Journal of Magnetism and Its Applications

ISSN: 2797-507X

https://doi.org/10.5281/zenodo.24499742

THE TRADE-READY DIGITAL MODERNIZATION (TRDM) METHODOLOGY: AN INTEGRATED ASSESSMENT OF CYBERSECURITY, BUSINESS CONTINUITY, AND EXPORT READINESS FOR SMALL AND MEDIUM-SIZED ENTERPRISES

Sheeraz Ali Shahzad Soomro[*1], Sher Muhammad Mahar[2], Sohaib Naseer[3], Malik Hassam[4]

*[*1]General Manager – Operations, Trading Corporation of Pakistan (TCP) – Government of Pakistan*
[2]General Manager-international Trade (Internal Control & Compliance) Head of Devision Trading Corporation of Pakistan (Pvt) Ltd.- TCP
[3]Software Developer, Department of Computer Science
[4]Digital Marketing & E-commerce Specialist

[*1]sheerazocp@gmail.com, [2]shermahar@gmail.com, [3]maliksohaibnaseer@gmail.com, [4]malikhassam033@gmail.com

Article History

Keywords:
Trade-Ready Digital Modernization (TRDM), Small and Medium-Sized Enterprises (SMEs), Cybersecurity, Business Continuity Management, Export Readiness, Digital Transformation, Organizational Resilience, Digital Trade.

Article History
Received: 25 August 2026
Accepted: 09 November 2026
Published: 24 November 2026

Copyright @Author
Corresponding Author: *
Sheeraz Ali Shahzad Soomro

Abstract

Digital technologies are rapidly evolving and changing the business landscape, leading to new opportunities and challenges for Small and Medium-Sized Enterprise (SMEs). While digital modernization is a tool that helps SMEs enhance business efficiency, competitiveness and access to international markets, cybersecurity risks, business continuity risks and lack of export readiness are still serious barriers for many small enterprises. This study introduces the integrated assessment framework called the Trade-Ready Digital Modernization (TRDM) Methodology that is proposed to assess and enhance the digital readiness of SMEs. The suggested methodology includes three interrelated dimensions: Cybersecurity preparedness, Business continuity management, and Digital export readiness. In the cybersecurity dimension, information security practices and data protection, cyber risk management, and organizational awareness are explored. The business continuity aspect assesses the disaster recovery plans, operational resilience, risk mitigation, and capacity to continue critical business operations during disasters. The export readiness dimension measures digital infrastructure, international trade, regulatory compliance, digital payment systems and access to global markets. For identification of organizational weaknesses and priorities for modernization, an integrated assessment approach, with measurable indicators, maturity levels and practical implementation strategies, is developed. It also offers a roadmap to help SMEs build their digital skills and minimize operational and technological risks. The goal of the TRDM methodology is to offer a practical base for organization resilience enhancement, international business confidence and sustainable involvement in digital trade. The framework proposed adds to the existing literature by linking cybersecurity, business continuity, and export readiness in a single digital modernization assessment model..

INTRODUCTION

The digital landscape has been changing rapidly and has profoundly influenced the world of business, presenting opportunities for organisations to enhance their global market access, competitiveness and operational efficiency. Small and Medium-Sized Enterprises (SMEs) are very important in the field of economic development, employment creation, innovation and international trade. While the value of SMEs is undeniable, numerous obstacles still exist for them to embrace modern digital technologies and set up secure, reliable and internationally competitive business operations. In fact, digital transformation has become a mandatory condition for SMEs as business models are no longer up to scratch for today's markets. For SMEs, the use of digital platforms, cloud-based systems, AI, electronic payments and data management helps to boost productivity and build customer and business partner engagement [5,20]. For successful digital modernization, however, it is not enough just to implement new technologies; cyber security management, operational resilience and compliance with international trade needs must also be taken into account.

One of the biggest challenges in this digital transformation of SMEs is cyber security. The growing reliance on digital platforms, cloud-based services, electronic communication, online transactions and transactions carries a range of cyber risks such as ransomware, phishing attacks, unauthorised access, data breaches and financial fraud. SMEs tend to be constrained in both terms of resources available and technical expertise, as well as in their cybersecurity setup. The restrictions make them as easy as ever targets for cyber events that might disrupt business operations, compromise confidential information and destroy customer trust. To secure their organizations against a variety of cyber threats, they must have suitable security policies, routinely evaluate risks, safeguard sensitive data, and take preventive and corrective security measures. There are international standards like ISO/IEC 27001 which give a structured approach to information security management, and the NIST Cybersecurity Framework gives hands-on guidance on how to identify, protect against, detect, respond to, and recover from cybersecurity threats [16,25]. Hence, the preparedness for cybersecurity is an integral part of digital modernization and a crucial demand of SMEs joining in international digital markets.

Besides cybersecurity, business continuity management is one more critical determinant towards the long-term sustainability and stability of SMEs. Unforeseen events such as cyberattacks, natural disasters, technological failures, supply chain disruptions, financial issues, and more can disrupt business operations. These disruptions can lead to business closures (temporary or permanent), customer dissatisfaction, reduced productivity, and financial losses. Resilience is crucial for any organization because it allows them to prepare for potential threats, make the necessary preparations, keep vital operations running and bounce back from unexpected disruptions. Recent studies on the issue of organizational resilience highlight the importance of adaptability, planning and continual improvement for a business to react positively to an uncertain situation [8,35]. Likewise, ISO 22301 offers worldwide requirements to establish and maintain business continuity management systems. Yet, most SMEs do not have formal continuity planning, disaster recovery planning or systematic risk management in place. Business continuity assessment can be incorporated in the process of digital modernization, which can identify weaknesses in operations, minimize risks from disruption and ensure the continuity of business services.

Another key aspect of SME development in a more globalized world is export readiness. Several of the traditional challenges to engaging in international trade have been overcome by the use of digital technology, which allows businesses to communicate with customers overseas, use digital technology to promote products internationally, process international payments, and coordinate cross-border transactions. However, there is more to it than having an online business in order to be successful in the international markets. SMEs need to prove they have sufficient digital infrastructure, information security systems, operational systems, awareness of the regulations and to be able to satisfy the expectations of international customers. The factors that have been found to be key obstacles to SME export development in previous research are limited financial resources, lack of international experiences, regulatory problems and lack of market knowledge [9,22]. Digital skills can boost international competitiveness to foster innovation, market expansion, and access to global business networks. The importance of digital technologies in enhancing the competitiveness of SMEs and

enabling SMEs to participate in international value chains has also been highlighted by international trade institutions [17,28]. Therefore, export readiness should be reviewed together with the aspects of cybersecurity and business continuity rather than as an independent business.

Background of the Study

The speed of changing information and communication technologies has affected the way businesses operate, compete and engage in international markets. The Small and Medium-Sized Enterprises (SMEs) are a crucial component of the global economy as they play an important role in employment generation, economic growth, innovation and industrial development. Yet, as digital markets become competitive, new demands have surfaced for SMEs in terms of technological development, information security, operational security, and international market involvement. Business models face more difficulties in the digital environment where buyers, suppliers, banks and international trading partners rely on digital systems for many of their processes. The opportunities that digital transformation offers to SMEs include enhanced productivity, cost reduction, better customer relationships, and greater market impact [5]. However, the modernization of SMEs must be approached holistically, taking into account not only the use of technological systems but also the issue of cybersecurity, business continuity and export readiness.

Digital modernization is especially crucial to the success of modern businesses, which rely on connected technological systems for their financial transactions, information management, communication, marketing, and supply chain operations. These advances also bring with them dangers of cyber attacks, system failures, data loss, and unanticipated operational disruptions. The resource-based view states that the resources and capabilities that organizations possess make them sustainable in gaining competitive advantage, and dynamic capabilities highlight the adaptation to business environments [4,35]. To this end, SMEs have to introduce a digital approach that allows them not only to embrace digital technologies but also secure and reliable business operations. The proposed Trade-Ready Digital Modernization (TRDM) Methodology leverages this requirement by bringing together preparedness for cybersecurity, business continuity management (BCM) and export readiness into a single assessment framework.

Problem Statement

Many small and medium enterprises are still struggling to bring them all under digital transformation roof, as there are ample opportunities in this area for improving the competitiveness of SMEs. Current strategies often address technology adoption, cyber security, business continuity, or internationalization, but do not offer a single tool for measuring the impact of multiple strategies on organizational readiness. This disjointed approach can result in various issues because the SME could take on advanced digital technology, but not put in place the corresponding cybersecurity measures or business continuity plans. On the other hand, an organisation could have secure information systems, but not the operational capacities or international trade needs to participate in world markets.

Research Objectives

1. To analyse the status quo of digital transformation and modernization of SMEs.
2. To identify the major cybersecurity risks and assess the information security preparedness of SMEs.
3. To assess business continuity management and organizational resilience.
4. To determine the technological, operational and regulatory factors affecting SME export readiness.
5. To create measurable cyber security, business continuity and export readiness indicators.

