ISBN: 978-81-974990-1-2

8. Exploring the Role of Risk Management in The Implementation of New Technologies and Digital Transformation

Dr. Suunil Losarwarr

Director,
Sharat Chandra Pawar Institute of Management,
Otur, Pune, India.

Dr. Girish Kumar Painoli

Professor, School of Commerce and Management,
Aurora Deemed to be University,
Hyderabad, India.

Abstract:

Modern risk management approaches are dependent on technology. It supports companies in their efforts to collect and analyze data, enhance decision-making, and automate and expedite risk management processes. Organizations need to change quickly in today's technology environment in order to stay competitive. The purpose of this article is to investigate how risk management and organizational resilience are affected by emerging technologies like block chain, AI, and the Internet of Things. We will explore these technologies' possible advantages and disadvantages as well as the kinds of issues they can resolve. We'll discuss in this essay. looking into how risk management fits into the adoption of new technologies and digital transformation.

Keywords:

Risk Management, Digital Transformation, New technologies, Cybersecurity Risks, Data Privacy Risks, Block chain, Risk Governance.

8.1 Introduction:

Enterprises need effective risk management to navigate uncertainties and maintain resilience in an increasingly complex and interconnected environment. As the business environment develops, companies are increasingly faced with new risks and challenges. In response to these worries, emerging technologies are significantly altering risk management techniques.

The importance of digital technology as a catalyst for innovation is gradually becoming acknowledged. Unmatched development and value-creation opportunities and capabilities are presented by the digital transformation. But none of the opportunities can materialize if the risks are not addressed.

Thus, an organization's capacity to handle risks determines whether it will be able to survive in the modern world. In today's ever changing business world, digital transformation has become crucial for firms to maintain relevance and competitiveness. However, there are dangers associated with implementing new technology and digital processes that must be properly managed. A strong risk management plan must be put into place to guarantee a successful digital transformation.

8.2 Artificial Intelligence and Machine Learning:

Artificial intelligence and machine learning, which provide improved analytics capabilities, are revolutionizing risk management. These technologies enable data-driven decision making, pattern identification, and large-scale data analysis for organizations. AI and ML algorithms can be used to discover irregularities, automate risk assessment processes, and evaluate risks in real-time, all while improving the accuracy and efficiency of risk management procedures.

8.3 Risk Management in Digital Transformation:

The following are the specifics of risk management in digital transformation:

Risks to Cybersecurity: Organizations are more vulnerable to cyberattacks when they use new technologies. Data breaches, ransomware attacks, phishing scams, and other forms of attacks are examples of cybersecurity dangers. To lessen these dangers, organizations must implement robust security measures like firewalls, intrusion detection systems, and encryption.

Risks to Data Privacy: A greater amount of data is being collected and stored by companies than ever before due to the increased usage of technology. This raises new concerns around data privacy and adherence to laws like the CCPA and GDPR. Employing access controls, encrypting data, and making sure privacy laws are followed are just a few of the safeguards that organizations must establish to protect sensitive data.

Vendor Risks: For technology solutions and services, organizations frequently depend on outside providers. These vendors may, however, also provide additional dangers, such as security flaws or data breaches. Organizations must adopt vendor risk management procedures, perform due diligence on suppliers, and make sure that vendors adhere to their security and privacy policies in order to reduce these risks.

Operational Risks: Along with these additional operational risks, digital transformation can also bring in human error, process breakdowns, and system outages. Establishing business continuity and disaster recovery strategies is vital for organizations to minimize risks and guarantee the prompt restoration of crucial systems and procedures in the event of an interruption or outage.

Risks of Change Management: Process and workflow adjustments are frequently necessary for a business to undergo digital transformation. New risks, such personnel turnover or resistance to change, may be brought forth by these developments.

Organizations must have change management procedures in place, properly inform staff members of changes, and offer assistance and training to help staff members adjust to new procedures and technological advancements in order to reduce these risks.

Organizations need to handle new risks brought about by digital transformation to make sure their initiatives succeed. Through risk identification and mitigation, organizations can leverage emerging technologies and accomplish their objectives related to digital transformation.

