Library Progress International
Vol.44 No. 3, Jul-Dec 2024: P. 18486-18500

Print version ISSN 0970 1052
Online version ISSN 2320 317X

Original Article

Available online at www.bpasjournals.com

The Impact of Digital Transformation Requirements on Risk Management

Nedal Alnawaiseh [1], Mohammad Abdalrheem Al-Mahasneh [2]

[1,2] Mu'tah University
Nedal.alnawaiseh@AB.gov.jo

How to cite this article: Nedal Alnawaiseh , Mohammad Abdalrheem Al-Mahasneh (2024) The Impact of Digital Transformation Requirements on Risk Management**.** *Library Progress International,* 44(3), 18486-18500.

ABSTRACT
This research takes a look at how the imperatives of digital transformation impose an impact on the landscape of risk management strategies across four dimensions: the adoption of technology, cybersecurity and data privacy, regulatory compliance, and finally, risk mitigation strategies. 100 participants from different walks of industry from jordan responded to structured questionnaires in the assessment of how such organizations operate to manage emerging risks ushered in by digital technologies. Results indicate that while digital transformation significantly enhances operational efficiency and agility, it introduces new causes for concern in cybersecurity and compliance. Respondents showed a high level of investment in technology with a mean of 4.3 and efficiency improvement at a mean of 4.5, although some shortcomings persist regarding employee cybersecurity awareness, with a mean of 3.6, and complexity of regulatory compliance, with a mean of 3.7. Although risk mitigation strategies have become common, only 32% of organizations have integrated their risk management teams into digital initiatives. This paper concludes by remarking on the basis of an update an organization needs to make to its risk management framework, improve cybersecurity training, and undertake proactive compliance mappings in order to achieve successful meeting of the complexities posed by the digital era.

Keywords
Digital Transformation, Risk Management, Cybersecurity, Data Privacy, Regulatory Compliance, Technology Adoption, Operational Efficiency, Compliance Complexity, Risk Mitigation

Introduction

This is so because the digitalization of enterprises has now become a strategic driver of innovation and competitiveness. The whole notion of integrating digital technologies into all aspects of business implies basic changes in how companies conduct business and deliver value to customers**(Rachinger et al., 2018)**. The unfolding of the current industrial revolution suggests that the use of new technologies like AI, big data, cloud computing, and IoT is becoming quite trendy**(Handfield)**. These technologies have many advantages: efficiency, better decision-making, and improving customer experiences. At the same time, digitalization also brings a number of drawbacks, especially in terms of risk management**(Tohănean et al., 2020)**.

Risk management is the important organizational function of identification, evaluation, and mitigation of risks that hamper the attainment of strategic objectives**(Monahan, 2008)**. Conventionally, risk management has focused on operational, financial, and compliance-related risks. Digital transformation brings new risks centered on cybersecurity, data privacy, technological disruption, and regulatory compliance. This complexity of managing these risks has forced a reevaluation of conventional risk management frameworks and practices**(Monahan, 2008)**.

The use of digital technologies introduced new vulnerabilities that organizations interested in the continuity of their business and protection of their assets need to address. Inadequately managed, cyber-attacks, data breaches, or system failures can drive businesses to catastrophic ends with possible severe financial losses, reputation damage, and legal liabilities**(Saeed et al., 2023)**. Moreover, the further application of digital platforms and data-driven decision-making exacerbates the risk associated with data governance, misaligned technology strategies,

and lagging regulatory compliance**(Anthony Jnr, 2022)**. Therefore, risk management will have to adapt not only to reduce the traditional risk factors but also to match the challenges presented by digital transformation**(Gerber & Von Solms, 2005)**.

The paper discusses the effect of the requirements for digital transformation on the organizational strategies of risk management. It seeks to find out, in particular, how the adoption of digital technologies influences the identification, assessment, and mitigation of risks. The role that risk management would play in assisting with the implementation of the digital transformation initiatives in such a way as to minimize risks and optimize the potential for business success will also be considered within the paper. This research has assessed various challenges and opportunities regarding digital transformation to provide insight into the ways organisations can use improved practices of risk management to address the complexities brought about by the digital age.

Digital Transformation and Its Strategic Importance

The concept of digital transformation has evolved to become an intrinsic part of organizational strategy in today's modern, fast-moving business world**(Gong & Ribiere, 2021)**. It is, in other words, the integration of digital technologies into all aspects of an organization that changes how businesses operate and deliver value to their customers**(Korhonen & Halén, 2017)**. More than technology advancement, digital transformation is about rethinking processes, roles, and systems to optimize performance in a world increasingly driven by technology**(Aguiar, 2020)**. Going digital is no longer a distinctive competitive advantage but an imperative for any organization that wants to remain relevant and competitive in its industry.

The role of digital transformation for modern organizations is far from merely adopting new technologies, as it inherently drives essential changes in business models, operational efficiencies, and customer experiences**(Gong & Ribiere, 2021)**. The rapid changes that are occurring in technology have rendered the conventional mode of operation in many industries somewhat obsolete and compelled companies to implement digital means in most transactions to meet the changing needs and expectations of consumers**(Frankel, 1955)**. Mainly, the consumer requires speedier service, personalization, and information at their fingertips, compelling the organizations to adopt technology measures to meet these demands**(Bitner et al., 2000)**.

The primary driver for digital transformation in companies is the opportunity to increase operational efficiency. Companies are able to manage the streamlining of processes and automation of tasks, thereby reducing human-generated errors, through the use of digital tools**(Berman, 2012)**. It provides an improvement in productivity and cost reduction. AI, big data analytics, and automation embedded in organizations make it efficient to optimize workflows, make data-driven decisions, and improve customer experiences**(Adesina et al., 2024)**. For instance, AI-powered chatbots can respond to customer queries around the clock, thus greatly reducing response times and improving overall customer satisfaction. Moreover, automating back-office tasks like invoicing, payroll, and inventory management frees up employees to undertake more strategic work of higher value**(Madakam et al., 2019)**.

Another very important driver for digital transformation is the ability to innovate and unlock new sources of revenue. Companies that have the power to connect effectively to digital technologies can unlock their full potential to introduce new business models offering more innovative products and services for the increasingly changing customer needs**(Berman, 2012)**. Digital has opened up paths for growth in several avenues, including e-commerce, subscription-based services, and cloud-based solutions. These business models provide further revenue opportunities but also better flexibility, and thus allow companies to scale fast and become more responsive to changes in the marketplace in real time**(Taherdoost, 2023)**.