Research Questions

1. What are the cybersecurity threats to the digital readiness and security of SMEs?
2. What is the level of implementation of continuity and disaster recovery to SMEs?
3. What are the technological and organisational factors that make SMEs export ready?

4. What are the possibilities of combining cyber security preparedness, business continuity and export readiness into a single assessment methodology?

Significance of the Study

The value of this study is that it suggests a unified approach to digital modernization for both cybersecurity and business continuity and export preparedness. The aforementioned areas have been covered in the previous studies, but they have not been explored together in relation to SMEs' digital preparedness. The TRDM methodology offers a holistic view, treating technological capabilities as part of organizational security, operational resilience as part of technology, and international trade needs as part of the organization.

The study adds to the body of work on digital transformation as it introduces a structured framework that bridges the three key aspects of organizational development. The study also serves as a basis for future research on the topics of digital maturity assessment, SME competitiveness, organizational resilience and internationalization. The framework is based on theories such as the resource-based view, dynamic capabilities theory, and the theories on organizational adaptation to business environment changes [4,35].

Scope and Limitations of the Study

This research will be limited to developing the Trade-Ready Digital Modernization (TRDM) Methodology for Small and Medium-Sized Enterprises (SMEs). The framework has three assessment dimensions: (1) cybersecurity preparedness, (2) business continuity management, and (3) export readiness. The cyber security aspect covers data protection, policies, identification of cyber risks, access management, awareness of employees and incident response. The business continuity element assesses the business risk management, disaster recovery planning, emergency preparedness, backup systems, and organisational resilience. The export readiness part is about digital infrastructure, electronic commerce, international payment skills, regulatory awareness, digital marketing and technology needs of cross-border business activities.

The methodology to be proposed should be used across various industries and geographical regions by SMEs. The assessment indicators can be adjusted based on the size of the organization, business activities, technological resources and the requirements for the international market. The framework also serves as a foundation to define digital maturity levels and action points for improvement. There are a number of limitations to the study. Firstly, there are significant differences in the industries, countries and organisational structures in which SMEs operate with respect to their digital capabilities and requirements. As such, the framework may need to be adapted prior to implementation in individual business contexts. Second, cybersecurity risks and international trade regulations are constantly changing and thus indicators for assessment should be reviewed and updated regularly. Third, some assessments may be less accurate because of the lack of reliable information regarding the organization. In some cases this may be because SMEs may not have documented their cybersecurity and/or business continuity procedures. Lastly, the proposed methodology of TRDM needs to be tested empirically in various sectors of SMEs and geographical areas to prove its reliability, practical effectiveness, and applicability in other sectors. The following are some of the restrictions that are seen, which will allow further research and development of the proposed framework.

LITERATURE REVIEW

With the growing relevance of digital technologies within business processes, researchers have focused considerable attention on digital transformation, especially on that of Small and Medium-Sized Enterprises (SMEs). Digital modernization is well known as a key enabler for organizations to be more productive, innovative, competitive and able to access international markets. Bharadwaj et al. [5] provided an explanation of digital business strategies as a means enabling the organizations to generate new opportunities by joining digital technologies with business goals and value-creation processes. In the same way, Khin and Ho [20] pointed out that there is a linkage between digital technology, organisational digital capacities and business performance, which is digital innovation for improving

organisational outcomes. Digital transformation goes beyond the mere introduction of specific technologies; it's a transformation of organisational structures, management processes, business models and operations. In their recent systematic research, Sagala and Őri [13] highlighted digital capabilities, organizational alignment, financial resources and continuous learning as important factors that contribute to successful SME digital transformation. They consider that SMEs need to plan for modernization in terms of their current capacities and constraints, and not to simply implement technologies without thought.

A theoretical understanding of the relationship between digital modernization and organizational competitiveness is offered by the resource-based view. Valuable resources and capabilities that competitors can be difficult to imitate offer an organization sustainable competitive advantages, according to Barney [4]. Digital infrastructure, technological skills, information management and organizational knowledge are important resources for business development in the context of SMEs. Teece expanded upon the dynamic capabilities theory, which focuses on how organizations acquire, combine and adapt resources in response to shifts in the business landscape [35]. Based on these theoretical frameworks, it can be concluded that the successful realization of digital modernization in SMEs needs to be accompanied by the creation of technological capacity with flexibility in adapting to market changes. At the same time, the concept of digital affordances in the generation of entrepreneurial opportunities and the development of entrepreneurial ecosystems was discussed by Autio et al. [3]. Hence, the technological resources, organizational capabilities and strategic management are an essential prerequisite for the proposed Trade-Ready Digital Modernization (TRDM) Methodology.

Various technological and organizational approaches have been used to study digital transformation in SMEs. Cloud computing, e-commerce, digital payment systems, AI, ERP, and data analytics are all key components that are enhancing business operations. In this study, Oliveira et al. [31] explored the factors that influence the adoption of cloud computing and emphasized that technology and organizational factors are important in the adoption of cloud-based services. In exploring digital transformation and customer value creation in SMEs, Matarazzo et al. [23] focused on the contributions that digital technologies and dynamic capabilities can make to enhancing business relationships and organizational performance. Likewise, Scuotto et al. [34] explored the link between digital business transformation and the innovation process and identified the role of digital technologies for organizational innovation. The introduction of digital technologies, however, doesn't mean digital modernization will be successful. SMEs should also take into account the skills of the workforce, management commitment, financial resources, technological compatibility and organizational readiness. The OECD [28] highlighted the need to build digital skills and to tackle digital obstacles for SMEs to fully reap the benefits of technology. The study findings show that digital transformation is not a one-off technology solution, but an enterprise-level initiative that demands a coordinated organizational strategy.

Digital Modernization

Digital modernization is an effort to systematically introduce advanced digital technologies into organizational processes, management systems, business processes and strategic planning. This is a significant step in the digital era as businesses are increasingly relying on digital infrastructure to boost productivity, minimize operational expenses, enhance communication, and stay competitive in the global marketplace. Digital modernization offers Small and Medium-Sized Enterprises (SMEs), the chance to enhance the efficiency of their organization and create new business models without having to deploy physical infrastructure like big enterprises. Cloud computing, artificial intelligence, e-commerce, enterprise resource planning systems, data analytics, and digital payment platforms are some of the digital technologies that play a vital part in the functioning of modern enterprises. As described by Bharadwaj et al. [5] digital business strategies combine technological capabilities with business objectives to offer novel opportunities to realize business value and business development.

Modernizing your digital environment is more than just setting up technological systems. It demands organizational changes in management practices, employee capabilities, information security,

operational procedures, customer service strategies. Teece [35] suggested that organizations must acquire dynamic capabilities to respond to market changes by modifying resources and processes. The same applies to Barney [4] who said that there are advantages in organizational resources and capabilities that can lead to sustainable competitive advantage. These theories suggest that, for successful digital modernization, SMEs should have the capability of creating technological resources and effectively applying them to meet business goals. OECD [28] emphasized the role of digital skills for enhancing productivity and competitiveness of SMEs. It is thus essential to view digital modernization in the context of ongoing organizational growth and development, which involves the integration of technology, strategic planning, cybersecurity readiness, and operational efficiency.

Digital Transformation and SME Competitiveness

The digital transformation is an important element of the competitiveness and sustainability of SMEs. It supports companies to optimize business processes, automate repetitive tasks, boost customer satisfaction, and gain access to new domestic and international markets. Digital technologies can help smaller businesses to coexist more effectively, by breaking down communication barriers, making information readily available and enabling better management of resources. Khin and Ho [20] underlined the significance of digital technology and digital capabilities in relation to digital innovation in support of organizational performance. Likewise, Matarazzo et al. [23] analyzed how digital transformation is affecting SMEs, and how digital capabilities are part of customer value creation and business development.

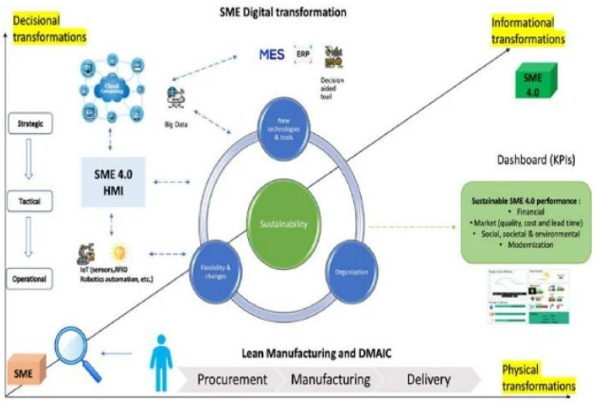

Fig 2.1 Digital Transformation and SME Competitiveness

Cybersecurity Challenges Facing SMEs

SMEs have come to rely on digital technologies, opening up their businesses to various types of cyber threats, which has put cybersecurity on the agenda. Internet-based applications, cloud computing services, electronic payment systems and digital communication systems are all tools which are used regularly by organizations to manage their operations. While these technologies are more efficient, they also open the door to hackers gaining access to sensitive data, spoofing companies, and committing financial fraud. Phishing, ransomware, malware, unauthorized access, identity theft, social engineering and data breaches are common cybersecurity threats. For SMEs these threats might pose a higher risk, as they usually lack financial resources, technical expertise and information security infrastructure.