8.3.1 Implementing a Risk Management Strategy:

A risk management strategy is usually implemented within an organization by a hierarchy of participants, each of whom is in charge of a certain task. The implementation of a risk management plan involves four crucial components.

Identify Existing Risks:

The first step in any effective risk management plan is risk identification. Organizations can establish a successful plan by proactively identifying risks rather than focusing on the ones that are already known. The methods and resources listed below can be utilized to identify risks.

- Reviews of documentation (such as organizational procedures, assets, and vulnerability reports)
- collaborating on ideas with teams from various departments inside the company that are aware of risk considerations (e.g., IT security teams, project managers, facilities managers)
- Root because analysis can reveal new dangers beyond those that are already known.
- SWOT analysis: Weaknesses, Opportunities, Threats, and Strengths
- A list of risk categories
- Analysis of assumptions, including a validity assessment
- An often-updated risk registers with new, removed, or altered issues

8.3.2 Assess the Risks:

Risks should be analyzed to ascertain their potential severity, predicted impact, and chance of developing into a problem after being inventoried. There are usually more dangers than resources for most firms. Organizations can ensure the success of their risk management plan by allocating scarce resources more efficiently by prioritizing risks.

These are some methods and instruments that can be used to evaluate risks.

- Probability and impact matrix
- Risk data quality assessment
- Analysis of risks
- Respond to risks

Organizations must develop strategies and plans to address risks after risk priorities have been determined. This involves quickly creating and putting into practice plans to reduce or eliminate hazards. During a risk management strategy's risk response phase, the following instruments and methods can be useful:

- Prioritized list of quantified risks
- Decision trees
- Risk register updates
- Calculations for time required to address specific risks

Monitor Risks:

Monitoring is the last stage of a risk management plan. This means developing and implementing identify, assess, and respond preventive procedures to get new threats into the previously mentioned flow. Risks always evolve and alter; thus, risk management should be an ongoing effort.

8.4 Technology Risk Management Process:

The first step in the technology risk management process is a technology risk analysis. The risk management team currently use methods to categorize and rank the technology hazards in order to assess and resolve such worries.

The identification of technology threats should be an ongoing activity. Therefore, it makes sense to panel a group of people in order to identify the causes of technology threats. To identify which risk management frameworks are appropriate for each prospective technology threat, these risk committee members' knowledge and experience should be combined.

After identifying the technical risks, the risk management team should prepare a risk management strategy for each risk. Next, the group should use a risk assessment software application to score and classify those hazards. Technology risks must to be prioritized in accordance with the potential harm they could do the business and the likelihood that they will manifest.

Organizations can also find potential technological risks that could thwart their desired business objectives by creating a technology risk register, which is a documented record of discovered concerns.

8.5 Review of Literature:

However, risk management is a challenging endeavor with numerous challenges. The rising interconnectivity of supply chain players has improved operations, but it has also increased businesses' dependence on one another, making them more vulnerable to disruptions (Mwangi et al., 2021).

The mass collection of data and the unpredictable nature of disruptions and vulnerabilities describe the current state of risk management, which affects operational efficacy and efficiency.

Managing inconsistent information resulting from the absence of a central shared database, managing multiple datasets in heterogeneous formats, managing inadequate supply chain visibility and traceability, minimizing discrepancies arising from manual reporting, and deriving strategic insights from large and rapidly accumulating data sets are just a few of the many tasks involved in risk management. The effectiveness of risk prediction, planning, and crisis management are all highly influenced by these activities.

New technologies such as block chain, cloud computing, AI, big data and analytics, Internet of Things, and industrial Internet of things are major drivers of digital transformation. Due to the numerous benefits of digital transformation, businesses are moving more quickly toward it.

Organizations need to protect their digital transformation tools and assets to ensure business continuity. Businesses now have serious concerns about cybersecurity. Consequently, companies implementing DT must ensure that cybersecurity measures are their top concern and that their systems are secure from intrusions.

Osborne and Brown (2013) Consequently, enterprise management's propensity to take risks is increased by digital transformation, which eventually raises the risk-taking levels of organizations.

Enterprise innovation is enhanced when there is a higher degree of risk-taking, better acceptance and recognition of innovation, a more favorable attitude toward innovation, stronger motivation for innovation, and a greater willingness to boost R&D investment in innovation.

