The Role of Digital Transformation in Enterprise Risk Management

Saif Alali Abbas Zghair[1], Dr. Sinda Ben Sedrine Doghri[2]

[1]University of Sfax, Faculty of Economics and Management of Sfax, Business Administration, saifalaliabbass@gmail.com
[2]Associate Professor, University of Tunis, Department of Human Resources, Management and Law, Sinda.doghri@gmail.com

Abstract

This research aims to study and evaluate the mutual impact between digital transformation and risk management in organizations. While digital transformation offers significant benefits in terms of increased efficiency and innovation, it also presents new challenges related to risk management. The main findings of the research indicate the following:

• Complexity of the risk landscape: Digital transformation leads to a more complex digital environment, increasing the types and number of risks faced by organizations, such as cyberattacks and data breaches.

• New opportunities for risk management: Conversely, digital technologies provide advanced tools such as artificial intelligence and big data analytics, enabling organizations to detect threats earlier and respond more effectively.

• Importance of digital culture: Building a strong digital culture within the organization, where all employees are aware of digital risks and how to address them, is crucial.

• Integration of technology and management: Organizations must integrate technology into their risk management strategies, considering human and organizational factors.

The research recommends the following Developing a comprehensive strategy: Organizations should develop a comprehensive strategy for digital risk management that covers all aspects, from technology to organizational culture.

Keywords: Digital transformation, risk management, organizations.

1. Introduction

Geopolitical tensions and the COVID-19 pandemic have destabilized global markets, causing significant disruptions to labor markets and supply chains. These events have forced companies to reprioritize their response to increasing regulatory requirements, particularly in the areas of risk management and compliance. As a result, pressures on supply chains, cybersecurity, and public safety have increased. This makes it imperative for companies to embrace digital transformation and risk management with urgency.

Enterprise risk management (ERM) has become a critical component of strategic planning and decision-making in a rapidly evolving business environment, as organizations navigate digital transformation. The complexity and scope of the risks they face are expanding, necessitating a more integrated, technology-driven approach to risk management. With its holistic view of enterprise risk, ERM is well positioned to address these challenges and transform them into opportunities. Abernethy, M.A.,Chua, W.F. ,1996))

The digital age has given rise to a new set of risks. Cybersecurity threats, digital privacy concerns, and technological disruptions are just a few examples of emerging risks that organizations must manage. These risks are not limited to the IT department; they have far-reaching implications for business continuity and operational resilience. (Farooq Rayees, 2019)

Business continuity involves maintaining essential functions during and after a disaster, ensuring that a company can continue to serve its customers, mitigate losses, and recover from operations quickly. Operational resilience is the ability of an organization to withstand, recover from, or adapt to a harmful event that could cause harm, destruction, or loss of the ability to perform mission-related functions while operating. (Elkington, 1997))

To ensure that organizations can successfully address the risks posed by digital technology, they must focus on both their business continuity and operational resilience. These two aspects are complementary and contribute to protecting the organization from various threats and ensuring its continuity (Dyllick, 2002).)

Digital transformation is a fundamental pillar in the contemporary business world, as it provides organizations with new tools and technologies to manage their operations more efficiently. Speaking of risk management, digital transformation plays a crucial role in this area. Despite the prevalence of the term digital transformation in technical circles, many business leaders do not fully realize the extent of the risks associated with large digital development projects. This neglect leads to high failure rates for digital transformation projects. Therefore, understanding the mechanisms of managing risks associated with digital transformation is a crucial factor in ensuring the success of these projects and achieving a rewarding return on investment (Dotson, 2016).

Our current research seeks to study the previous dimensions of digital transformation in enterprise risk management, to determine the extent of its impact and how to enhance the positive points of this transformation and avoid the threats resulting from it.

Research Problem

Digital transformation and risk management cannot be separated; they are two sides of the same coin. Digital transformation creates new risks, while at the same time providing new tools and methods to manage them. This research seeks to explore the complementary relationship between digital transformation and risk management, and how organizations can achieve a balance between leveraging digital technology and building their capacity to face emerging challenges, thus answering the following questions:

- What is the impact of digital transformation on the traditional risk management model in organizations?