Cybersecurity policies and systematic security management procedures are not in place, which is one of the challenges that impact SMEs and their businesses. Some businesses use simple anti-virus programs and passwords and don't have a full system of security measures in place. Some don't conduct frequent on-going cybersecurity training for employees, which can lead to human mistakes and unauthorized disclosure of information. The National Institute of Standards and Technology [26] states that organizational governance, risk identification, protective measures, threat detection, incident response, and recovery are crucial components of cybersecurity management. Likewise ISO/IEC 27001 [16] is a standard for the implementation of information security management systems and the control of organizational information security risks.

Cybersecurity Risk Assessment and Management

A systematic process for identifying, analysing, assessing and prioritising risks to an organisations information systems and digital infrastructure. It allows businesses to identify the areas where they may be vulnerable and take necessary steps to minimize the risk of a cyber incident and the potential damage. The first step in managing cybersecurity risks is to determine what information assets are critical, such as customer records, financial information, business documents, communication systems, and operational databases. Organizations need to identify what assets should be protected at the highest levels and assess threats that may impact the confidentiality, integrity and availability of these assets.

Business Continuity Management in SMEs

Business continuity management is the systematic approach to preparing organisations to keep key activities running during unexpected events and recover to normal operations in an acceptable time. SMEs should be especially concerned about it, as business disruptions can result in financial challenges, loss of customer satisfaction, and competitive disadvantage. The disruptions can be caused by cyberattacks, natural disasters, equipment failure, lack of electricity, supply chain disruptions, etc. A good business continuity management helps companies to identify crucial business processes, evaluate risks, develop recovery plans, and ensure the continuity of essential services in case of emergencies.

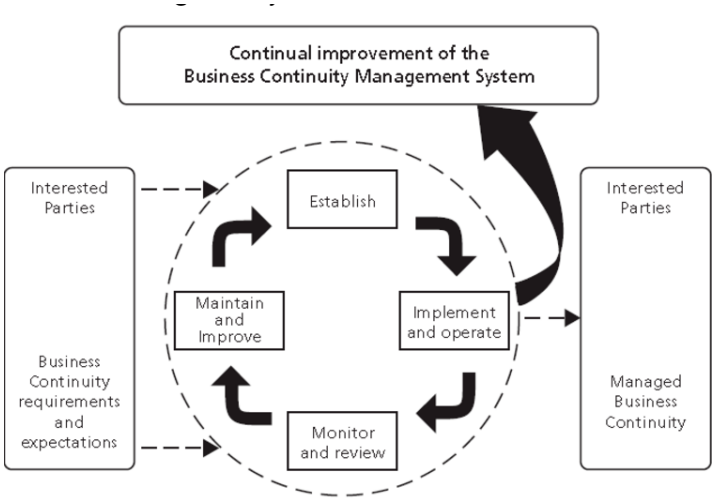

Fig 2.2 Business Continuity Management in SMEs

Disaster Recovery and Operational Resilience

Operational resilience and disaster recovery are synonymous and are designed to ensure organisational stability when disaster strikes. Disaster recovery is mostly about getting information technology systems, applications, networks, databases and digital services back up and running after a disaster. Operational resilience is more comprehensive as it refers to an organisation's capacity to continue operating, react to varying conditions and recover from various disruptions. These ideas are especially relevant for SMEs as their business activities nowadays rely heavily on digital infrastructure and information systems.

The National Institute of Standards and Technology [24] offers guidance on contingency planning for information systems, focusing on the need to have recovery procedures, backups, test, and restore technological services. By keeping secure data backups, alternative communication plans, recovery documentation, and having access to necessary resources, organizations can lessen the effects of a disruption. ISO 22301 [15] also highlights the need to have continuity procedures in place to help maintain and restore critical business activities.

Digital Trade and International Export Requirements

Digital trade has dramatically transformed international business activities, allowing organizations to share information, promote products, process payments, and create commercial relationships via digital platforms. Electronic commerce, online markets, digital marketing, cloud-based applications, and

electronic payment systems have opened up new opportunities for SMEs to enter the international markets. These have lowered some geographical, communication and market access limitations. The World Trade Organization (WTO) [42] explored how digital technologies affect trade worldwide and their potential to change global trade.

UNCTAD [37] highlighted the significance of cross-border data flows and of digital economic development, noting the increasing role of information infrastructure in international business. Likewise, the World Bank [40] pointed to the economic opportunities around digital technologies and how they can enhance access to information, markets and business services. The developments shows that the international market demands digital skills among SMEs.

Export Readiness and Digital Capabilities

Export Readiness is the readiness of an organisation to prepare, enter and participate in international markets successfully. It requires a number of organizational skills, such as financial resources, management skills, product competitiveness, market knowledge, technological infrastructure and the ability to do business internationally. The capacities are more and more tied to the digital technologies, as enterprises rely on electronic platforms to communicate with international clients, promote products, accept payments and organize cross-border transactions in the digital economy.

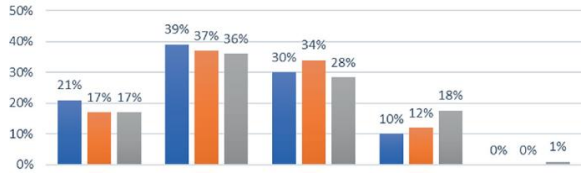

Fig 2.3 Export Readiness and Digital Capabilities

Financial constraints, lack of market information, lack of operational resources, and external market constraints were cited by Leonidou [22] as some of the barriers to export development faced by small businesses. Etemad [9] analyzed the internationalization process of SMEs and emphasized on the role of organizational resources and capabilities in the international business development. The studies show that export awareness is not only the internal organization but also the requirement of the market.

RESEARCH METHODOLOGY

The research design of this study is descriptive and analytical research in order to develop the methodology in the form of a Trade-Ready Digital Modernization (TRDM) Methodology for small and medium-sized enterprises (SMEs). The research is based on three key aspects of the digital modernization of SMEs - cyber security preparedness, business continuity management and export preparedness. The descriptive part provides information on current practices, challenges and capacities of SMEs, and the analytical part analyses the interactions, connections and relationships between the three dimensions and their impact on overall digital modernization readiness.

Cross-sectional survey design is suggested for data collection from the owners/managers of SMEs, the IT professionals and employees involved in the operation of SMEs. Data are collected at a single point in time to assess the existing level of digital preparedness. The study also draws on relevant academic literature, international standards and institutional reports to create assessment indicators for the TRDM framework. The assessment structure can be developed based on standards like ISO/IEC 27001:2022 [16], ISO 22301:2019 [15] and the NIST Cybersecurity Framework 2.0 [26].

The research design is suitable since the proposed methodology involves understanding the current practices of SMEs and insight into the relationship between cyber security, business continuity and export readiness. The result is a comprehensive evaluation tool that can assist SMEs in finding their strengths and determining their priorities for improvement.

Research Approach

The research method used in this research is a method that combines quantitative and qualitative methods. The quantitative component is dedicated to gathering measurable data on the cybersecurity measures, business continuity plans and readiness for export of SMEs. The qualitative element allows to gather more insight into organizational challenges, management decisions and barriers to digital modernization.

Data collected in quantitative form with structured questionnaires and closed ended questions and likert scale statements. The respondents have to assess their organizations' current practice, policy, resources and technological capabilities. The following five-point Likert scale is suggested: 1 (Strongly Disagree) to 5 (Strongly Agree).

The qualitative part could involve semi-structured interviews with selected owners of the SMEs, senior managers, IT personnel, and business development personnel. These interviews can help to pinpoint practicalities that may not be captured by answers to the questions on the questionnaire.

The combination of both approaches provides a broader understanding of the research problem. Quantitative analysis detects patterns and relationships, while qualitative provides explanations for patterns. This allows for the creation of a viable TRDM methodology that incorporates organizational capabilities that can be measured and actual real-life business scenarios.

Target Population and Sampling Technique

The target population are small and medium scale businesses across various lines of business. These can involve manufacturing, retail, information technology and professional services, wholesale and other business activity. The study aims at companies that are Small and Medium Enterprises (SMEs) that are utilizing digital technologies in their business processes or could be applying digital technologies to enhance productivity and access international markets.

The chief respondents are business owners, managing directors, general managers, IT managers, cyber security personals, operations managers and employees involved in export or business development activities. The individuals are deemed to be in an appropriate position because they are familiar with organizational technology, security practices, operational procedures, international business activity.

The respondents were proposed using a purposive sampling technique and were selected as they have information about the digital operations of their organization. Stratified sampling might also be considered where there is a suitable list of SMEs to ensure representation from a range of sectors and business sizes.