Secondly, digital transformation enhances informed decision-making ability for an organization. All the abundant data generated by digital systems, if appropriately channeled, serve valuable insights into customer behavior, market trends, and operational performance**(Shah, 2018)**. Analytics would thus allow an enterprise to understand customers more, predict the future, and present areas that require improvement**(Davenport et al., 2010)**. Large volumes of data being analyzed in real time possess capabilities that provide a competitive advantage for a business with quicker and finer decision-making**(Kitchens et al., 2018)**. For example, predictive analytics will let the organization project or estimate customer needs so its supply chain operations are optimized and the risk of stockout or overstocking minimized.

there are also drawbacks among many advantages. The major reason that is holding organizations back from completely implementing digital transformation is the integration of new digital technologies with already built ones on a legacy system foundation**(Herbert, 2017)**. To date, businesses continue to run predominantly on

infrastructure that was designed and built using technologies no longer applicable or compatible with newer digital solutions. In this way, the old and new systems fall out of step; inefficiencies abound, data silos build up, and security is compromised. This assumes complex and sometimes cumbersome integration, which may mean investment in infrastructure upgrades, as well as employee training. Organizations need adequate planning and integration of the new technology if digital transformation is to succeed

Impact of Digital Transformation on Risk Management

Digital transformation has redefined the concept of risk management in organizations of all walks of life. As more and more companies make use of digital technologies in their line of businesses, the face of risk has also completely changed, therefore forcing firms to reconsider their means of identifying, assessing, and mitigating various forms of risks**(Siebel, 2019)**. If one were to look back, then traditionally, risk management had its focus on operational, financial, and compliance-related risks**(Feroz et al., 2021)**. However, with the advent of the digital age, a whole new dimension of risks has surfaced that includes cybersecurity threats, data privacy concerns, and technological disruptions, among others**(Thakur, 2024)**. This evolution has brought a need for organizations to reshape their conventional risk management framework to not only mitigate these digital risks but also ensure business continuity in an ever-connected and data-driven world**(Hubbard, 2020)**.

The ever-changing risk management in today's digital world is brought about by the pervasiveness of cloud computing, AI, big data, and IoT**(Fataftah, 2022)**. These have changed organizational functions for good, where operations are performed with greater efficiency, data analysis is done in real time, and better customer experiences are afforded**(Dhayanidhi, 2022)**. But these advantages also leave companies with several new vulnerabilities, to which traditional ways of managing those risks may not be wholly adequate**(Waters, 2011)**. For example, while operational risks were all but internal and part of the business processes in the past, digital transformation has introduced external threats in the form of cyberattacks, data breaches, and hacking attempts that pose severe financial, operational, and reputational damages**(Saeed et al., 2023)**.

Cybersecurity is probably the most prominent risk caused by digital transformation. While organizations are becoming increasingly dependent on digital platforms and data-driven processes, they also are getting more exposed to the threats of cyberattack**(Möller, 2023)**. These are the weak points through which cybercrimes attack the infrastructures and have the potential for information leaks: customer data, intellectual property, financial records, among other sensitive pieces of information**(Taplin, 2020)**. Ransomware attacks, phishing schemes, and other forms of cybercrime have driven organizations to build robust cybersecurity mechanisms**(Perwej et al., 2021)**. Unfortunately, many businesses, especially those in the process of first-time digital transformation, could lack the expertise and resources to provide adequate protection for all their digital assets. This tears a big hole into their risk management strategy and exposes them to potential breaches and costly repercussions**(Borghesi & Gaudenzi, 2012)**.

Besides cybersecurity risks, digital transformation carries operational risks. New technologies integrated into already operational business systems can often bring in problems of compatibility, system downtimes, and technical glitches**(Kechagias et al., 2022)**. Since most organizations run on legacy systems, most modern digital tools are not really designed to interface with these, resulting in disruptions to operations upon introducing new technologies. Besides, the complexity of operating from a multi-digital platform base and managing seamless flow within departments for the smooth flow of data might lead to inefficiencies, delays, and higher operational costs**(Seacord et al., 2003)**. This cannot be supported by the risk management teams, which need to account for these possible breaks. In such a case, smooth integration of digital technologies and contingency plans in case of a technical failure are required**(Naimi-Sadigh et al., 2022)**.

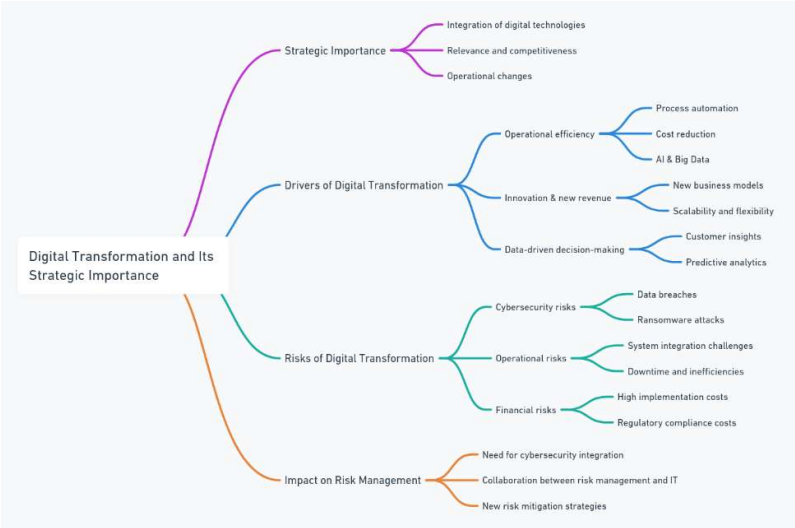
Another growing concern in the context of digital transformation relates to financial risk. The cost of implementing digital technologies could be quite high, especially for smaller organizations or those in highly regulated industries**(Zhu et al., 2006)**. On the other hand, the capital investment is huge for investment in new technologies, upgrades of existing systems, and training of employees in their use. But most importantly, risks do not stop with financial investment**(Chanias et al., 2019)**. Unless properly managed, digital transformation presents a number of extra costs involving cybersecurity incidents, regulatory non-compliance, and operation disruptions for an organization. Furthermore, the fast movement in technological development requires any organization to invest in new tools and solutions constantly, which puts pressure on financial resources**(Marotta & Madnick, 2021)**.