- How can organizations leverage digital technology to enhance their ability to identify and address emerging risks?
- What are the best practices in risk management in a constantly changing digital environment?
- What are the challenges facing organizations in integrating risk management into digital transformation strategies?

Research Objectives

The current research seeks to achieve the following objectives:

Evaluating the impact of digital transformation on risk management:

- Evaluating the effectiveness of digital tools and technologies in detecting, assessing and managing risks.
- Comparing traditional risk management models with their digital models.

Analyzing challenges and opportunities:

- Identifying the challenges facing organizations in integrating risk management into digital transformation strategies.
- Exploring the opportunities provided by digital transformation to enhance organizations' resilience and ability to face risks.

Developing a Framework:

- Developing a comprehensive framework for risk management in a changing digital environment.
- Proposing a set of principles and guidelines for organizations to enhance their ability to manage digital risks.

Research Importance

The current research is of great importance in light of the rapid technological development that the world is witnessing. This research gains its importance from several aspects:

1- Protecting institutions:

- Reducing financial losses: The research helps identify the risks that threaten institutions and how to prevent them, which contributes to reducing the financial losses resulting from these risks.
- Protecting reputation: Helps maintain the reputation of the institution by effectively managing crises resulting from digital risks.

- Ensuring business continuity: Contributes to ensuring the continuity of the institution's business by building flexibility and the ability to adapt to the continuous changes in the digital environment.

2- Developing business strategies:

- Making informed decisions: The research provides the information necessary to make informed strategic decisions regarding investment in digital technologies and managing the risks associated with them.
- Improving performance: Helps improve the performance of institutions by identifying weaknesses and enhancing strengths.
- Innovation: Encourages innovation in the field of risk management by developing new tools and methods.

3- Developing scientific knowledge:

- Bridging knowledge gaps: Contributes to bridging knowledge gaps in the field of digital risk management.
- Building new theories: Helps build new theories about the relationship between digital transformation and risk management.
- Curriculum development: Provides valuable information for developing curricula in the field of business administration and information technology.

4- Policy making:

- Regulation development: Helps develop the necessary regulations and legislation to protect institutions from digital risks.
- Community awareness: Contributes to raising community awareness of the importance of cybersecurity and risk management.

2. Research Methodology

The current research adopts the descriptive analytical approach based on describing phenomena and events as they exist in reality, without the researcher intervening to change or control them. This approach relies on collecting data from various sources such as observation, interviews and questionnaires, and then analyzing this data to describe reality accurately.

First: Concept and Terminology

1- The concept of enterprise risk management:

Enterprise risk management (ERM) is a comprehensive system for managing the risks faced by the organization. These risks are diverse and include multiple aspects, ranging from employee safety and data protection to compliance with laws and combating fraud. These risks may be

caused by internal factors such as technical failures, or external factors such as natural disasters. It is worth noting that identifying risks varies according to the nature of each organization. (Donate, 2015).

It is a proactive process that aims to protect the organization from potential damage before it occurs. Instead of waiting for crises to occur, risk management works to identify and assess potential risks and take the necessary actions to reduce their impact. Each organization has a unique set of risks it faces, so the enterprise risk management framework provides a flexible framework that can be adapted to the needs of each organization. In this way, risk management helps organizations achieve their goals more sustainably. (Dent, 1990).

It is more than just protecting the organization from harm; it enables it to make the most of available opportunities. By identifying and assessing potential risks, an organization can make informed strategic decisions that enhance its performance and protect its investments. This approach complements business continuity management (BCM), where risk management helps identify threats that may disrupt operations and develop effective contingency plans to ensure business continuity and fulfill its obligations to all stakeholders. (Das, 1998)

2- Distinguishing between governance and risk management:

Governance, risk and compliance management (GRC) and enterprise risk management (ERM) are fundamental concepts in risk management. Although they are often used interchangeably, there are clear differences between the two. Darroch, 2003)

Daniel, E. (1999) asserts that GRC refers to a strategy for managing an organization's overall governance, managing enterprise risk and complying with regulatory systems. It involves coordinating strategy, processes, technology and people to promote effective decision-making and encourage a risk-aware culture. The four components of GRC consist of strategy, processes, technology and people. These elements work together to ensure that an organization's governance framework, strategic risk management plans and compliance protocols are practical and aligned with business objectives.