The size of the final sample should be based on the size of the population available, resources available, expected response rate, and statistical analysis requirements. In a quantitative study a sample size that is suitable may be determined by applying a known sample-size method or by statistical power analysis. Interviews may be used and participants selected according to their professional experience and knowledge of the dimensions of the research.

The following table presents the proposed respondent categories

Table 3.1: Target Respondent Categories

Respondent category	Relevant area of knowledge
SME owners and directors	Overall business strategy and digital investment
IT managers and professionals	Digital infrastructure and cybersecurity
Operations managers	Business continuity and operational risks
Export managers	International trade and export readiness
General managers	Organizational policies and management practices
Administrative employees	Daily use of digital systems and procedures

At this point the study does not make any assumptions regarding the country, city or sample size. These should be agreed upon based on the specific research context and availability of the SMEs involved.

Data Collection Methods

The information comes from academic journal articles, books, international standards, government documents and reports from trusted institutions. These sources will be used to put the foundation of the proposed framework and to find them related indicators.

Key sources are ISO/IEC 27001:2022 (information security management) [16], ISO 22301:2019 (business continuity management) [15], NIST Cybersecurity Framework 2.0 (cybersecurity risk management) [26], and OECD publications [27–30] on SME digital transformation and competitiveness.

Research Instrument Development

Structured questionnaire is the main research instrument which has been prepared based on the three aspects of the TRDM methodology. The tool aims to measure the current level of preparedness in the area of cybersecurity, business continuity management and export preparedness of SMEs.

Table 3.2: Proposed Likert Scale

Scale	Response	Interpretation
1	Strongly Disagree	Very low preparedness
2	Disagree	Low preparedness
3	Neutral	Moderate preparedness
4	Agree	High preparedness
5	Strongly Agree	Very high preparedness

The items in the questionnaire are formulated based on literature review, international standards, and previous studies on the SME digital transformation. The cybersecurity section is based on ISO/IEC 27001:2022 [16] and the NIST Cybersecurity Framework 2.0 [26]. The business continuity section is based on ISO 22301:2019 [15] and export readiness indicators are created on the basis of research work on internationalization of SMEs and digital trade [6,17,22,28]. The Likert scale of 1 to 5 is suggested to assess respondents' agreement with each statement.

Cybersecurity Assessment Indicators

The dimension of cybersecurity assessment measures the effectiveness of SMEs to defend their information systems, business data, digital transactions and technological resources from cybersecurity threats. Cybersecurity is crucial in digital modernization, as SMEs rely more and more on online systems, cloud-based services, electronic payment and communication.

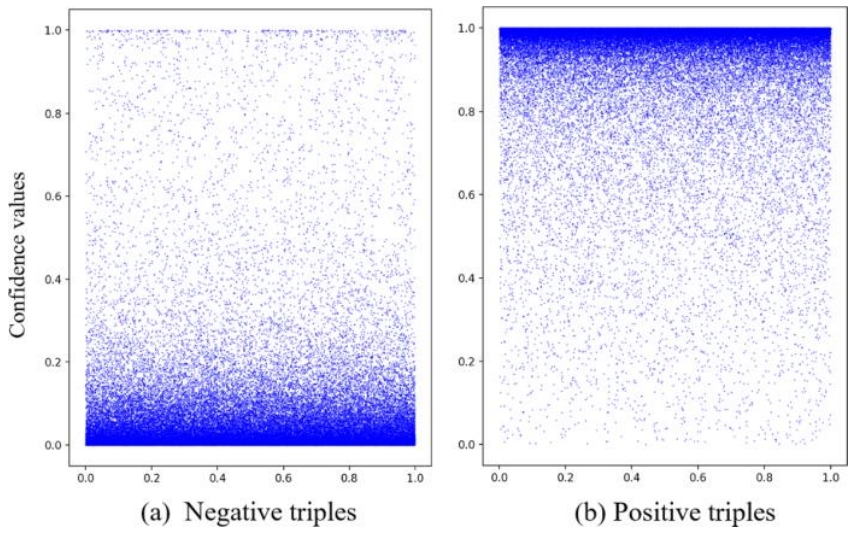

Fig 3.1 Cybersecurity Assessment Indicators

The assessment indicators are developed with reference to information security management principles in ISO/IEC 27001:2022 [16] and the NIST Cybersecurity Framework 2.0 [26]. Indicators are based on organizational policies, technical safeguards, employee awareness, risk management and incident response.

Table 3.3: Cybersecurity Assessment Indicators

Indicator	Assessment focus
Cybersecurity policies	Availability of documented security policies
Access control	Use of passwords, authentication, and user permissions
Data protection	Protection of confidential business and customer information
Network security	Security of organizational networks and connected devices
Employee awareness	Staff knowledge of phishing, malware, and online threats
Risk assessment	Regular identification and evaluation of cyber risks
Incident response	Procedures for responding to cybersecurity incidents
Software updates	Regular updating and patching of systems
Data backup security	Secure storage and protection of backup data
Third-party security	Assessment of risks from suppliers and external service providers

The evaluation of each indicator is based on the statements in the questionnaire. A cybersecurity policy, for instance, could be among the questions asked, as could whether access to sensitive information is limited and/or whether employees are aware of cybersecurity training.
The outcome is to establish strengths and weaknesses in the cybersecurity practices of the SMEs involved. The assessment is not intended to be a technical security audit, but rather an organizational-level assessment of cybersecurity preparedness.

Business Continuity Assessment Indicators
The dimension of business continuity assessment is the ability of SMEs to continue the activities of business operation during unexpected events and resume normal operation within an acceptable time frame. This disruption can happen when the system is hacked, equipment fails, a power outage occurs, a natural disaster strikes, a problem with the supply chain arises, or other issues occur.
BCM is a significant part of organisational resilience. The ISO 22301:2019 [15] offers a well-known standard for developing, implementing, maintaining and enhancing a business continuity management system. This guidance is used in the proposed TRDM methodology to create indicators for SMEs.
Evaluation of whether a SME has documented procedures for responding to disruptions and whether important business functions can continue in the event of an unexpected disruption. Special attention is placed on disaster recovery, backup procedures, contingency of operations, and continuity planning.
The results will assist in deciding if an SME has sufficient measures in place to safeguard its critical operations. They also pinpoint areas that can be improved in order to strengthen the resilience of the organisation and minimise the effects of operational disruptions.

Export Readiness Assessment Indicators
Export readiness assessment dimension measures SMEs' capacity to leverage digital technologies and organizational assets to engage in international markets. The term 'export readiness' is more than just being able to produce products or services. It also needs to have a suitable digital infrastructure, international customer communication, secure payment arrangements, understanding of export regulations, and effective ordering procedures.

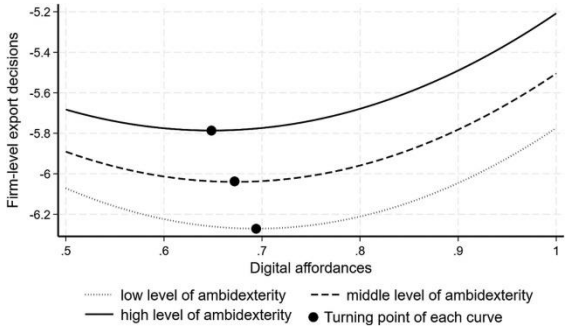

Fig 3.2 Export Readiness Assessment Indicators

Digital technologies can assist the SMEs in reaching foreign customers, marketing their products and services, conducting transactions, and organizing activities related to international business. But, there is a lack of technological proficiency, financial constraints, regulatory uncertainty, online security concerns etc. which could limit their access to global markets [6, 17, 22].

The indicators are assessed by the responses to the statements in the questionnaire, which focuses on the current export-related capacity of SMEs. Respondents can be asked if their organization has a professional business website, if it accepts digital payments from overseas customers, if it knows about the relevant export documentation, and if it uses digital tools to communicate with foreign customers, for instance. The evaluation also takes into account SMEs, which are not yet exporting but have the potential to do so. This is crucial as the TRDM methodology features to identify current capabilities and areas that need improvement before international expansion.

RESULTS AND DISCUSSION

This chapter provides the findings and discussions of the proposed small and medium sized enterprises (SMEs) Trade-Ready Digital Modernization (TRDM) Methodology. The chapter highlights the assessment of three key aspects of digital modernization, namely on the cybersecurity readiness, on the business continuity capability and on the digital export readiness.

This chapter aims to analyze the preparedness of SMEs for the adoption of digital technologies, the protection of organizational information, continuity of business operations in the face of unforeseen disruptions and involvement in international digital trade. The relationships between these dimensions and their total contribution to the overall digital preparedness for modernization are also taken into account.

Proposed assessment includes answers to the questions on the questionnaire, descriptive statistics and appropriate analytical methods. The three TRDM dimensions are individually explored and then combined for a comprehensive evaluation. This helps to determine the strengths, weaknesses and improvement needs of SMEs.