These increasing risks necessitate re-aligning traditional risk management frameworks to accommodate and meet the needs of the digital era. Precisely, it requires integrating cybersecurity into general risk management**(Wegener, 2007)**. No longer confined to the IT department, cybersecurity risks have now become a major cause of concern for the entire organization. The risk management teams must seriously collaborate with the IT professionals in identifying possible vulnerabilities, assessing the likelihood and impact of cyberattacks, and developing mitigation measures that could help avoid them**(Sommer & Brown, 2011)**. This will involve investment in sophisticated security technologies, including firewalls, encryption, and multi-factor authentication, as well as regular security audits and employee training sessions to ensure that all staff are cognizant about cybersecurity best practices**(Cavusoglu et al., 2009)**.

Cybersecurity and Data Privacy in Digital Transformation

Cybersecurity and data privacy have emerged in the digital times as two of the biggest concerns in relation to digital transformation. The companies, while introducing advanced digital technologies to make their operations more effective, the customer experiences richer, and decision-making wiser, are faced at the same time with a whole set of new vulnerabilities**(Wang et al., 2024)**.

Thus, the cyber-attackers, data breaches, and unauthorized access to sensitive information are gaining momentum nowadays, posing major potential threats to the financial stability, reputations, and legal standing of



businesses**(Möller, 2023)**. This is considered a huge issue because digital transformation brings increased dependency on such technologies; therefore, nothing is more important than robust cybersecurity measures and comprehensive data privacy practices. The rise in the expansion of digitization efforts has increased the importance of cybersecurity**(Saeed et al., 2023)**.

These are organizations that heavily rely on the connected systems, cloud computing, AI, big data, and IoT to achieve innovation and efficiency. These same technologies unleash unprecedented benefits while introducing new avenues for cyber threats**(Rabah, 2018)**. From lone hackers to state-sponsored groups, these malicious actors develop sophisticated methods of taking advantage of vulnerabilities in digital infrastructures. These can disrupt operations, pilfer valuable data, and create enormous financial losses. In organizations that deal in sensitive customer information, proprietary data, or critical infrastructure, cybersecurity has emerged as one of the prime concerns**(White, 2014)**. Data privacy is accorded a place next to cybersecurity in the line of digital transformation. This ranges from personal and financial data, which organizations increasingly collect and store**(Mattsson, 2023)**. Best practices to reduce cybersecurity risks and data privacy must be integrated into a company's digital transformation process. One of the foundational building blocks in cybersecurity involves setting up robust access control mechanisms**(Möller, 2023)**. This ensures that only certain sensitive systems or data have access to those personnel who are so authorized, reducing the chances of internal breaches and accidents**(Möller, 2023)**.

MFA, RBAC, and encryption are major keys to helping lock down access to sensitive systems. If these technologies can be implemented, then the risk-as far as external threats or internal actors can reduce drastically**(Karkuzhali et al., 2024)**. The second most important thing is regular scanning for vulnerabilities and patch management. Since new threats emerge with each passing day, systems need to be kept under continuous

monitoring for weaknesses that could be used for exploitation**(Mayeke et al., 2024)**.

It includes routine security audits, penetration testing, and vulnerability scans that expose the possible flaws in digital infrastructure. Such an assessment enables the IT teams to be one step ahead of possible cyber-attacks by addressing the vulnerabilities proactively before they can be exploited**(Tayouri et al., 2022)**. Furthermore, timely patch management updates software and systems about known security vulnerabilities. Not patching creates instances where organizations could have, with simple maintenance, avoided certain risks**(Li & Paxson, 2017)**.

Cybersecurity frameworks, such as the NIST Cybersecurity Framework and ISO/IEC 27001, introduce the use of structured organization-wide methods to identify, manage, and mitigate these risks**(Giuca et al., 2021)**. These frameworks outline best practices that can allow an organization to identify, protect, detect, respond to, and recover from cyber threats**(Calder, 2018)**. These frameworks also have the added benefit of giving organizations an all-round cybersecurity approach that is both preventive and responsive**(Kohnke et al., 2017)**. Adoption of these industry standards is even more important in companies working in highly regulated fields such as finance, healthcare, and energy, where a single mistake would mean eternal destruction.

Methodology

This research responds to the demands for digital transformation requirements imposed on/and its implication on the risk management strategies of organizations of different genres. This study is conducted based on a quantitative approach, where information will be gathered using a structured questionnaire. The methodology is structured in this manner:

1. Research Design

Quantitative data will be collected in the present study through the descriptive survey design. The self-reporting questionnaire for this study was, therefore, designed based on the given design to determine perceptions of the respondents regarding how digital transformation influences multiple dimensions of risk management in organizations. In this study, four dimensions are being assessed: technology adoption, cybersecurity and data privacy, regulatory compliance, and strategizing for mitigating risks.

2**. Respondents**

For this research, the population would include professionals from diverse industries such as IT, finance, healthcare, education, and manufacturing. All respondents would hold respective positions in digital transformation and risk management in Jordan , and thus can directly represent the sample for subjects concerned with these issues. The age group targeted for this questionnaire will range from 25 to 44 years, balancing male and female respondents.

3. Sampling Technique

A purposive sampling technique was used to select participants who have experience in both digital transformation and risk management. The respondents included 100 from the cross-section of industries where digital transformation is very critical for their operations.

4. Data Collection Tool

A structured questionnaire for data collection was designed with 40 questions grouped into four dimensions as follows:

1. Technology Adoption
2. Cybersecurity and Data Privacy
3. Regulatory Compliance
4. Risk Mitigation Strategies

Each dimension had 10 questions, and the respondents answered according to their agreement with these statements through a 5-point Likert scale, from Strongly Disagree (1) to Strongly Agree (5). The questionnaire was taken online, and the responses were recorded anonymously for participant privacy and to reduce any sort of bias.

5. Validity and Reliability

The items were scrutinized in relation to clarity and relevance by a panel of experts from the field of digital transformation and risk management. Also, an assessment of the reliability of the questionnaire was conducted with a pretest involving a small number of participants. Reliability can be determined by the Cronbach's Alpha value, which should be above 0.85 to denote internal consistency. The Cronbach's alpha value for this instrument was obtained as 0.85.