On the other hand, COSO, (2017) indicated that enterprise risk management (ERM) is a process driven by leaders, aimed at identifying potential events that may affect an entity and managing risks to be within the entity's risk appetite, to provide reasonable assurance about achieving the entity's objectives.

However, ERM often faces three major challenges according to (Cortiñas, M., Chocarro, R. and Villanueva, M. L.) (2010):

- Lack of integration across the organization
- Insufficient support from top management
- A reactive rather than proactive approach to risk management

These challenges can hinder the effectiveness of ERM and prevent organizations from realizing its full benefits.

The difference between them can be summarized in the following table:

Concept	Objective	Focus	Key Elements
Governance, Risk and Compliance Management	Ensure efficient, transparent and compliant operation	General framework for managing the organization	Strategy, Processes, Technology, People
Enterprise Risk Management	Protect the organization's objectives	Identifying and managing risks	Risk Identification, Risk Assessment, Risk Management

Second: The role of digital transformation in risk management

1. Improving the comprehensive view of risks:

Digital technologies enable the collection of huge amounts of data related to businesses and operations, which helps to identify potential risks early and accurately assess them. (Birasnav, M., 2013),

Data collection and analysis form the backbone of risk management in the digital age. Thanks to the tremendous advances in digital technologies, organizations have become able to collect huge and diverse amounts of data, ranging from internal transaction records to customer interactions on social media platforms. (Matarazzo, 2021)

Digital transformation has revolutionized the field of data collection, providing unprecedented opportunities to achieve deeper and more accurate insights into businesses, customers, and markets. Here are some of the key roles that digital transformation plays in developing data collection. Jafari-Sadeghi, 2021))

Data is no longer limited to traditional records, but has become available from countless sources such as sensors, social media sites, smartphone applications, and the Internet of Things. Digital technologies enable the collection of more accurate and detailed data, which leads to improving the quality of analyses. (Zhang, J. C.; Long, J. ;2021)

Automation has accelerated the process of collecting, storing, and processing data, saving time and effort. Data can be analyzed immediately after collection, allowing for faster and more responsive decisions to market changes. (An, T. L. ;2022).

These technologies help discover complex patterns and hidden trends in data, improving the accuracy of predictions and decision-making. Data can be used to anticipate future events and take proactive actions. (Zhai, H. Y. ;2022).

Digital technologies can also handle massive amounts of data, enabling more comprehensive analyses, allowing technologies such as text analysis and image analysis to be used to analyze new types of data. (Chi, M. M.; Wang, 2022)

The benefits of integrating data from different sources include creating a comprehensive picture of the business, as well as improving customer understanding: to provide a deeper understanding of customer needs and desires. (Chen, H.; Tian, 2022).

2. Enhancing Response Speed

2-1- Automation

Many routine tasks related to risk management can be automated, which speeds up the decision-making process and crisis response, as the idea of automating routine tasks related to risk management is a remarkable development in the field of business management. Expanding on explaining this idea requires diving into the mechanisms by which this automation works and how it contributes to improving the decision-making process and crisis response. (Wu, F.; Hu, H. Z.; Lin, 2021)

As for the mechanisms for automating routine tasks in risk management, this automation is based on a set of smart technologies and software that aim to:

 Identify risks: By analyzing big data and available information, automated systems can identify potential risks and classify them according to the level of importance and impact. (Pramanik, H. S.; 2019)

 Risk assessment: Using complex analytical models, risks are accurately and quantitatively assessed, which helps in setting priorities and allocating the necessary resources. (Chen, X. H.; Zhang, 2021)

 Developing response plans: Automated response plans are developed to deal with various possible scenarios, which speeds up the response process in the event of a crisis.