The discussion is grounded in theoretical concepts and previous research discussed in Chapter 2. Digital transformation can enhance the competitiveness of the organization, but for its proper implementation, it is necessary to have the necessary technology skills, security and management support [5, 20]. Similarly, business continuity and export readiness are important for developing resilient and internationally competitive SMEs [1, 6].

Demographic and Organizational Characteristics of SMEs

This background information is important for understanding their digital modernization capabilities: the demographic and organizational characteristics of the participating SMEs. Adoption of cybersecurity practices and business continuity arrangements could be impacted by business sector, organizational size, years in business, employee size, and how digital technologies are used.

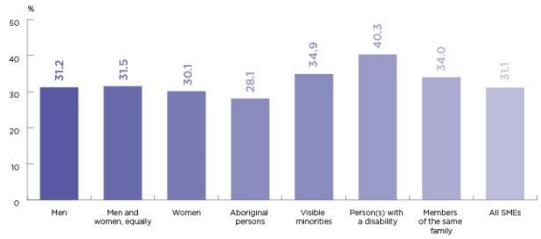

Fig 4.1 Demographic and Organizational Characteristics of SMEs

The study is designed for SMEs in a variety of industry sectors, such as manufacturing, retail, information technology, professional services and wholesale. A range of sectors is included to give a more comprehensive picture of digital modernization challenges.
The table below shows an example of the distribution of all SMEs participating. These are illustrative numbers and not necessarily reflective of the actual survey results.

Table 4.1: Illustrative Distribution of SMEs by Business Sector

Business sector	Number of SMEs	Percentage
Manufacturing	30	30%
Retail and wholesale	25	25%
Information technology	20	20%
Professional services	15	15%
Other services	10	10%
Total	**100**	**100%**

The illustrative distribution depicts companies across a variety of industries. In addition to service-based companies, the manufacturing and retail sectors are covered. The digital challenges are not the same across all sectors, due to varying operational processes, customer needs and technology needs.

Table 4.2: Illustrative Distribution According to Organizational Size

Organizational category	Number of SMEs	Percentage
Micro enterprises	20	20%
Small enterprises	45	45%
Medium enterprises	35	35%
Total	**100**	**100%**

The classification by organizational size allows for an analysis of whether capacities for digital modernization vary based on the resources and capacities of companies. Small businesses might have trouble budgeting and deploying financial and technical resources for cybersecurity systems, business continuity planning, and global market expansion. The management structures in medium sized enterprises may be better defined, but they can also lack expertise and investment in digital.

Table 4.3: Illustrative Distribution According to Digital Technology Usage

Digital technology usage	Number of SMEs	Percentage
Basic digital tools	25	25%
Moderate digital systems	40	40%
Advanced digital systems	25	25%
Limited digital technology	10	10%
Total	**100**	**100%**

The table below shows that the uptake of digital technology can differ between SMEs. Advanced digital systems could offer more opportunities for automated processes, customer data management and global market access for organisations. But the implementation of technology isn't enough to make organizations ready. It must be protected by cyber security measures, continuity measures and suitable management procedures.

Assessment of SME Cybersecurity Preparedness

The first important pillar of the TRDM methodology is cybersecurity preparedness. It assesses the capabilities of SMEs to safeguard their digital systems, business information, customer records and online transactions from cybersecurity threats.

The assessment takes into account security policies, access control, data protection, employee awareness, risk assessment, incident response, and backup security. The indicators are created based on ISO/IEC 27001:2022 [16] and the NIST Cybersecurity Framework 2.0 [26].

Table 4.4: Illustrative Cybersecurity Preparedness Assessment

Cybersecurity indicator	Illustrative mean score
Cybersecurity policies	3.20
Access control	3.45
Data protection	3.10
Network security	3.25
Employee awareness	2.85
Risk assessment	2.70
Incident response	2.60
Software updates	3.50
Data backup security	3.30
Third-party security	2.65
Overall mean	**3.06**

The illustrative results show that software updates and access control are relatively more important, whereas incident response, third-party security and formal risk assessment are relatively less important. The pattern might imply that SMEs might be more adept at simple technical security measures than in structured cybersecurity management.



Fig 4.2 Illustrative Cybersecurity Preparedness Assessment

The lower illustrative score for incident response reinforces the need for having procedures in place to identify, report, and manage cyber security incidents, that are clear. Likewise, employee awareness is crucial as it can make organisations vulnerable to security threats, through phishing attacks, weak passwords, and unsafe digital practices. Cybersecurity preparedness should therefore include not only technological solutions, but also organizational solutions. The previous studies and international guidelines highlight the importance of an ongoing process of information security risk assessment,

controls and management involvement [11, 16, 26]. In general, in the TRDM approach, cybersecurity is not just a technical necessity, but a core organizational capability to facilitate secure digital operations and international business activities.

Evaluation of Business Continuity Capabilities

The second dimension of TRDM is business continuity. It assesses if the SME is able to continue essential operations during unexpected disruptions and then resume to normal operations following an incident.

The assessment is completed on business impact analysis, identification of risk, continuity planning, disaster recovery, data backup, disaster response, and recovery objectives. These indicators are derived from the ISO 22301:2019 [15] and related research in the field of organisational resilience [1, 8].

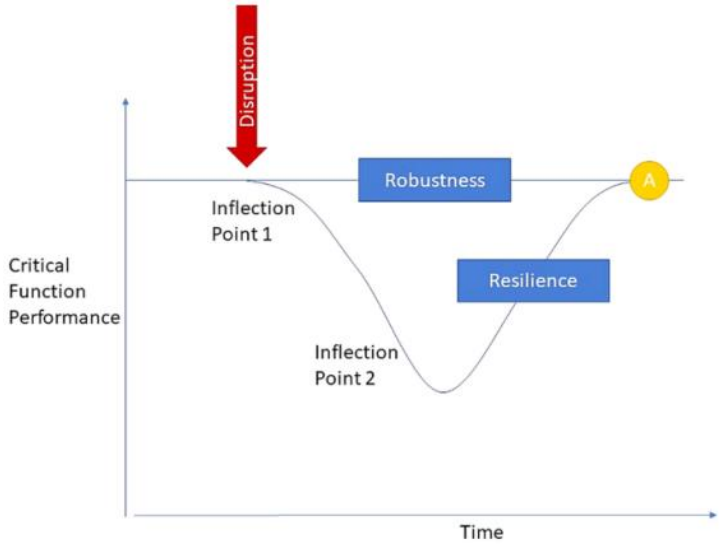

Fig 4.3 Evaluation of Business Continuity Capabilities

Table 5.5: Illustrative Business Continuity Assessment

Business continuity indicator	Illustrative mean score
Business impact analysis	2.80
Risk identification	3.00
Continuity planning	2.65
Disaster recovery	2.75
Data backup	3.55
Emergency response	2.90
Recovery objectives	2.50
Supply-chain continuity	2.85
Employee preparedness	2.95
Continuity plan testing	2.40
Overall mean	**2.84**

The illustrative results suggest that data backup might be a relatively well established practice among SMEs, and formal continuity plan testing and recovery goals might have lower scores. This implies that organisations do not need to have an extensive business continuity management system but can have basic back-ups.

The lower illustrative score for continuity plan testing emphasizes the need to regularly review the feasibility and effectiveness of recovery measures. SMEs need to be aware of their critical business activities, establish responsibilities, develop alternative operating procedures and decide on recovery time.

BCP is of special significance to businesses which rely on digital platforms, electronic transactions, customer online services, and external suppliers. A disruption in these activities can impact productivity, customer trust and financial bottom line.

In its methodology, the TRDM approach therefore considers business continuity a key theme of digital modernization. A digitally advanced SME could still fall vulnerable if it is not able to maintain or resume essential services in the event of unforeseen disruption.

Assessment of Digital Export Readiness

Digital export readiness is the third dimension of the TRDM methodology. It looks at the capacity of SMEs to access, operate and engage in international markets with the required digital technologies and organizational resources.

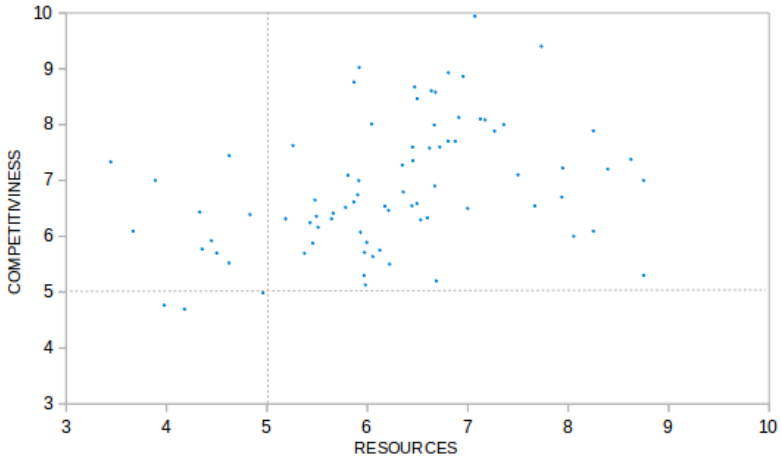

Fig 4.4 Assessment of Digital Export Readiness

Table 5.6: Illustrative Digital Export Readiness Assessment

Export readiness indicator	Illustrative mean score
Digital infrastructure	3.60
E-commerce capabilities	3.20
Digital marketing	3.50
International payments	2.85
Export documentation	2.75
Regulatory awareness	2.60
International customer management	3.10
Digital order management	3.00
Logistics coordination	2.70
International market knowledge	2.80
Overall mean	**3.01**

Assessment involves the digital infrastructure, ecommerce, digital marketing, international payment, export documentation, regulatory awareness, customer management and logistics coordination. These are indicative of the relevance of digital skills for the internationalization and export activities of SMEs [6, 17, 22].