Thus, this study postulates that the degree of risk-taking mediates the relationship between enterprise innovation and digital transformation, i.e., the innovation of organizations is influenced by their amount of risk-taking as a result of their digital transformation.

Due to digitalization and the phenomenon of digital transformation, businesses and organizations are functioning in essentially different ways (Collin et al. 2015). Despite being acknowledged as a major barrier to complex organizational change, the direction and scope of research in the subject of transition have not yet shown conclusive results.

Predicting the effects of the digital transition is still difficult, with many different estimates that contradict one another. There is some risk associated with their organizational adaptation as a result. The necessity for e-leadership, a new form of leadership, has arisen from the increased expectations placed on leaders of digital businesses. A computer-mediated communication method of leadership is called e-leadership.

Hartl and Hess (2017) conducted a study on experts in digitalization and found that the effectiveness of digital transformation was largely dependent on the experts' preference for

flexible organizational cultures (i.e., clan/adhocracy) over control organizational cultures (i.e., hierarchical/market). Cultures that fostered traits like adaptability, tolerance for failure, openness to change, and a willingness to learn were more highly regarded during the digital transformation.

Important organizational principles that were mentioned included cooperation, community, and customer-centricity, as well as innovation, risk affinity, and entrepreneurship. Another study that involved stakeholders in the company discovered that by implementing techniques like reverse mentoring to enhance digital competences and skills, organizations may create transparent cultures, overcome resistance to digitalization, and promote digital cultures.

8.6 Objectives:

- Study the Risk Management and implementation Strategies
- Examining the Role of Risk Management in the Implementation of New Technologies and Digital Transformation
- Study the Digital risk management framework with a specific focus on mitigating cybersecurity and data leak risks

8.7 Research Methodology:

This study's overall design was exploratory. The research paper is an endeavor that is founded on secondary data that was obtained from reliable online resources, newspapers, textbooks, journals, and publications. The research design of the study is mostly descriptive in nature.

8.8 Result and Discussion:

Emerging Technologies:

Among the most well-known emerging technologies are artificial intelligence (AI), machine learning (ML), distributed ledger technology (DLT), and the Internet of Things (IoT). AI and ML are transforming data analysis, enabling organizations to recognize potential risks and take quicker, more informed decisions.

In order to identify trends that may indicate future dangers or vulnerabilities, AI-driven systems, for example, are able to analyze massive volumes of data. Internet of Things (IoT) is transforming asset management and monitoring for businesses by enabling real-time data collection and analysis through device and sensor connections to the internet. This enables faster and more effective risk detection and response for organizations.

Furthermore, by offering a decentralized and impenetrable record of transactions and data, DLT (such as Block chain) is improving security, trust, and transparency in risk management procedures. In figure 8.1 below, the vast amount and diversity of developing technologies are highlighted.