 Continuous monitoring: Risks are continuously monitored by automated systems, allowing for early detection of any changes or developments that may affect the level of risk. (Shang, H. T. ,2021)

As for the benefits of automating routine tasks in risk management, automation contributes to significantly accelerating the decision-making process, as automated systems can process huge amounts of data in a short time and provide accurate recommendations, and it also reduces the possibility of human errors in the risk assessment and decision-making process. (Ma, H. D. ;2022)

Automated systems can learn from historical data and improve their performance over time, leading to continuous improvement in the risk management process. (Pratono, A. H, 2018).

It also allows employees to focus on strategic tasks that require high human skills, such as creative thinking and complex problem solving. (Liu, X. X. ;2020)

Despite the great benefits provided by the automation of routine tasks in risk management, it faces some challenges, such as:

- Data quality: The accuracy of the results obtained by automated systems depends largely on the quality of the input data. (Tan, C. ;2020)
- Cost: The process of implementing automated systems may require significant financial investments.
- Cybersecurity: Automated systems must be protected from cyber-attacks that may affect the integrity of data and decision-making.

It can be said that the automation of routine tasks in risk management represents a qualitative leap in this field. It contributes to improving the efficiency of organizations and their ability to adapt to the continuous changes in the economic environment. However, this technology must be approached with caution and its benefits and challenges must be evaluated in an integrated manner.

2-2- Instant Communication:

Digital technologies facilitate instant communication between different parts of the organization, ensuring the rapid and effective exchange of information in the event of any threat. The idea of digital technologies facilitating instant communication between different parts of the organization is the cornerstone of building a strong defense system capable of confronting the various threats facing organizations in our current era. Expanding on explaining this idea requires diving into the mechanisms by which these technologies work and how they contribute to improving the process of exchanging information in the event of any threat. (Hajli, M.; Sim, J. M.; 2015)

As for the mechanisms of digital technologies in facilitating institutional communication, Farooq Rayees (2019) confirms that they rely on a wide range of tools and software that aim to:

 Create instant communication channels: Digital technologies provide a variety of channels for instant communication such as email, instant messaging, video conferencing, and collaborative collaboration applications, allowing employees to communicate with each other at any time and from anywhere.

- File and document exchange: Digital technologies facilitate the rapid and secure exchange of files and documents, allowing employees to access the information they need to make appropriate decisions in the event of any threat.

- Real-time collaboration: Digital technologies allow employees to collaborate in real time on projects and tasks, which speeds up the process of resolving problems and responding to threats.

- Creating shared dashboards: Organizations can create shared dashboards that display important data and information in real time, ensuring that all employees are aware of the latest developments.

Among the benefits of facilitating institutional communication with digital technologies in the face of threats according to (Donate, M. J. and Guadamillas, F.) (2015), are:

- Speed in decision-making: Digital technologies contribute to accelerating the process of exchanging information and reaching appropriate decisions in record time, which reduces the impact of threats on the organization.

- Access to accurate information: Digital technologies ensure that all employees have access to accurate and up-to-date information, which helps them make informed decisions.

- Effective collaboration: Digital technologies facilitate collaboration between different departments and employees, leading to increased efficiency and productivity.

- Rapid response to crises: Organizations can respond to crises faster and more effectively thanks to instant communication between different parts of the organization.

Matarazzo (2021) points out that despite the great benefits that digital technologies offer in facilitating corporate communication, they face some challenges,

- Information security: Sensitive information must be protected from hacks and cyber-attacks.
- Data quality: The accuracy and reliability of data exchanged between employees must be ensured.
- Training: Employees need to be trained to use digital technologies effectively.

It can be said that digital technologies play a vital role in enhancing the ability of organizations to confront various threats. They contribute to improving communication and collaboration between employees, accelerating the decision-making process, and responding quickly to crises. However, organizations must take into account the challenges associated with the use of these technologies and take the necessary measures to protect information and train employees.