The illustrative results imply that digital infrastructure and digital marketing are relatively more developed areas, while regulatory awareness, logistics coordination and international payment arrangement are relatively less developed areas for improvement.

An SME can have professional website, have social media accounts, but not know how to manage international orders, payments, shipping and export documentation, not to mention all the systems. This shows that having a digital presence isn't enough for export readiness.

Financial constraints, lack of market information, regulatory complexity, and lack of organizational capability have been found to be significant challenges to internationalization of SMEs [6, 22]. The TRDM methodology addresses these issues by incorporating various export indicators, technological as well as business.

SMEs have to build a solid digital infrastructure, master international trade needs, arrange suitable payment methods, and communicate with foreign customers to become export ready.

Integrated Evaluation Through the TRDM Methodology

The integrated evaluation reflects the three aspects of the proposed TRDM methodology: cybersecurity preparedness, business continuity capabilities and digital export readiness. The goal is not to have an in-depth look at the various capabilities but to have a holistic view of digital modernization of SMEs.

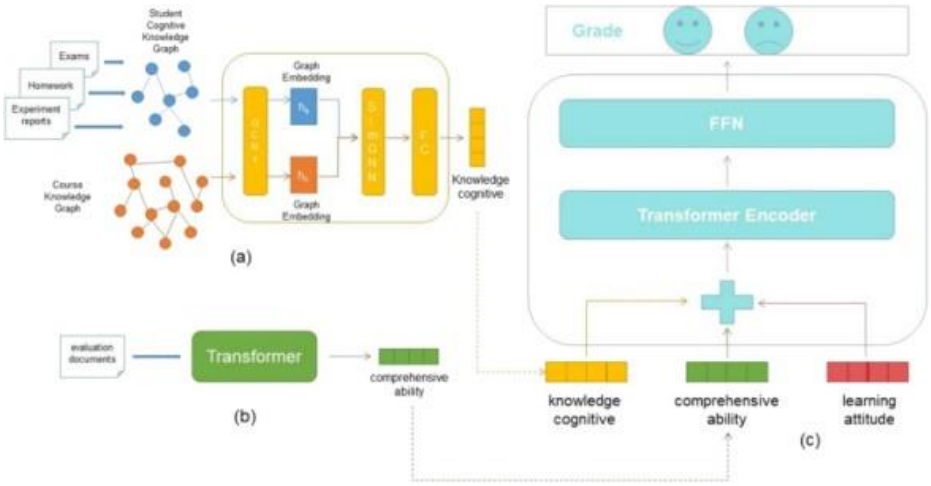

Fig 4.5 Integrated Evaluation Through the TRDM Methodology

The mean scores for the three dimensions are used for the evaluation. Equal weighting is being suggested to calculate the overall TRDM score in an initial model.

This score is the mean divided by the maximum possible score (5) and multiplied by 100 to give a percentage. This is a normalized questionnaire score and not the percentage of SMEs that are fully prepared.

The illustrative assessment shows that the highest score is for cybersecurity preparedness, followed by digital export readiness, and digital business continuity has the lowest score. This trend implies that SMEs need to be more focused on continuity planning, recovery plans and frequent testing.

Table 5.7: Illustrative Integrated TRDM Assessment

Assessment dimension	Mean score	Percentage of maximum score
Cybersecurity preparedness	3.06	61.2%
Business continuity	2.84	56.8%
Digital export readiness	3.01	60.2%
Overall TRDM score	**2.97**	**59.4**%

The TRDM methodology can also assign proposed maturity levels to organizations.

The overall score is an example of 2.97 which would indicate the organisation is at Level 3: Established. This classification is a suggested classification of the TRDM methodology and must be reviewed, tested and validated in practice by experts before it can be regarded as a maturity classification standard.

Table 5.8: Proposed TRDM Digital Modernization Maturity Levels

Mean score	Maturity level	Interpretation
1.00–1.80	Level 1: Initial	Very limited preparedness
1.81–2.60	Level 2: Developing	Basic practices are emerging
2.61–3.40	Level 3: Established	Moderate organizational preparedness
3.41–4.20	Level 4: Advanced	Strong and organized capabilities
4.21–5.00	Level 5: Optimized	Highly developed and continuously improved capabilities

The integrated evaluation highlights the need for an integrated assessment of cybersecurity, continuity and export readiness. Improving in one area does not necessarily make up for a failing in another. An SME with strong cybersecurity measures in place could still have significant operational issues if it didn't have a continuity plan.

Relationship Between Cybersecurity and Business Continuity

Cybersecurity and business continuity are interconnected as cyber security incidents can have an impact on business activities and performance. The consequences of a cyber-attack can include data breaches, downtime, unauthorized access, financial loss, and loss of customer service.

Table 5.9: Proposed Relationship Between Cybersecurity and Business Continuity

Cybersecurity capability	Related continuity capability	Expected contribution
Data protection	Secure data recovery	Reduces the impact of data loss
Access control	Operational system availability	Limits unauthorized system disruption
Risk assessment	Business impact analysis	Improves identification of organizational threats
Incident response	Emergency response planning	Supports coordinated incident management
Secure backups	Disaster recovery	Helps restore critical information
Employee awareness	Employee emergency preparedness	Improves staff response to disruptions

The implementation of cybersecurity controls reduces the probability and severity of a security incident, and implementations of business continuity planning helps to ensure that an organization's critical operations continue or are restored in the event of disruption. Thus, both dimensions have an impact on organizational resilience.

In this regard, ISO/IEC 27001:2022 [16] gives guidance for managing information security risks, while ISO 22301:2019 [15] is concerned with how businesses must continue to function in the event of a disruption. They complement each other, making it possible to combine cybersecurity and continuity planning in the TRDM methodology.

The correlation indicates that as the preparedness to cyber security increases, the business continuity preparedness should rise too. For instance, if there is a disruption and secure data backups are not readily recoverable, they are not useful. Ensuring incident response procedures are aligned with business recovery responsibilities is also similar.

The proposed framework thus assumes that improved cyber security capabilities and arrangements can be used to bolster business continuity arrangements. This correlation, however, needs to be tested using information from the actual surveys to determine its strength and statistical significance.

To test the association between the cybersecurity and the business continuity scores, correlation analysis can be performed. The regression analysis can also be used to determine if there is a significant difference in business continuity capabilities after controlling for the relevant organizational factors regarding cybersecurity preparedness.

Relationship between Digital Modernisation and Export Readiness

Digital modernization can enhance SMEs' capacity for global markets to facilitate online communication, electronic transactions, digital marketing, customer relationship management, and automation of business processes.

But internationalisation is not achieved simply through the use of digital technologies. SMEs require a secure system, reliable operations, knowledge about export regulations, appropriate payment terms, and efficient logistics management as well. Technological capabilities can then be matched with the proper organizational practices in the context of digital modernization and in this way contribute to export readiness.

The importance of digital competences for enhancing SME competitiveness and internationalization has been also underlined in previous studies [6, 20, 23]. Digital platforms can help overcome communication challenges and access international customers, and cybersecurity and continuity plans helps build trust and ensure reliability of operations.

The relationship shows that SMEs obtain important capabilities to enter international markets related to digital modernization. Customer confidence and secure transactions are the advantages of cybersecurity, whereas business continuity ensures uninterrupted operations and customer expectations are met.

The export readiness dimension also shows that international market participation is related to organizational knowledge and management skills. SMEs need to be aware of the needs of end-users and to create appropriate arrangements for international users, payments, documentation and logistics.

In the TRDM methodology, digital modernization is thus seen as a holistic process in which the different aspects of technological preparedness, operational resilience and export ability complement each other. The correlation and regression analysis can be carried out to examine the relationship between the relationship variables empirically, in which the data of the participating SMEs is used.