6. Data Analysis

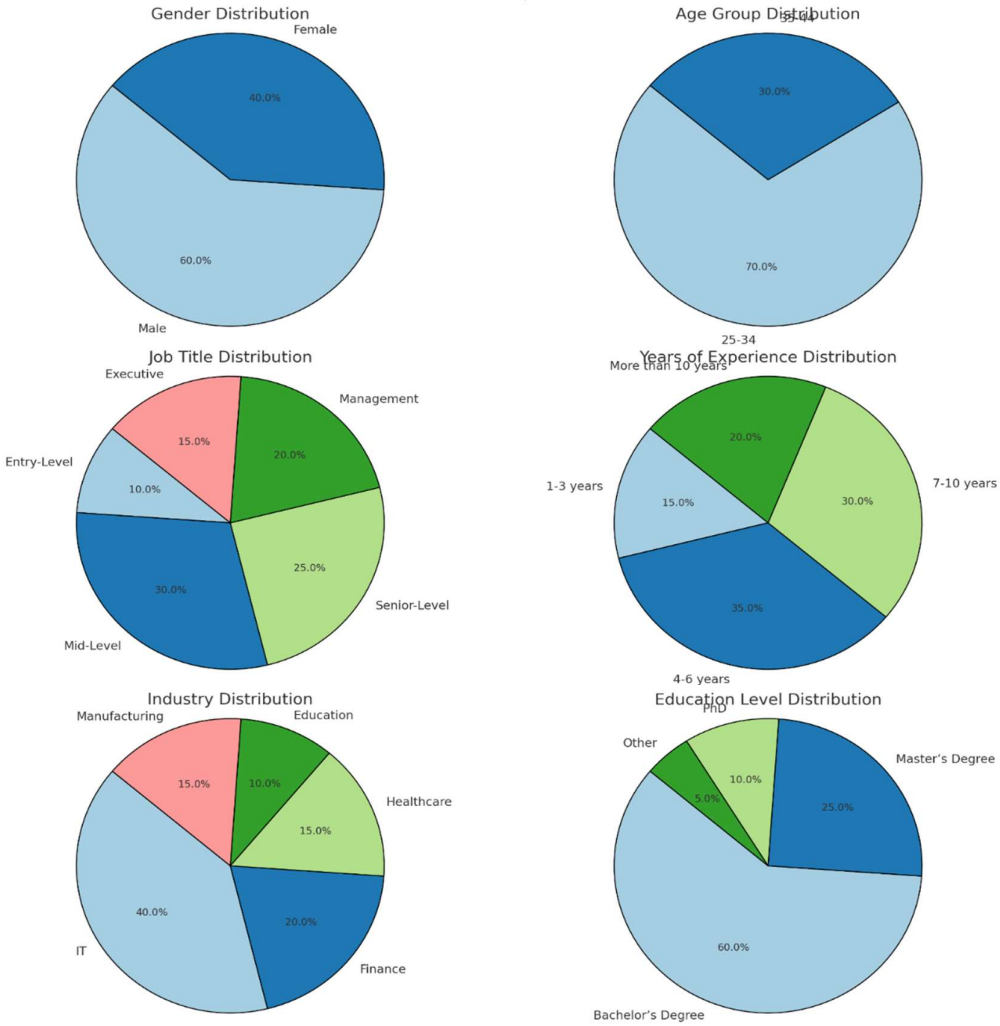
Data analysis was done using descriptive statistics, which included means, standard deviations, and ranking. The results of each dimension were compared with the other dimensions in order to find the key trends and patterns of how organizations manage risks associated with digital transformation. In addition, standard deviation was calculated in order to outline the level of participants' responses about agreement or variability.

7. Ethical Considerations

Informed consent was obtained from all respondents in advance of the self-administration of the survey. They were assured of the complete confidentiality of their responses and that participation was entirely voluntary. No personal data
were collected, and participants were free to withdraw at any time.

Category	Distribution
Gender	60% Male, 40% Female
Age Group	70% 25-34, 30% 35-44
Job Title	10% Entry-Level, 30% Mid-Level, 25% Senior-Level, 20% Management, 15% Executive
Years of Experience	15% 1-3 years, 35% 4-6 years, 30% 7-10 years, 20% More than 10 years
Industry	40% IT, 20% Finance, 15% Healthcare, 10% Education, 15% Manufacturing