3. Improving the Efficiency of RISK Management:

3-1- Integrated risk management systems:

Digital systems can provide a unified platform for managing all aspects of risks, from identifying and assessing them to developing response plans, as risk management systems provide an integrated framework that covers the entire risk management lifecycle. From the stage of identifying and classifying risks, through assessing their likelihood and impact, to developing comprehensive response plans, these systems contribute to improving the efficiency of decision-making processes and reducing the negative effects of potential risks. (Jafari-Sadeghi, 2021)

Unification and Consistency:

Digital systems collect risk-related data from multiple sources, ensuring the unification of information and avoiding inconsistencies. They also provide a consistent methodology for assessing risks, which facilitates comparing different risks and making informed decisions. (Zhang, 2021)

Advanced Analysis:

Digital systems provide users with advanced analytical tools, such as statistical analysis and modeling, to assess risks more accurately. These systems can use artificial intelligence and machine learning techniques to predict future risks and take preventive measures. (Hajli, M.; Sim, J. M.; 2015)

Institutional Integration:

Farooq Rayees (2019) confirms the interconnection of digital systems, risk management systems with other systems in the organization, such as project management systems and quality management systems, which ensures institutional integration, in addition to facilitating the

sharing of knowledge and expertise between different departments in the organization, which enhances the culture of risk management.

Rapid Response:

Digital systems can automatically activate response plans when a risk event occurs, which reduces response time, as they track and evaluate the effectiveness of response plans, which contributes to their continuous improvement. (Chi, M. M. ; Wang,2022)

3-2- Characteristics of digital systems:

- The most important characteristics of using digital systems in risk management are: (Tan, C.; 2020)

A- Increased flexibility: Digital systems help organizations adapt to changes quickly and respond to crises effectively.

B- Improved decision-making: These systems provide the information and analysis necessary to make informed decisions about risk management.

C- Reducing costs: Digital systems contribute to reducing costs associated with risk management, such as insurance costs and repair costs.

D- Compliance with regulations: These systems help organizations comply with regulations and laws related to risk management.

Digital systems are a powerful tool for enhancing the efficiency and effectiveness of risk management in various organizations. By providing a unified and integrated environment, these systems contribute to improving the ability to identify, assess and respond to risks, which leads to increased flexibility of organizations and improved performance.

3-3- Integration Between Systems:

Risk management is one of the fundamental pillars of the success of any organization, whether small or large. In the ever-changing business world, companies face a variety of challenges and risks that threaten their continuity. Therefore, developing effective risk management strategies has become an urgent necessity. In this context, the importance of integrating risk management systems with other systems such as enterprise resource planning (ERP) systems and customer relationship management (CRM) systems emerges.

Integrating risk management systems with other systems represents a qualitative shift in the field of risk management, as it contributes to achieving many benefits, including: (Pratono, A. H, 2018)

- Improving operational efficiency: By integrating these systems, organizations can simplify their operations and unify data, which leads to reducing the time and effort required to make decisions.

- Reducing errors: Integration helps reduce human errors by automating many routine tasks and improving data accuracy.

- Increasing transparency: Integration provides a comprehensive view of potential risks, which helps managers make more informed decisions.
- Improve decision making: By providing the necessary data and analysis, managers can better assess risks and make more effective decisions.
- Rapid response to crises: Integrated systems can detect potential risks early, allowing organizations to respond quickly and effectively to crises.
- Identify customer-related risks: Integrating risk management systems with CRM can identify customers that pose the greatest risk to the organization, helping to take preventive measures.
- Assess supply chain risks: Integrating risk management systems with ERP can assess risks associated with the supply chain, such as shipping delays or supply disruptions.
- Identify financial risks: Integrating risk management systems with ERP can identify potential financial risks, such as exchange rate fluctuations or increased costs.
- Improve operational risk management: Integrating risk management systems with ERP can improve management of operational risks, such as equipment failures or natural disasters.

3. Conclusion

Digital transformation is a fundamental pillar in the contemporary business world, as organizations increasingly rely on digital technologies in all aspects of their work. This transformation, although it brings with it many promising opportunities, poses new challenges related to risk management.

This research has shown that digital transformation significantly affects the nature of risks facing organizations, as it increases the complexity of the digital environment and provides new opportunities for cyber-attacks and fraud. However, digital technology also provides powerful tools to manage these risks more effectively.