CONCLUSION AND RECOMMENDATIONS

This research aimed to build the integrated assessment framework for developing the Trade-Ready Digital Modernization (TRDM) Methodology to assess the digital modernization capacity of small and medium-sized enterprises (SMEs). The study took a look at the necessity of integrating cybersecurity readiness, business continuity management and digital export readiness in a single assessment approach. The research came from the recognition of the role of digital technologies in the modern business environment. To boost productivity and connect with customers, SMEs have increasingly relied on digital platforms, online transactions, cloud based systems and electronic communication. However, successful digital transformation requires more than adopting new technologies. In addition, organizations need to safeguard their digital assets, keep their operations running in case of unforeseen events, and build the skills necessary for engaging in global markets.

The study analysed the literature and international standards concerning the issues of digital transformation, cyber security, organizational resilience, business continuity and SME internationalization. Guidance for the creation of the assessment dimensions was provided by important frameworks such as ISO/IEC 27001:2022 [16] and ISO 22301:2019 [15] as well as the NIST Cybersecurity Framework 2.0 [26].

The proposed TRDM methodology incorporates three key aspects

Cybersecurity Preparedness: Assesses SMEs' capacity to safeguard information systems, business data, networks, and digital transactions.

Business Continuity Capabilities: Assesses SMEs' ability to run key business operations and bounce back from unexpected interruptions.

Digital Export Readiness: Indicates SMEs capacity to engage in international markets with digital technologies and organisational resources.

The proposed research method was a mixed method, which involved questionnaires, interviews, literature analysis and statistical analysis. The goal of the overall project was to create a structured evaluation procedure, which assists SMEs to identify their weak elements, assess their current skills and priorities for digital modernization.

Major Findings

The key results of this study are presented within the framework of the three dimensions of the proposed TRDM methodology and their relationships.

Cybersecurity Preparedness

Cyber security is recognized as an integral part of a framework for research on sustainable digital modernization. The right security policies, access controls, data protection, employee awareness, risk assessment and incident response plans are essential to SMEs. An organized security management approach is required with basic technical practices to ensure that the site is protected.

Business Continuity Capabilities

Business continuity is recognized as one of the critical elements to ensure organizational resilience. SMEs need to have a business impact analysis, a documented continuity plan, secure backups, disaster recovery plan, emergency responsibilities and regular testing. The proposed framework highlights the need for organizations to be ready for disruptions rather than relying solely on reactive responses.

Digital Export Readiness

The study highlights digital export readiness as one of the key capabilities to boost SME competitiveness and export to the international markets. Important aspects of this dimension include digital infrastructure, e-commerce platforms, international payment systems, digital marketing, export documentation, regulatory knowledge, and customer management.

The integration of the Three Dimensions

The proposed TRDM methodology highlights the need for a holistic assessment of cybersecurity, business continuity and export readiness. The dimensions are interlinked since secure digital operations contribute to customer confidence, the continuity arrangements enhance service reliability and export capabilities open up opportunities for the international development of business.

Overall Assessment

This framework offers a suggested maturity level-based evaluation of the preparedness for digital modernization of SMEs. It can assist organizations in determining the level they are at and prioritizing areas for improvement. But the efficacy and the statistical relations between the proposed framework must be validated by applying real empirical data.

Conclusion

Digital transformation of SMEs has taken on more significance than ever, both in terms of competitiveness and operational efficiency and in order to be able to participate in international markets. However, digital modernization can not be achieved by simply adopting technology. Organizations must also be prepared against cyber threats and have business continuity capabilities, as well as ability to do digital business across borders.

This research introduces a methodology called the Trade-Ready Digital Modernization (TRDM) Methodology that can be employed to meet these requirements. TRDM is different from methods that focus on cybersecurity, business continuity and export readiness in isolation, as it integrates them into a single assessment framework.

The methodology proposed is systematic to analyse the organizational capabilities, their weaknesses and set a prioritisation for the improvement. It also acknowledges that SMEs have different financial, technological and managerial circumstances. Thus, the evaluation can provide insight into the

organizations current abilities and action plans for enhancement based on resources and business needs.

One of the key strengths of the proposed framework is its emphasis on the interlinkage between digital security, OP resilience, and preparedness for international business. Cybersecurity contributes to safeguarding digital resources, business continuity contributes to maintaining essential business operations and export readiness contributes to the use of digital technologies for market participation in the international market for SMEs.

The TRDM methodology provides a proposed integrated framework to support SME digital modernization as a conclusion. Its practical value will hinge on the appropriate implementation, evaluation by experts, and empirical testing by various business sectors in different organizational contexts.

Theoretical Contributions

The proposed research adds to the body of knowledge on SME digital transformation by combining three key organizational capabilities into a single assessment methodology.

First, the study is a development of the application of the Resource Based View (RBV) theory, which says that the organization's resources and capabilities can lead to competitive advantage [4]. In the TRDM methodology, cybersecurity systems, digital infrastructure, continuity arrangements and export-related capabilities are identified as important organizational resources that can be used to increase the competitiveness of SMEs.

Secondly, the framework is linked to Dynamic Capabilities Theory, which focuses on the capacity of organizations to reconfigure, develop and adapt their resources to various business environments [35]. The TRDM methodology embodies this attitude, where SMEs are continuously evaluating their capacity and looking into new risks while enhancing their digital processes.

Thirdly, the research brings together the concepts of cybersecurity preparedness to BCM in the literature on organizational resilience. The dimensions are usually talked separately, but the approach here is to acknowledge that there is a deep connection between information security and operational recovery.

Fourthly, the framework links digital transformation to the internationalization of SMEs. It views digital technologies as assisting the businesses themselves and not just for improving internal processes, but also as tools that can help with the management of international customers, online transactions and export development.

Finally, the research suggests an integrated assessment structure based on the organization's security, operational resilience and international trade aspects. This lays the conceptual groundwork for comprehensive research on the impact of those dimensions on SME digital modernization.

Practical and managerial implications

There are some practical implications for SME owners, managers, IT professionals and business development staff in the implementation of the proposed TRDM methodology.

For SME Owners and Senior Management

The framework offers a comprehensive tool to grasp the issues of an organization and to prioritize digital modernization. The three dimensions of assessment can be used by managers to determine if their organization has the necessary security controls, continuity arrangements and export-related capabilities.

For IT Managers and Cybersecurity Professionals

Cyber security aspect emphasizes the need for policies, access control, data security, employee training and reporting. These factors can help IT professionals identify vulnerabilities and create viable security enhancement plans.

For Operations Managers
The business continuity dimension stimulates managers to identify critical business activities, evaluate risks to operations, develop recovery plans, and regularly test continuity plans. These practices helps to minimize impact of disruptions when they happen unexpectedly.

For Export & Business Development Managers
This export readiness dimension is useful for managers to assess how ready their digital marketing, e-commerce, payments, export documents, and international customer management are for export. This can contribute to international business activities preparation.

For Business Consultants
The TRDM framework can also be used as a preliminary evaluation instrument for consultants that work with SMEs. It can assist them in detecting organizational weaknesses and can suggest the methods to enhance it according to the requirement of every business.

Recommendations for SMEs
The following recommendations are proposed for SMEs wanting to enhance digital modernization capabilities based on the TRDM methodology proposed.

Create Cybersecurity Policies: SMEs should have clear policies in place for data protection, access control, password management, network security, and acceptable technology use.

Provide Regular Employee Training: Ensure employees get updated training on phishing, malware, suspicious links, data protection, and safe online practices.
Perform periodic risk assessments: Organizations should periodically determine cyber security threats, operational risks and vulnerabilities in their digital infrastructure.

Develop Business Continuity Plans: SMEs should document plans to explain how essential business activities will continue in the event of a surprising event.

Improve Backup & Recovery Plans: Organize important data in a way that it is backed up regularly and safely stored. Recovery plans should be tested to support the recovery of information and systems when necessary.

Enhance Digital Infrastructure: SMEs should develop appropriate Digital Infrastructure including Internet connectivity, software products, secure cloud services, and digital business systems based on the needs of their operations.

Implement E-Commerce Facilities: Organizations ought to consider appropriate ecommerce platforms and online sales channels to access customers beyond their local markets.

Build International Trade Knowledge: SMEs interested in export should enhance their knowledge of export documentation, international payment systems, customs and market regulations.

Enhance Digital Customer Management: Organisations should leverage the right digital tools to address their international customers' needs, order management and respond to customer needs.

Policy Recommendations
It is important that the government, regulatory authorities, business associations and SME development institutions provide support for the digital modernization of SMEs.

The following policy suggestions are made

Establish SME Cybersecurity Support Programs

Government institutions should offer technical support, awareness programmes and practical cybersecurity advice to SMEs, at affordable prices. Small businesses, which traditionally don't have the same depth of IT and security expertise, should be a special focus.

Promote Affordable Digital Infrastructure

Policies should promote the use of cloud computing, technology in SMEs, especially in remote areas, digital payment systems and affordable internet connectivity.

Foster Business Continuity Awareness

Business continuity planning and disaster recovery training, risk management training, and organizational resilience training should be made available to SME development authorities and business associations.

Enhance Digital Export Training

Export promotion organizations should conduct training sessions on subjects such as, ecommerce, international digital marketing, export documentation, international payment arrangements and international customer management.