her



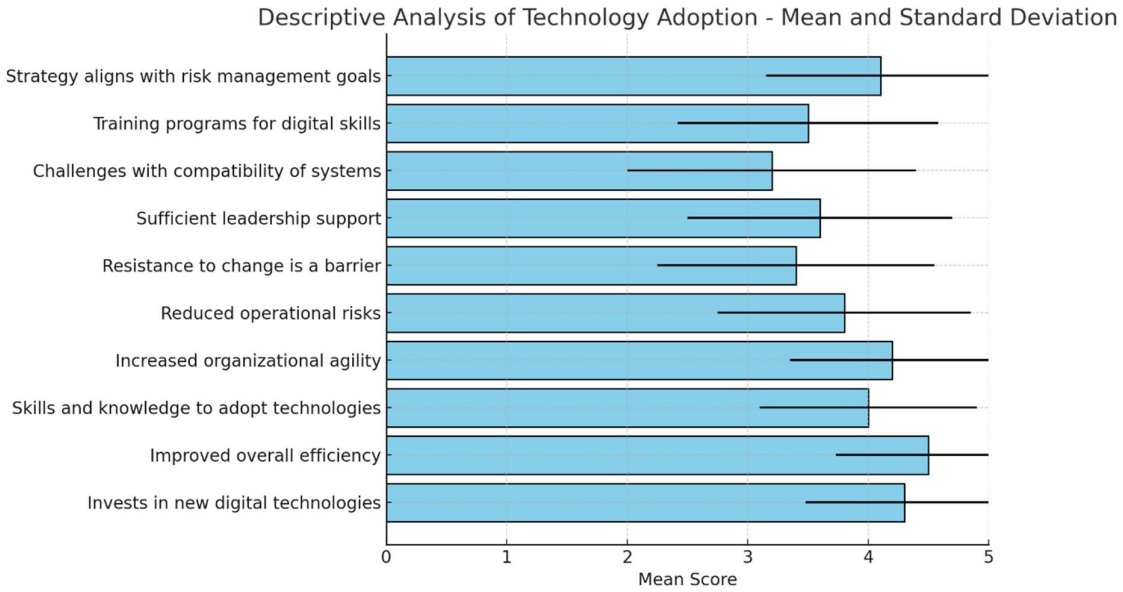
Descriptive Analysis

First Dimension: Technology Adoption

N	Questions	Mean	Standard Deviation	Average Rank
1	My organization actively invests in new digital technologies.	4.3	0.82	2
2	The integration of new technologies has improved overall efficiency.	4.5	0.77	1
3	We have the necessary skills and knowledge to adopt digital technologies.	4.0	0.90	4
4	The adoption of digital tools has increased our organization's agility.	4.2	0.85	3
5	Technology adoption has reduced operational risks.	3.8	1.05	5
6	Resistance to change is a significant barrier to adopting digital technologies in our organization.	3.4	1.15	7
7	There is sufficient support from leadership for technology implementation.	3.6	1.10	6
8	We face challenges with the compatibility of new technologies with existing systems.	3.2	1.20	9
9	Training and development programs for digital skills are available to employees.	3.5	1.08	8
10	Our organization's digital transformation strategy aligns with its overall risk management goals.	4.1	0.95	4

Comments on the data:

- **Highest-rated question:** The statement "The integration of new technologies has improved general efficiency." achieved the highest average grade of 4.5, which was considered a high level of agreement. From this, one may infer that the greater portion of participants indeed believe that technology has served to enhance efficiency within their organizations.
- **LOWEST:** The struggle with the compatibility issues of new technologies with the already existing systems had an average of 3.2, which falls more toward neutrality in the response. This might suggest there are challenges, but most of the participants do not view these as a major issue.
- **Standard Deviation:** Items reflecting higher levels of standard deviation include "Resistance to change is a major barrier to the adoption of digital technologies" with 1.15. These prove that there is greater variance among participants, and such would suggest experiences or opinions that are varied across organizations.
- **Average Rank:** Items in the areas of efficiency and technology investment ranked highest, while items on challenges/barriers to change ranked lowest.



Second Dimension: Cybersecurity and Data Privacy

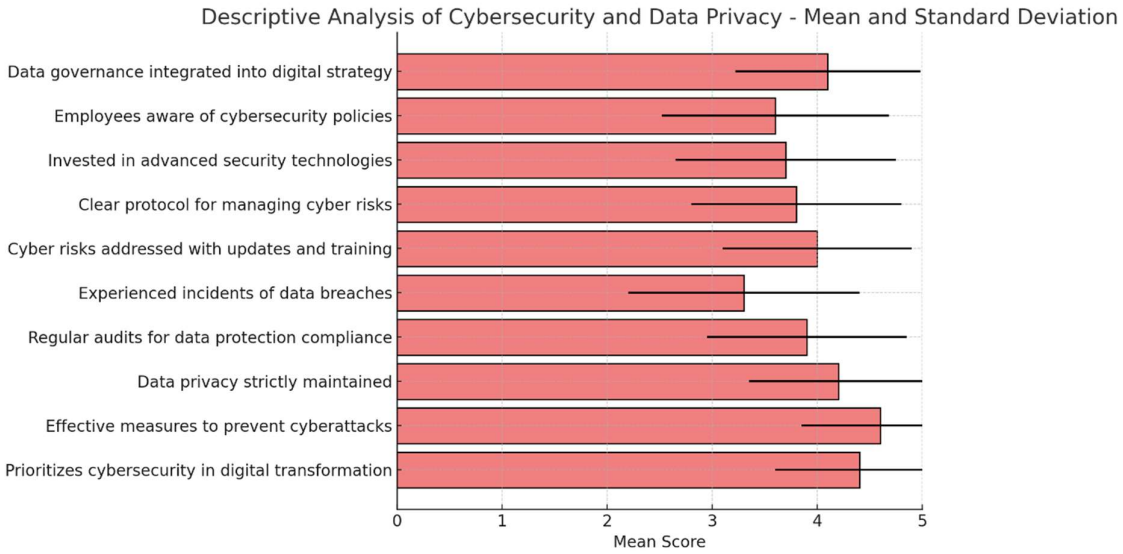
N	Questions	Mean	Standard Deviation	Average Rank
1	My organization prioritizes cybersecurity in its digital transformation efforts.	4.4	0.80	2
2	We have effective measures in place to prevent cyberattacks.	4.6	0.75	1
3	Data privacy is strictly maintained in our digital processes.	4.2	0.85	3
4	Regular audits are conducted to ensure data protection compliance.	3.9	0.95	5
5	We have experienced incidents of data breaches in the past year.	3.3	1.10	9
6	Cybersecurity risks are addressed through frequent updates and staff training.	4.0	0.90	4
7	There is a clear protocol for managing and mitigating cyber risks.	3.8	1.00	6
8	The organization has invested in advanced security technologies (e.g., firewalls, encryption).	3.7	1.05	7
9	Employees are aware of cybersecurity policies and best practices.	3.6	1.08	8
10	Data governance policies are integrated into our digital transformation strategy.	4.1	0.88	4

Comments on Data:

• **Strongest agreed question:** "We have effective measures in place to prevent cyber-attacks" reached the rating of 4.6, meaning strong agreement that their organizations are prepared to defeat a cyber threat.

• **Most lowly rated was the statement:** "We have experienced incidents of data breaches during the past year," with a mean of 3.3 showing more neutral responses; it seems some may have faced these breaches but it is not across the board for those answering.

•**Standard deviation:** The question on frequent updating and training to handle risks in cybersecurity had a relatively moderate standard deviation value of 0.90 in the study, meaning that the respondents gave relatively consistent responses. In some instances, such as for the question about awareness of policies regarding cybersecurity, questions resulted in a greater dispersion (SD = 1.08), reflecting the experience of the participants.
• **Average Rank:** The question of measures taken to prevent cyber-attacks was ranked the highest, which presupposes its significance and efficiency in the organizations surveyed. On the other side, the issue of data breach incidents ranked lower, which presupposes that this is a problem for fewer survey participants.