4. Results

- Increased complexity of risks: Digital transformation has led to the emergence of new and diverse risks, such as cyber-attacks, data breaches, and reliance on digital infrastructure.
- New opportunities for risk management: Digital technologies provide advanced tools for data analysis, threat monitoring, and incident response, which contribute to improving risk management.
- The importance of digital culture: Organizations must build a strong digital culture that encourages risk awareness and taking the necessary precautions.

- The role of technology in risk management: Technology can play a crucial role in risk management, by providing tools such as artificial intelligence, machine learning, and blockchain.
- Integration of technology and management: Organizations should integrate technology into their risk management strategies, taking into account human and organizational factors.

5. Recommendations

- Develop a comprehensive digital risk management strategy: Organizations should develop a comprehensive strategy that covers all aspects of digital risk, define roles and responsibilities, and allocate the necessary resources.
- Invest in technology: Organizations should invest in the latest technologies and tools to protect digital assets and detect threats.
- Build digital competencies: Organizations should build digital competencies among their employees through training and awareness.
- Collaborate with partners: Organizations should collaborate with external partners, such as cybersecurity companies, to share information and knowledge.
- Continuous review: Organizations should conduct a continuous review of their risk management strategies to ensure that they are adapting to the ongoing changes in the digital environment.

Digital transformation is a great opportunity to improve organizations' performance and increase their competitiveness. However, managing the risks associated with this transformation requires special attention and careful planning. By following the recommendations in this research, organizations can reduce their risks and achieve their strategic objectives.

WORKS CITED

Jafari-Sadeghi, V., Garcia-Perez, A., Candelo, E., & Couturier, J. (2021). Exploring the impact of digital transformation on technology entrepreneurship and technological market expansion: The role of technology readiness, exploration and exploitation. Journal of Business Research, 124, 100-111.

An, T. L., & Wen, R. (2022). Mechanisms and empirical evidence of the impact of digital transformation on innovation in Chinese enterprises. Mod. Econ. Discuss, 5, 1-14.

Birasnav, M. (2013). Knowledge management and organizational performance in the service industry: the role of transformational leadership beyond the effects of transactional leadership. Journal of Business Research, 67(8), 1622-1629.

C Tan, C He, Z Shi, G Mo, X Geng. (2022, February). How does CEO demission threat affect corporate risk-taking? Journal of Business Research, 139, 935-944.

Chauhan, S., Gupta, P. and Jaiswal, M. (2018). Factors inhibiting the internet adoption by base of the pyramid in India (Vol. 20). Digital Policy, Regulation and Governance.

Chen, H., & Tian, Z. (2022). Environmental uncertainty, resource orchestration and digital transformation: A fuzzy-set QCA approach. Journal of Business Research, 139, 184-193.

Chen, X. H., & Zhang, H. W. (2021). How the digital economy affects the level of corporate risk-taking. Journal of Economy and Management, 43, 91-108.