Encourage Public-Private Partnerships

Governments need to support SMEs with technical assistance and digital modernization services by working with technology firms, universities, cybersecurity experts and business associations.

Create SME Digital Assessment Programs

Voluntary digital readiness assessment programmes based on internationally recognised standards could be introduced by relevant institutions. The suggested TRDM methodology could be tested as one of the possible assessment methods following further validation.

The recommendations can contribute to creating a conducive environment for the implementation of digital technologies by SMEs and their enhancement of security, resilience and competitiveness on the international market.

Suggestions for Future Research

The proposed TRDM methodology can be further developed and extended by empirical validation, sector-specific applications, and development of the assessment indicators in future research. future research should be conducted with a larger number of SMEs to assess the reliability, validity and application of the TRDM model. The researchers can compare the digital modernization of SMEs from different countries to understand the difference in their cybersecurity readiness, business continuity and export readiness. The framework can be industry specific, with separate industry tests undertaken to find industry-specific requirements. Future research may lead to the development of a software-based TRDM assessment tool which can enable SMEs to assess their capabilities and generate improvement recommendations. Structural equation modelling and other appropriate statistical methods can be employed to investigate the relationships between Cybersecurity, Business Continuity, Digital Modernization and Export Performance. Future researchers could investigate variations in SME capabilities over time after the deployment of cybersecurity controls, continuity plans, and strategies for digital exports. Further research could explore the relationship between the implementation of TRDM and factors such as financial resources, employee digital skills, management commitment and organizational size. Future iterations of the framework could explore the application of AI to help with cybersecurity monitoring functions, risk identification, business continuity planning and digital export operations. In general, further studies should seek to validate the proposed model in real organizational contexts and provide empirical evidence for the development of the evaluation system. The

developments can contribute to reinforcing the TRDM methodology and build its value as an integrated approach to SME digital modernization.

REFERENCES

Ali, Q. S. A., Hanafiah, M. H., & Mogindol, S. H. (2023). A systematic literature review of business continuity management (BCM) practices and the integration of organisational resilience and performance in small and medium enterprises (SMEs) BCM framework. International Journal of Disaster Risk Reduction, 99, 104135. https://doi.org/10.1016/j.ijdrr.2023.104135

Alford, P., & Page, S. J. (2015). Marketing technology for adoption by small business. The Service Industries Journal, 35(11–12), 655–669.

Autio, E., Nambisan, S., Thomas, L. D. W., & Wright, M. (2018). Digital affordances, spatial affordances and the emergence of entrepreneurial ecosystems. Strategic Entrepreneurship Journal, 12(1), 72–95.

Barney, J. (1991). Resources of a firm and sustainable competitive advantages. Journal of Management, 17(1), 99–120.

Bharadwaj, A., El Sawy, O. A., Pavlou, P. A., & Venkatraman, N. (2013). Digital business strategy: the next generation of insights. MIS Quarterly, 37(2), 471–482.

The information above was obtained from: 6. Calheiros-Lobo, N., Ferreira, J. V., & Au-Yong-Oliveira, M. (2023). SME Internationalization and export performance – A systematic review and bibliometric analysis. Sustainability, 15(11), 8473. https://doi.org/10.3390/su15118473

De Matteis, J., Elia, G., & Del Vecchio, P. (2023). Business continuity management and organizational resilience from a small and medium enterprises (SMEs) point of view. Journal of Contingencies and Crisis Management, 31(4), 670–682. https://doi.org/10.1111/1468-5973.12470

Duchek, S. (2020). Organizational Resilience: A conceptualization in terms of capability. Business Research, 13, 215–246.

Etemad, H. (2004). A grounded theoretical framework for internationalization of small and medium sized enterprises and an overview. Canadian Journal of Administrative Sciences 21(1): 1-21.

European Commission. (2020). An SME strategy for a sustainable and digital Europe. The European Union's Publishing Office.

European Union Agency for Cybersecurity. (2021). Small and medium enterprises (SMEs) – Cyber security challenges and recommendations. ENISA.

Freeman, J., & Styles, C. (2014). Is there a location effect on export performance? International Marketing Review, 31(2), 181–208.

Gaffar, H. S., & Őri, D. (2024). Towards SMEs digital transformation success: A systematic literature review. Information Systems and e-Business Management, 22, 667–719.

International Organization for Standardization. (2018). Risk management – Guidelines (ISO Standard No. 31000:2018). ISO.

Standardization is the 15th of the International Organization for Standardization. (2019). Security and resilience – Business continuity management systems – Requirements (IS0 Standard No. 22301:2019). ISO.

The international organization for standardization. (2022). Information security, cybersecurity and privacy protection – Information security management systems – Requirements (ISO Standard No. 27001:2022). ISO.

International Trade Centre. (2018). SME competitiveness outlook 2018: Business ecosystems for the digital age. ITC.

International Trade Centre. (2021). SME competitiveness outlook 2021: Empowering the green recovery. ITC.

International Trade Centre. (2023). SME competitiveness outlook 2023: Small businesses in fragile and conflict-affected settings. ITC.

Khin, S., & Ho, T. C. F. (2019). Digital technology, digital capability and organizational performance: Digital innovation as the mediator. The International Journal of Innovation Science 11(2) 177-195.

Knight, G. A., & Cavusgil, S. T. (2004). Innovation, born global firm and organizational abilities. Journal of International Business Studies, 35, p. 124-141.

Leonidou, L. C. (2004). Identification and analysis of impediments to export development of small enterprises. Journal of Small Business Management, 42(3), 279-302.

Matarazzo, M., Penco, L., Profumo, G., & Quaglia, R. (2021). The Digital transformation and the creation of customer value in Made in Italy SMEs: a dynamic capabilities approach. Journal of Business Research, 123, 642–656.

National Institute of Standards and Technology. (2010). A NIST Special Publication titled Contingency planning guide for federal information systems provides guidance on how to plan for contingencies when working with federal information systems. This booklet was compiled from data gathered by the U.S. Department of Commerce.

National Institute of Standards and Technology. (2020). The NIST Special Publication 800-53 Revision 5 is a government publication that contains security and privacy controls for information systems and organizations. The U.S. Department of Commerce.

National Institute of Standards and Technology. (2024). The NIST cybersecurity framework (CSF) 2.0. U.S. Department of Commerce.

OECD. (2019). OECD SME and entrepreneurship outlook 2019. OECD Publishing.

OECD. (2021). Digitalization of SMEs. OECD Publishing.

OECD. (2023). OECD SME & entrepreneurship outlook 2023. OECD Publishing.

OECD. (2024). OECD SME and entrepreneurship outlook 2024. OECD Publishing.

Oliveira, T., Thomas, M., & Espadanal, M. (2014). Key factors in the adoption of cloud computing – manufacturing and services. Information & Management, 51(5), 497–510.

Roffia, P., & Dabić, M. (2024). The role of management control and integrated information systems for the resilience of SMEs. Review of Managerial Science, 18, 1353–1375.

Sagala, G. H., & Őri, D. (2025). A systematic literature review about the digital transformation strategy to be used to reach the goal of being resilient and antifragile of SMEs. Journal of Small Business & Entrepreneurship, 37(3), 495–524.

Scuotto, V., Santoro, G., Bresciani, S., & Del Giudice, M. (2017). Empirical analysis of SMEs shifting intra- and inter-organizational innovation processes towards digital business. Creativity and Innovation Management 26(3) 247-255.

Teece, D. J. (2007). The nature and micro foundations of (sustainable) enterprise performance - Explicating Dynamic Capabilities. Strategic Management Journal, 28(13), 1319–1350.

Tornatzky, L. G., & Fleischer, M. (1990). The processes of technological innovation. Lexington Books.

UNCTAD. (2021). Digital economy report 2021: Cross-border data flows and development: For whom the data flow. United Nations.

UNCTAD. (2024). The 2024 Digital economy report: Building an environmentally sustainable and inclusive digital future. United Nations.

Wagner, S. M. (2006). A company's reactions to insufficient suppliers and competitive advantage. Journal of Business Research, 59(6), 686–695.

World Bank. (2016). Featuring in the world development report 2016: Digital dividends. World Bank.

World Bank. (2021). World development report 2021: Data for better lives. World Bank.

World Trade Organization. (2018). World trade report 2018: The future of world trade: How digital technologies are transforming global commerce. WTO.

World Trade Organization. (2023). The World trade report 2023: Re-globalization for a secure, inclusive and sustainable future. WTO.

Yuwono, T., Suroso, A., & Novandari, W. (2024). A systematic literature review of information and communication technology in SMEs. Journal of Innovation and Entrepreneurship, 13, Article 31.

Bargoni, A., Ferraris, A., Vilamová, Š., & Wan Hussain, W. M. H. (2024). Digitalisation and internationalisation in SMEs: A systematic review and research agenda. Journal of Enterprise Information Management, 37(5), 1418–1457.