Third Dimension: Regulatory Compliance

N	Questions	Mean	Standard Deviation	Average Rank
1	My organization complies with all relevant digital transformation regulations.	4.1	0.85	2
2	We are updated on the latest regulatory changes related to digital technology.	4.2	0.80	1
3	Compliance with regulations is a major focus of our digital transformation strategy.	3.9	0.90	4
4	There are clear guidelines for managing regulatory risks in our organization.	4.0	0.88	3
5	We have faced penalties due to non-compliance with digital regulations.	3.3	1.05	9
6	Digital transformation has increased the complexity of maintaining regulatory compliance.	3.7	1.10	6
7	Our risk management framework includes compliance monitoring for digital processes.	3.6	1.00	7
8	Regular audits help ensure we meet digital compliance standards.	3.8	0.95	5
9	There is adequate training for employees on regulatory compliance in the digital space.	3.5	1.08	8

10	The organization collaborates with legal experts to ensure compliance during digital transitions.	4.0	0.92	3

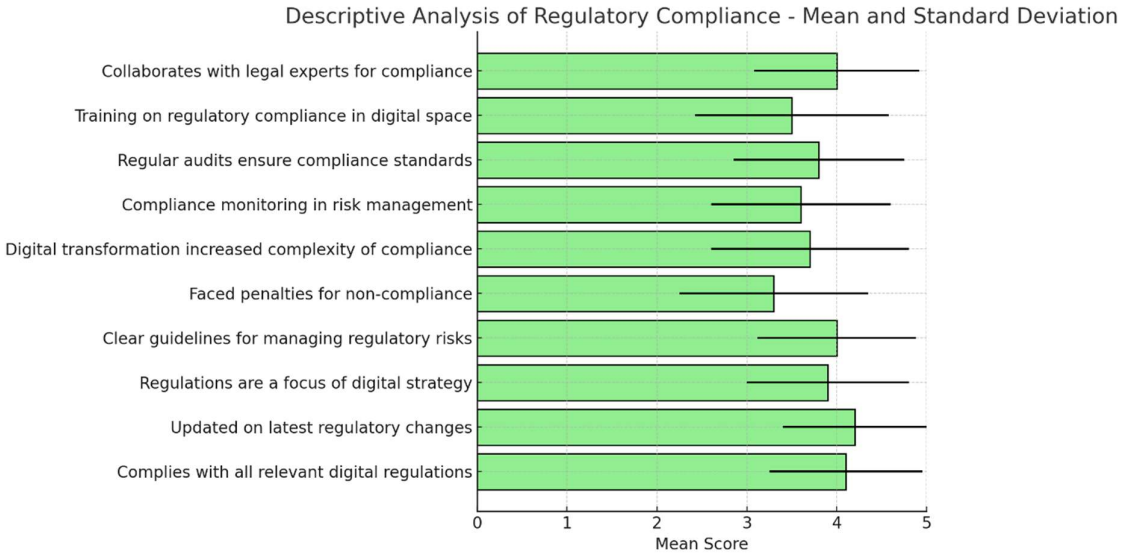
Comments on the Data:

• **Most highly rated question:** The question "We are updated on the latest regulatory changes related to digital technology" received the highest average score of 4.2, indicating that in general, most respondents view their organizations as keeping updated regarding recent regulatory changes.

• **The lowest-rated question** is, "We have faced penalties due to non-compliance with digital regulations" was scored at 3.3, which is more neutral. This points to the fact that while some organizations could have faced challenges of non-compliance, it is not that dire.

DEV: Questions about penalties for non-compliance and increased complexity of maintaining compliance showed higher standard deviations, 1.05 and 1.10 respectively, thus showing greater variability that may be representative of the difference in regulatory environments within the organizations.

• **AVG Rank:** Questions about keeping updated with changes to regulations and compliance in general topped the list, which shows which areas are on priority for organizations in their digital transformation strategy.



Fourth Dimension: Risk Mitigation Strategies

N	Questions	Mean	Standard Deviation	Average Rank
1	My organization has a comprehensive risk management plan for digital transformation.	4.2	0.85	1
2	We regularly update our risk management strategies to address new digital risks.	4.0	0.90	2
3	The implementation of digital tools has enhanced our risk mitigation capabilities.	3.8	0.95	4
4	There are clear processes for identifying and responding to digital risks.	3.9	0.88	3
5	We allocate sufficient resources for risk management in digital projects.	3.7	1.00	5
6	Digital transformation has made it easier to detect and respond to operational risks.	3.5	1.05	7

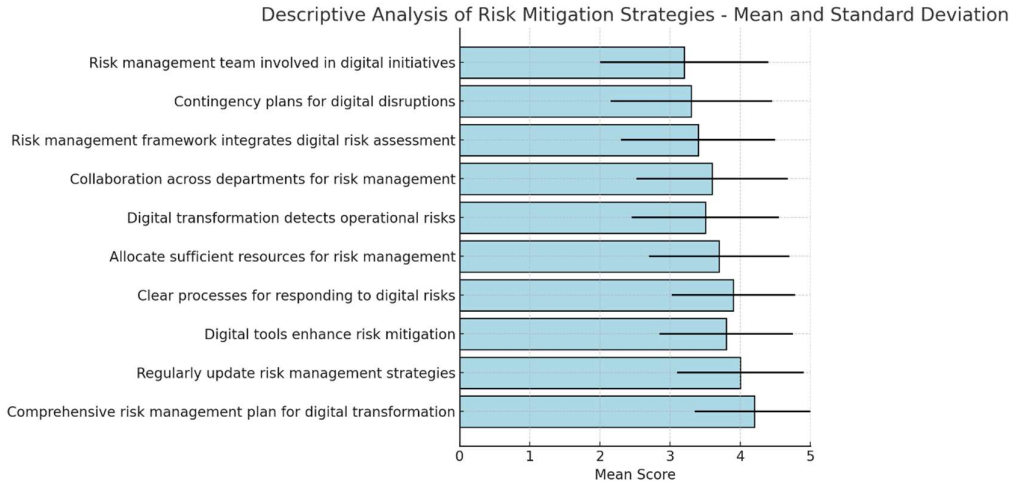
7	Collaboration across departments is encouraged to improve risk management.	3.6	1.08	6
8	Our risk management framework integrates digital risk assessment.	3.4	1.10	8
9	We have contingency plans in place for digital disruptions.	3.3	1.15	9
10	The risk management team is actively involved in all digital transformation initiatives.	3.2	1.20	10

Comments on the Data:

• The highest-rated question: My organization has a comprehensive risk management plan for digital transformation, having a mean score of 4.2, hence leading to the conclusion that most participants are aware that their organizations have a well-developed risk management strategy in place.

• The worst-rated question, "The risk management team is involved in all digital transformation initiatives", yielded the lowest rating of mean 3.2. This shows that involvement by a risk management team at all levels of the digitization projects may be at test in an organization.