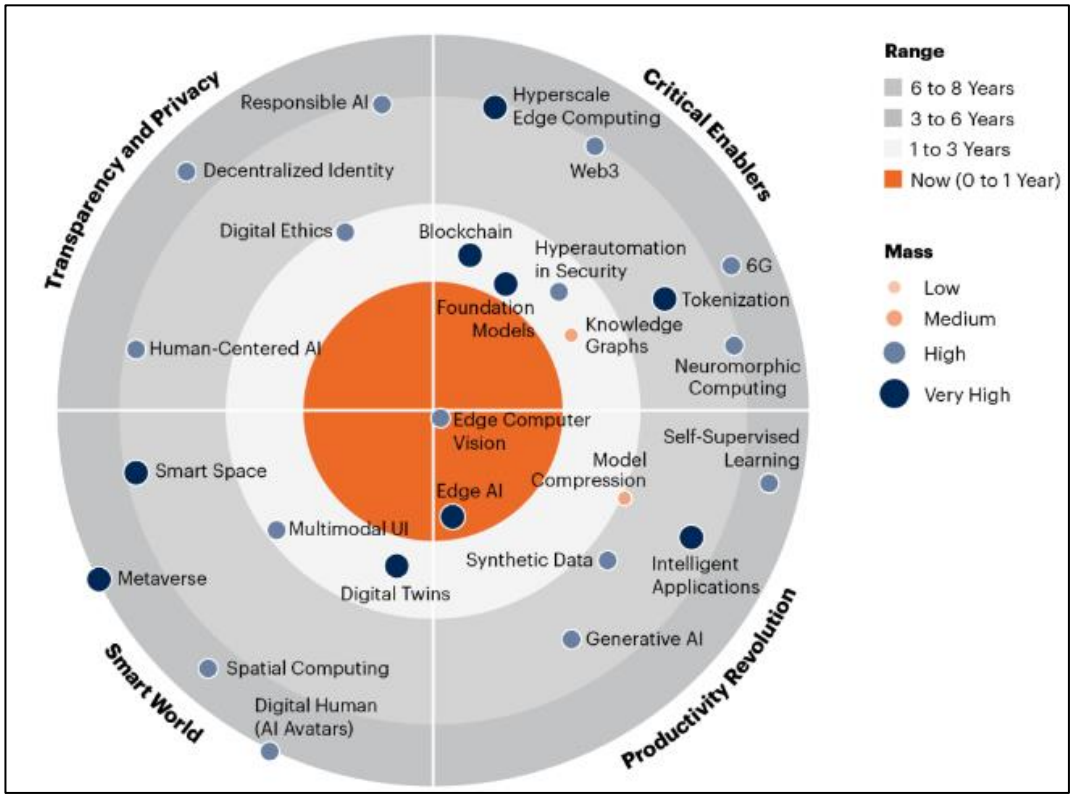

Figure 8.1: New Emerging Technologies and Trends Impact Radar (Source: Gartner, 2023)

The exponential growth of processing power, the speed at which data processing and storage are developing, the expansion of connectivity and data sharing, and other variables all contribute to the rate of technological improvement.

Processor technology breakthroughs and the shrinking of electronic components have led to an exponential expansion in computing capacity, which has allowed organizations to process and analyze data at previously unheard-of speeds.

This has made it easier to create increasingly complex risk management models and algorithms.

Taking risks acts as a bridge between enterprise innovation and digital transformation:

As illustrated in Figure 8.2, our study suggests an intermediary effect model for how enterprise innovation is affected by digital transformation.

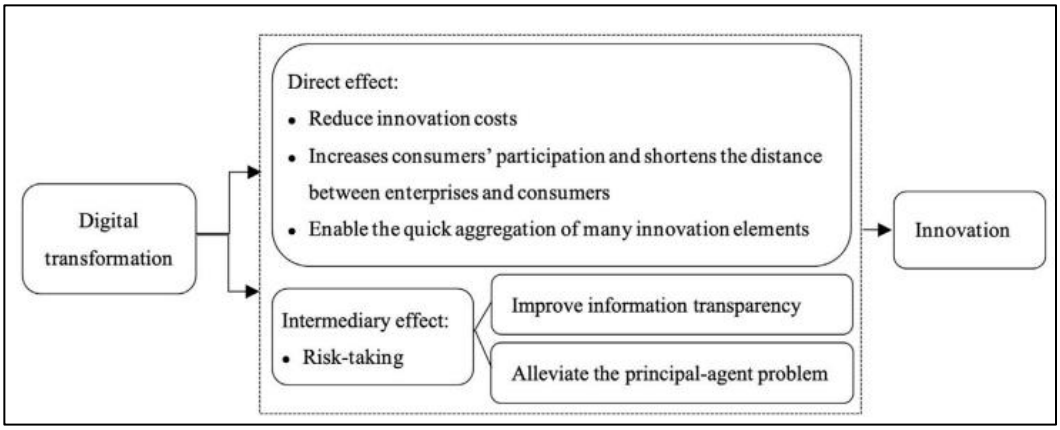

Figure 8.2: Mechanism Roadmap

8.9 How to Manage Digital Risk:

Visibility, insights, and remediation are the three cyclical components of effective digital risk management, and each quadrant is powered by the information gleaned from the one before it.

Digital foot printing is used to gain visibility in order to monitor exposed assets. Visibility data is put into threat intelligence platforms to give them insights into the best remediation tactics. Remedial techniques that are incredibly effective can be devised and put into practice with the help of insights from the digital landscape.

