Gitto International Journal of Business Research Management (IJBRM)*, *15*, 43.

Research Article

[15] Marar, S., Hamza, M. A., Ayyash, M., & Abu-Shaheen, A. (2023). Development and validation of an instrument to assess the knowledge and perceptions of predatory journals. *Heliyon*, *9*(11). https://doi.org/10.1016/j.heliyon.2023.e22270

[16] Minzar, M., & Mishra, M. K. (2024). Digital Transformation In Cooperatives: Opportunities And Challenges. *IOSR Journal of Business and Management*, *26*(10), 23–31. https://doi.org/10.9790/487X-2610132331

[17] Morales-Sáenz, F. I., Medina-Quintero, J. M., & Reyna-Castillo, M. (2024). Beyond Data Protection: Exploring the Convergence between Cybersecurity and Sustainable Development in Business. In *Sustainability (Switzerland)* (Vol. 16, Issue 14). Multidisciplinary Digital Publishing Institute (MDPI). https://doi.org/10.3390/su16145884

[18] Nalmpanti, A. D., Wong, C. Y., & Oghazi, P. (2024). Collaborating for innovation: The inhibiting role of constraints. *Journal of Innovation and Knowledge*, *9*(3). https://doi.org/10.1016/j.jik.2024.100504

[19] Nepal, S., Ko, R. K. L., Grobler, M., & Camp, L. J. (2022). Editorial: Human-Centric Security and Privacy. In *Frontiers in Big Data* (Vol. 5). Frontiers Media S.A. https://doi.org/10.3389/fdata.2022.848058

[20] Neri, M., Niccolini, F., & Martino, L. (2024). Organizational cybersecurity readiness in the ICT sector: a quanti-qualitative assessment. *Information and Computer Security*, *32*(1), 38–52. https://doi.org/10.1108/ICS-05-2023-0084

[21] Pangandaheng, F., Maramis, J., Saerang, D., Dotulong, L., Soepeno, D., Pangandaheng, F., Baren Maramis, J., Paul Elia Saerang, D., & Otto Herman Dotulong, L. (2022). Digital Transformation: A literature in the business and government sector. *10*(2), 1106–1115.

[22] Parasuraman, A. (2000). Technology Readiness Index (TRI) A Multiple-Item Scale to Measure Readiness to Embrace New Technologies. In *Journal of Service Research* (Vol. 2, Issue 4).

[23] Saeed, S., Altamimi, S. A., Alkayyal, N. A., Alshehri, E., & Alabbad, D. A. (2023). Digital Transformation and Cybersecurity Challenges for Businesses Resilience: Issues and Recommendations. In *Sensors* (Vol. 23, Issue 15). Multidisciplinary Digital Publishing Institute (MDPI). https://doi.org/10.3390/s23156666

[24] Santos, F. J., Guzmán, C., & Ahumada, P. (2024). Assessing the digital transformation in agri-food cooperatives and its determinants. *Journal of Rural Studies*, *105*. https://doi.org/10.1016/j.jrurstud.2023.103168

[25] Sari, P. K., Handayani, P. W., Hidayanto, A. N., Yazid, S., & Aji, R. F. (2022). Information Security Behavior in Health Information Systems: A Review of Research Trends and Antecedent Factors. In *Healthcare (Switzerland)* (Vol. 10, Issue 12). MDPI. https://doi.org/10.3390/healthcare10122531

[26] Subekti, R., Ohyver, D. A., Judijanto, L., Satwika, I. K. S., Umar, N., Hayati, N., Handika, I. P. S., Joosten, Migunani, Boari, Y., & Saktisyahputra. (2024). *Transformasi Digital : Teori & implementasi Menuju Era Society 5.0* (E. Rianty, Ed.; 1st ed., Vol. 1). PT.SonpediaPublishingIndonesia.

[27] Vial, G. (2019). Understanding digital transformation: A review and a research agenda. In *Journal of Strategic Information Systems* (Vol. 28, Issue 2, pp. 118–144). Elsevier B.V. https://doi.org/10.1016/j.jsis.2019.01.003

[28] Vinh, L., Ngoc Long, N., Vinh Quang, L., Chi Minh City, H., & Chandra Debnath, N. (2023). Managing Risks in the Adoption of Cybersecurity Technology in Manufacturing Enterprises: Identification and Assessment. In *IJCA* (Vol. 30, Issue 4). https://www.researchgate.net/publication/377443403

[29] Zhai, H., Yang, M., & Chan, K. C. (2022). Does digital transformation enhance a firm's performance? Evidence from China. *Technology in Society*, *68*. https://doi.org/10.1016/j.techsoc.2021.101841

[30] Zhao, J., Li, X., & Gao, Z. (2025). From innovativeness to insecurity: unveiling the facets of translation technology use behavior among EFL learners using TRI 2.0. *Humanities and Social Sciences Communications*, *12*(1). https://doi.org/10.1057/s41599-025-04777-0

[31] Zhao, N., Hong, J., & Lau, K. H. (2023). Impact of supply chain digitalization on supply chain resilience and performance: A multi-mediation model. *International Journal of Production Economics*, *259*. https://doi.org/10.1016/j.ijpe.2023.108817