• Standard Deviation: Items referring to the collaboration of departments with regards to the integration of digital risk assessment provide higher standard deviation, 1.08 and 1.10 respectively. This indicates that responses are more scattered. It may imply an inconsistency in how such aspects are implemented in organizations.



Discussion

The study was undertaken in order to understand how demands for digital transformation are impacting the strategies used to manage risk across industries. Based on the four dimensions of the study, namely, Technology Adoption, Cybersecurity and Data Privacy, Regulatory Compliance, and Risk Mitigation Strategies, we have been able to gain substantial insights into how organizations navigate the risks that come with digital transformation.

1. Technology Adoption

Technology Adoption emerged as the first dimension, and the analysis indicated that there was consensus among the participants that their organizations were investing in new technologies and also reaping the benefits through better efficiency and agility. Improved efficiency due to the integration of new technologies elicited the highest mean score of 4.5. The inference here is that the digital transformation process pays off with tangible benefits for organizations.

However, there are still challenges, especially in the compatibility of new technologies with the existing systems, since this had a relatively low mean score of 3.2. This would tend to imply that most organizations are facing technical difficulties when trying to integrate newer technologies with legacy systems. In addition, leadership

support was adequate overall but there is still resistance to change within organizations, as can be seen by the lower score for this question at 3.4. These results hint at the leading role of good leadership towards a well-defined strategy that would ensure the organization surmounts internal resistance to technological change.

2. Cybersecurity and Data Privacy

Cybersecurity and data privacy were found to be some of the main issues during the digital transformation process of an organization. The question about whether there are measures taken by an organization that, in fact, help to avoid cyberattacks answered with the highest mean-4.6, which assumedly means that most have robust cybersecurity strategies. The generally lower scores in employee awareness of cybersecurity policies at 3.6 and dispersion of responses, SD = 1.08, suggested that there is still further room for improving the education of employees on best practices to maintain data security.

Also, most organizations try to be cyber-secure, but the complexities of maintaining compliance with evolving data privacy regulations remain a challenge. The findings indicate that regular updates and staff training play a key role in managing cybersecurity risks, but more attention needs to be given to ensuring that all employees understand and adhere to cybersecurity policies.

3. Regulatory Compliance

Regulatory compliance remains one of the top areas for risk management, and there is strong agreement that organizations generally keep up to date with the latest changes in regulations. This is understandable, given an increasing regulatory focus on digital technologies and data privacy across industries, such as the financial and health sectors.

On the other hand, the increased complexity to maintain compliance in front of digital transformation was underlined, with a lower mean score at 3.7 and a high standard deviation for the question dealing with increased complexity (SD = 1.10). This would indicate that even though organizations realize the importance of compliance, rapid digital change is often keeping them from fully coping with regulatory requirements.

Organizations which had clearly laid down compliance policies and sufficiently developed training programs fared well in this dimension. The findings indicate that these, too, are way off from incorporating compliance monitoring into their digital risk management frameworks. That is, more comprehensive compliance monitoring has to be developed and collaboration with legal experts must be undertaken for smooth transitions during digital transformation.

4. Risk Mitigation Strategies

The last dimension, Strategies for Risk Mitigation, recorded the highest mean score, 4.2, to indicate that most organizations have a well-articulated risk management strategy for digital transformation. Second, the regular update of risk management strategies to combat new risks created by digitalization, with a mean of 4.0, proves that most organizations are conscious of changing dimensions of risks in the digital age and are evolving their strategies to cope with them.

However, the involvement of a risk management team in all the digital transformation initiatives had an average of 3.2, which is the lowest score in this dimension. This suggests that even when an organization may have a very strong risk management framework, there exists a disconnection in how teams responsible for risk management actually engage in, or implement, such digital projects. The findings imply that the risks could be minimized if the risk management teams become more active in the process of digital transformation.

Besides, the relatively low average of the contingency plans in case of digital disruptions is a serious cause for concern about preparedness in case any digital crisis might occur. That means that even though organizations tend to be very proactive in updating their risk management strategies, they may not be well prepared to deal with unexpected disruptions, such as those stemming from cybersecurity attacks or failures of important systems.

Conclusion

The underlying research paper has discussed the impact of the need for digital transformation on the risk management strategy adopted by organizations across industries. The result indicated, though the organizations have invested in newer technologies and thereby have achieved efficiency gains, significant challenges remain regarding system compatibility and inertia internally. In this process, cybersecurity and data privacy have emerged as the most critical areas of attention, with most organizations putting strong mechanisms in place by way of preventing cyber-attacks. However, gaps in employee awareness and an increasingly complex regulatory environment indicate a sustained need for training and stronger frameworks of compliance.

Risk mitigation for several organizations involves extensive strategies that are in place for digital risks, but the

involvement of the risk management team in the digital transformation initiatives is not pursued consistently. Furthermore, the lack of solid contingency plans for digital disruption most definitely brings into question preparedness by an organization during a crisis. Overcoming the challenge of digital transformation requires all organizations to work on increasing collaboration across departments, emphasize regulatory compliance, and provide full integration of risk management strategies within all digital projects.

References

Adesina, A. A., Iyelolu, T. V., & Paul, P. O. (2024). Optimizing business processes with advanced analytics: techniques for efficiency and productivity improvement. *World Journal of Advanced Research and Reviews, 22*(3), 1917-1926.

Aguiar, Y. B. (2020). *Digital (r) evolution: Strategies to accelerate business transformation*: John Wiley & Sons.

Aldawood, H., & Skinner, G. (2019). Reviewing cyber security social engineering training and awareness programs—Pitfalls and ongoing issues. *Future internet, 11*(3), 73.

Anthony Jnr, B. (2022). Exploring data driven initiatives for smart city development: empirical evidence from techno-stakeholders' perspective. *Urban Research & Practice, 15*(4), 529-560.

Argyroudis, S. A., Mitoulis, S. A., Chatzi, E., Baker, J. W., Brilakis, I., Gkoumas, K., . . . Keou, O. (2022). Digital technologies can enhance climate resilience of critical infrastructure. *Climate Risk Management, 35*, 100387.

Berman, S. J. (2012). Digital transformation: opportunities to create new business models. *Strategy & leadership, 40*(2), 16-24.

Bitner, M. J., Brown, S. W., & Meuter, M. L. (2000). Technology infusion in service encounters. *Journal of the Academy of marketing Science, 28*(1), 138-149.