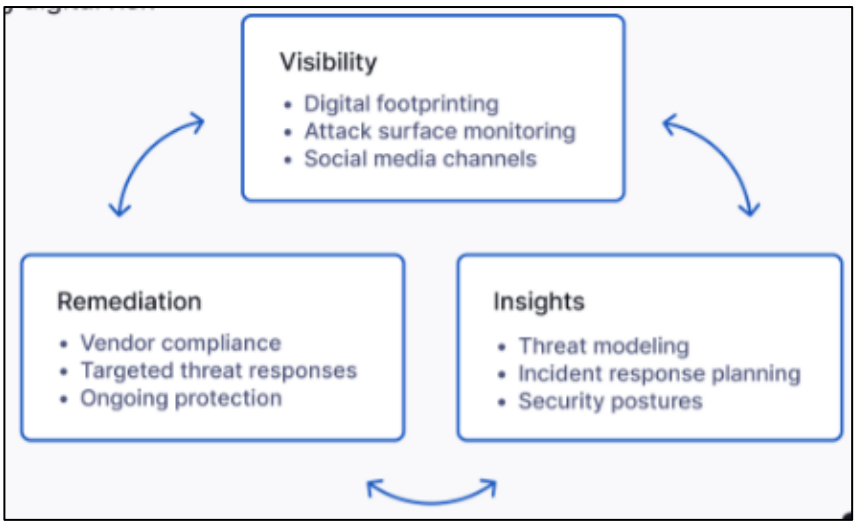

Figure 8.3: Manage Digital Risk

A methodology for digital risk management is outlined below, with an emphasis on reducing the risks associated with data leaks and cybersecurity:

Step 1: List every asset that is exposed

List every asset that might be subject to illegal access. All social media platforms and other sources that contain sensitive data should be included in this. An attack surface monitoring solution can assist in mapping a digital footprint.

Step2: Keep monitoring out for data leaks

Using a data leak detection tool, you may find any data leaks related to your business, providing you with visibility and vulnerability insights into this frequently ignored attack vector.

Step 3: Update your risk and threat models

After establishing your digital footprint, you can compile all threat intelligence information to create a threat landscape model. Updates to incident response, business continuity, and disaster recovery plans should also be considered by organizations to ensure that all security teams are equipped to address any potential cyber risk element. By doing this, cyber resilience will rise.

Step 4: Safe access to every resource that's exposed

Privileged accounts and digital assets should be secured to prevent harm to one's reputation. The scope of detection criteria should be expanded to identify and prevent all illegal network access, rather than concentrating just on well-established cyber defenses surrounding critical resources.

8.10 Future of Risk Management:

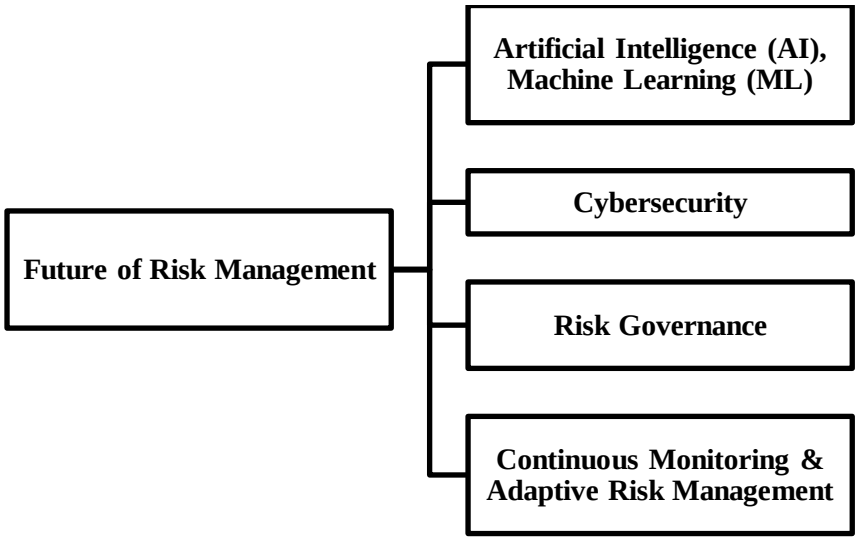

Figure 8.4: Future of Risk Management

Cybersecurity:

Cybersecurity is now a vital component of risk management due to the spread of digitalization and networked technologies. Cyberattacks, data breaches, and information security vulnerabilities are becoming more and more of a concern to organizations.