Chenhall, R.H. (2003). Management control systems design within its organizational context: findings from contingency-based research and directions for the future (Vol. 28). Accounting, Organizations & Society.
Chenhall, R.H. and Morris, D. (1995). Organic decision and communication processes and management accounting systems in entrepreneurial and conservative business organizations (Vol. 23). Omega.
Chi, M. M., Wang, J. J., & Wang, W. J. (2022). Research on the influencing mechanism of firms' innovation performance in the context of digital transformation: A mixed method study. Stud. Sci. Sci, 40, 319-331.
Collier, P.M. (2005). Entrepreneurial control and the construction of a relevant accounting (Vol. 16). Management Accounting Research.
Cortiñas, M., Chocarro, R. and Villanueva, M.L. (2010). Understanding multi-channel banking customers. Journal of Business Research, 63(11), 1215-1221.
COSO. (2019). Enterprise Risk Management—Integrating with Strategy and Performance, Executive Summary (Vol. 2). Diakses pada Tanggal.
Daniel, E. (1999). Provision of electronic banking in the UK and the Republic of Ireland. International Journal of Bank Marketing, 17(2), 72-82.
Darroch, J. (2005). Knowledge management, innovation and firm performance. Journal of Knowledge Management, 9, 101-115.
Darroch, J. and Mc Naughton, R. (2002). Examining the link between knowledge management practices and types of innovation. Journal of Intellectual Capital, 3(3), 210-222.
Darroch, J. and McNaughton, R. (2003). Beyond market orientation: knowledge management and the innovativeness of New Zealand firms. European Journal of Marketing, 37(3/4), 572-593.
Das, T. and Teng, B. S. (n.d.). Between trust and control: developing confidence in partner cooperation in alliances. Academy of Management Review, 23(3), 491-512.
Dent, J. F. (1990). Strategy, organization and control: some possibilities for accounting research. Accounting, Organizations & Society, 15(1/2), 3-25.
Donate, M. J. and Guadamillas, F. (2015). An empirical study on the relationships between knowledge management, knowledge-oriented human resource practices and innovation. Knowledge Management Research & Practice, 68(2), 134-148.
Donate, M.J. and de Pablo, J. D. S. (2015). The role of knowledge-oriented leadership in knowledge management practices and innovation. Journal of Business Research, 68(2), 360-370.
Dootson, P., Beatson, A. and Drennan, J. (2016). Financial Institutions Using Social Media – Do Consumers Perceive Value? International Journal of Bank Marketing, 34(1), 9-36.
Dyllick, T., & Hockerts, K. (2002). Beyond the business case for corporate sustainability. Business Strategy and the Environment. Journal of Management Development, 11, 130-141.
Elkington, J. (1997). Cannibals with Forks: The Triple Bottom Line of 21st Century Business. Oxford: Capstone.
Farooq Rayees. (2019). Developing a conceptual framework of knowledge management. International Journal of Innovation Science, 11(1), 139-160.
Hajli, M., Sims, J.M. and Ibragimov, V. (2015). Information technology (IT) productivity paradox in the 21st century. International Journal of Productivity and Performance Management, 64(4), 457-478. Retrieved from https://doi.org/10.1108/IJPPM-12-2012-0129
Ma H, Jia X, Wang X. (2022). Digital Transformation, Ambidextrous Innovation and Enterprise Value: Empirical Analysis Based on Listed Chinese Manufacturing Companies. Sustainability Journal, 14(15), 9482. Retrieved from https://doi.org/10.3390/su14159482
Matarazzo, M., Penco, L., Profumo, G., & Quaglia, R. (2021). Digital transformation and customer value creation in Made in Italy SMEs: A dynamic capabilities perspective. Journal of Business research, 123, 642-656.
Pramanik, H. S., Kirtania, M., & Pani, A. K. (2019). Essence of digital transformation—Manifestations at large financial institutions from North America. Future Generation Computer Systems, 95, 323-343.
Pratono, A. H. (2018). Does firm performance increase with risk-taking behavior under information technological turbulence? Empirical evidence from Indonesian SMEs. The Journal of Risk Finance, 19(4), 361-378.
Shang, H. T., & Wu, T. (2022). Digital transformation, social responsibility and corporate value. Journal of Technology and Economy, 41, 159-168.
Song, C., Nahm, A. Y., & Song, Z. (2021). Entrepreneurs' hobbies and corporate risk taking: Evidence from China. International Review of Financial Analysis, 77, 101856.

Wu, F., Hu, H., Lin, H., & Ren, X. (2021). Enterprise digital transformation and capital market performance: Empirical evidence from stock liquidity. Management world, 37(7), 130-144.
Zhai, H. Y., & Li, Q. R. (2022). Has digital transformation of enterprises improved audit quality? An empirical test based on a multi-temporal double difference model. Econ. Res, 37, 69-80.
Zhang, J. C., & Long, J. (2022). Digital transformation, dynamic capability, and enterprise innovation performance: Empirical evidence from high—Tech listed companies. J]. Economics and Management, 36(03), 74-83.
Zhang, J., Long, J., & Von Schaewen, A. M. E. (2021). How does digital transformation improve organizational resilience?—findings from PLS-SEM and fsQCA. Sustainability, 13(20), 11487.
Zhou, Z., Luo, J., & Li, X. (2019). Identity and risk-taking level of private enterprises. Management World, 35(11), 193-208.