Strong cybersecurity procedures must be put in place to safeguard confidential information, intellectual property, and client data. Advanced cybersecurity technologies such as threat intelligence, encryption, and behavioral analytics are critical for identifying and mitigating cyber threats.

Risk Governance:

A key component of efficient risk management is risk governance. To guarantee accountability and openness, it entails creating precise risk management frameworks, rules, and procedures. Organizations must take a proactive approach to risk governance in light of the changing nature of the risk landscape. This entails creating risk-aware cultures, creating risk-management strategies that are in line with company goals, and incorporating risk management into decision-making processes at all organizational levels.

8.10.1 Continuous Monitoring and Adaptive Risk Management:

Traditional risk management techniques frequently include periodic appraisals. However, the future of risk management will be shaped by continuous monitoring and adaptable risk management strategies. Businesses may swiftly recognize emerging threats and take preventative measures by leveraging real-time data.

8.10.2 For Risk Management (RM) to be effective, a corporation at all levels must abide by eleven principles. Risk management should do the following of these:

Create and safeguard value: Risk management (RM) serves to enhance performance in various domains like as security, legal compliance, environmental protection, product quality, operational efficiency, governance, and reputation. It also assists in verifying the attainment of objectives.

Risk management should be a fundamental part of all organizational processes; it cannot be carried out independently of other tasks and organizational policies. It is the responsibility of management and an essential part of all organizational processes, including strategy development, project management, and change management;

Participate in decision-making—RM assists decision-makers in identifying options, prioritizing activities, and making well-informed decisions;

Be organized, timely, and systematic: An organized, timely, and systematic approach to risk management promotes efficiency and thoughtful, consistent, and reliable outcomes;

Be open and inclusive. Ensuring that decision-makers are appropriately and quickly involved with stakeholders at all organizational levels contributes to the relevance and current risk management. In addition to the framework and guiding principles, the standard outlines the risk management process that can be implemented in any type of company. It makes sense that the risk management process should be a crucial part of management, incorporated into the customs and practices of the organization, and tailored to its specific business operations. Figure 8.5 shows the risk management process as it is stated in.

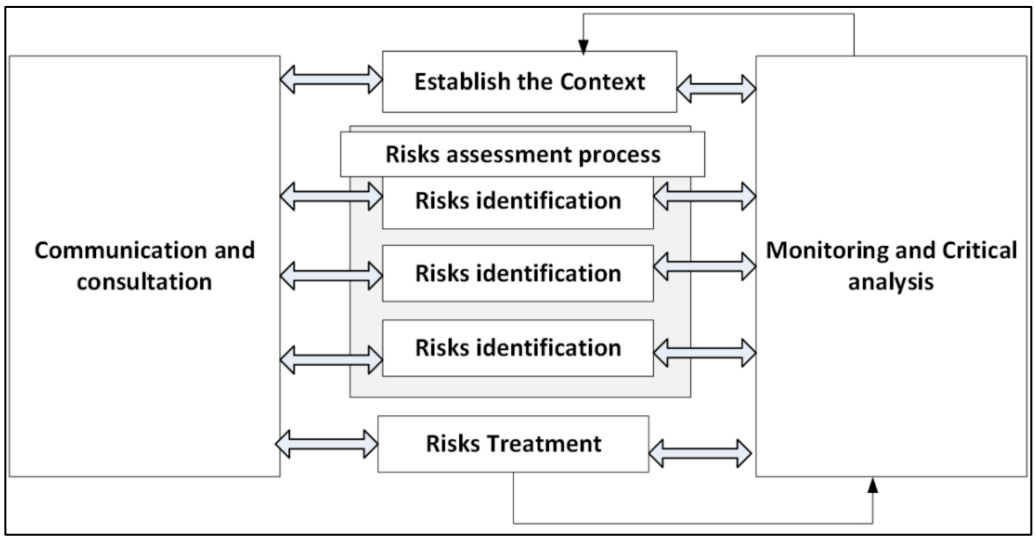

Figure 8.5: Risk Management Process

Ensuring that there is communication and consultation with both internal and external stakeholders at every stage of the risk management process is the aim of the communication and consultation process. The parameters that need to be considered for risk management, such as the scope and risk criteria, are established by contextualization.

The term "risk assessment process" refers to the complete set of steps involved in risk detection, analysis, and evaluation. The best solutions to reduce the risks are chosen, together with the strategies required to put them into action. This is known as risk treatment. On the other hand, the goal of critical analysis and monitoring is to get more data to enhance risk assessment and to guarantee that risk-related controls are efficient and successful.

8.11 Conclusion:

Organizations starting their digital transformation journeys must have excellent risk management. Businesses may confidently traverse the challenges of digital transformation and accomplish their strategic goals by putting proactive risk mitigation methods into place and cultivating a risk-aware culture. The business environment is changing quickly due to digital transformation across all industries, which presents chances for new initiatives and capabilities to grow dramatically. Organizational agility is one of the most important success criteria in this digital era.

Companies can design a flexible and customized approach, along with a well-defined digital strategy and a suitable business case, to create a scalable and adaptive digital experience. In addition to implementing digital transformation, enterprises must effectively manage environmental risks and their effects on the current ecosystem in order to maximize the value of their digital activities.

8.12 References:

1. Bongiovanni, C.; L. Pancaldi; U. Stegemann; G. Taglioni, Transforming Enterprise Risk Management for Value in the Insurance Industry, McKinsey & Company, July 2016,
2. Brown, L., & Osborne, S. P. (2013). Risk and innovation: Towards a framework for risk governance in public services. Public Management Review, 15(2), 186–208.
3. Contreras, Francoise, Elif Baykal, and Ghulam Abid. 2020. E-Leadership and Teleworking in Times of Covid-19 and beyond: What We Know and Where Do We Go. Frontiers in Psychology 11: 590271.
4. Ferris, P. A., Sinclair, C., and Kline, T. J. (2005). It takes two to tango: personal and organizational resilience as predictors of strain and cardiovascular disease risk in a work sample. J. Occup. Health Psychol. 10, 225–238.
5. G.M. Mwangi, S. Despoudi, O.R. Espindola, K. Spanaki, T. Papadopoulos A planetary boundaries perspective on the sustainability: resilience relationship in the Kenyan tea supply chain Ann. Oper. Res. (2021)
6. Guldentops, E.; De Haes, S.; Hardy, G.; Ormsby, J.; Singleton, J. Board Briefing on IT Governance; IT Governance Institute: Schaumburg, IL, USA, 2009.
7. Hajli, M.; Sim, J.M.; Ibragimov, V. Information tech-nology (IT) productivity paradox in the 21st century. Int. J. Product. Perform. Manag. 2015, 64, 457–478.
8. Hartl, E., and Hess, T. (2017). The role of cultural values for digital transformation: insights from a Delphi study. Paper Presented at the 23rd Americas Conference on Information Systems, Boston, MA.
9. Hausberg, J. P., Liere-Netheler, K., Packmohr, S., Pakura, S., & Vogelsang, K. (2019). Research streams on digital transformation from a holistic business perspective: a systematic literature review and citation network analysis. Journal of Business Economics, 89, 931-963.
10. Matt C., Hess T., Benlian A. Digital transformation strategies. Bus. Inf. Syst. Eng. 2015; 57:339–343. doi: 10.1007/s12599-015-0401-5.
11. Radicic, D., & Petković, S. (2023). Impact of digitalization on technological innovations in small and medium-sized enterprises (SMEs). Technological Forecasting and Social Change, 191, 122474.
12. Renn, O. Risk Governance: Coping with Uncertainty in a Complex World; Routledge: Abingdon, UK, 2017
13. Schein, Edgar H. 2010. *Organizational Culture and Leadership*, 4th ed. San Francisco: Jossey Bass.
14. Standards Australia, "AS 8015-2005: Australian Standard for Corporate Governance of Information and Communication Technology," Standards Australia, 2005,
15. Wang, Q., & Waltman, L. (2016). Large-scale analysis of the accuracy of the journal classification systems of Web of Science and Scopus. Journal of informetrics, 10(2), 347-364.