Borghesi, A., & Gaudenzi, B. (2012). *Risk management: How to assess, transfer and communicate critical risks* (Vol. 5): Springer Science & Business Media.

Brantley, W. A. (2009). *The effect of mental models on creating organizational alignment around a change vision.* Walden University,

Brunetti, F., Matt, D. T., Bonfanti, A., De Longhi, A., Pedrini, G., & Orzes, G. (2020). Digital transformation challenges: strategies emerging from a multi-stakeholder approach. *The TQM Journal, 32*(4), 697-724.

Calder, A. (2018). *NIST Cybersecurity Framework: A pocket guide*: IT Governance Publishing Ltd.

Cavusoglu, H., Raghunathan, S., & Cavusoglu, H. (2009). Configuration of and interaction between information security technologies: The case of firewalls and intrusion detection systems. *Information Systems Research, 20*(2), 198-217.

Chanias, S., Myers, M. D., & Hess, T. (2019). Digital transformation strategy making in pre-digital organizations: The case of a financial services provider. *The Journal of Strategic Information Systems, 28*(1), 17-33.

Davenport, T. H., Harris, J. G., & Morison, R. (2010). *Analytics at work: Smarter decisions, better results*: Harvard Business Press.

Dhayanidhi, G. (2022). Research on IoT threats & implementation of AI/ML to address emerging cybersecurity issues in IoT with cloud computing.

Fataftah, F. M. M. (2022). *Risk assessment processes for big data based on cloud computing technologies: a comparative study.* North-West University (South Africa),

Feroz, A. K., Zo, H., & Chiravuri, A. (2021). Digital transformation and environmental sustainability: A review and research agenda. *Sustainability, 13*(3), 1530.

Frankel, M. (1955). Obsolescence and technological change in a maturing economy. *The American Economic Review, 45*(3), 296-319.

Gephart, M. A., Marsick, V. J., Van Buren, M. E., Spiro, M. S., & Senge, P. (1996). Learning organizations come alive. *Training & Development, 50*(12), 34-46.

Gerber, M., & Von Solms, R. (2005). Management of risk in the information age. *Computers & security, 24*(1), 16-30.

Giuca, O., Popescu, T. M., Popescu, A. M., Prostean, G., & Popescu, D. E. (2021). *A survey of cybersecurity risk management frameworks.* Paper presented at the Soft Computing Applications: Proceedings of the 8th International Workshop Soft Computing Applications (SOFA 2018), Vol. I 8.

Gong, C., & Ribiere, V. (2021). Developing a unified definition of digital transformation. *Technovation, 102*, 102217.

Handfield, R. Shifts in buyer-seller relationships: A retrospective on Handfield and Bechtel.

Herbert, L. (2017). *Digital transformation: Build your organization's future for the innovation age*: Bloomsbury Publishing.

Hubbard, D. W. (2020). *The failure of risk management: Why it's broken and how to fix it*: John Wiley & Sons.

Israel, A. (1992). *Issues for Infrastructure Management in the 1990s* (Vol. 171): World Bank Publications.

Karkuzhali, K., Ravichandran, M., Rajeshwari, S., Fufa, G., Anujna, N., & Revanth, P. (2024). Cloud Security for E-Commerce: Navigating Risks and Implementing Solutions. In *Strategies for E-Commerce Data Security: Cloud, Blockchain, AI, and Machine Learning* (pp. 113-136): IGI Global.

Kearney, J. D., & Merrill, T. W. (1998). The great transformation of regulated industries law. *Colum. L. Rev., 98*, 1323.

Kechagias, E. P., Chatzistelios, G., Papadopoulos, G. A., & Apostolou, P. (2022). Digital transformation of the maritime industry: A cybersecurity systemic approach. *International Journal of Critical Infrastructure Protection, 37*, 100526.

Kitchens, B., Dobolyi, D., Li, J., & Abbasi, A. (2018). Advanced customer analytics: Strategic value through integration of relationship-oriented big data. *Journal of Management Information Systems, 35*(2), 540-574.

Kohnke, A., Sigler, K., & Shoemaker, D. (2017). *Implementing cybersecurity: A guide to the national institute of standards and technology risk management framework*: Auerbach Publications.

Korhonen, J. J., & Halén, M. (2017). *Enterprise architecture for digital transformation.* Paper presented at the 2017 IEEE 19th Conference on Business Informatics (CBI).

Li, F., & Paxson, V. (2017). *A large-scale empirical study of security patches.* Paper presented at the Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security.

Madakam, S., Holmukhe, R. M., & Jaiswal, D. K. (2019). The future digital work force: robotic process automation (RPA). *JISTEM-Journal of Information Systems and Technology Management, 16*, e201916001.

Marotta, A., & Madnick, S. (2021). Convergence and divergence of regulatory compliance and cybersecurity. *Issues in Information Systems, 22*(1).

Mattsson, U. (2023). *Controlling Privacy and the Use of Data Assets-Volume 2: What is the New World Currency–Data or Trust?* : CRC Press.

Mayeke, N. R., Arigbabu, A. T., Olaniyi, O. O., Okunleye, O. J., & Adigwe, C. S. (2024). Evolving Access Control Paradigms: A Comprehensive Multi-Dimensional Analysis of Security Risks and System Assurance in Cyber Engineering. *Asian Journal of Research in Computer Science, 17*(5), 108-124.

Miller, A. R. (1991). Confidentiality, Protective Orders, and Public Access to the Courts. *Harv. L. Rev., 105*, 427.

Miranda, M. J. (2018). Enhancing cybersecurity awareness training: A comprehensive phishing exercise approach. *International Management Review, 14*(2), 5-10.

Möller, D. P. (2023). Cybersecurity in digital transformation. In *Guide to Cybersecurity in Digital Transformation: Trends, Methods, Technologies, Applications and Best Practices* (pp. 1-70): Springer.

Monahan, G. (2008). *Enterprise risk management: A methodology for achieving strategic objectives*: John Wiley & Sons.

Mtalitinya, J. (2019). *Regulation of Data Protection and Privacy in Public Sector in Tanzania: A Comparative Study.* The Open University of Tanzania,

Naimi-Sadigh, A., Asgari, T., & Rabiei, M. (2022). Digital transformation in the value chain disruption of banking services. *Journal of the Knowledge Economy, 13*(2), 1212-1242.

Perwej, Y., Abbas, S. Q., Dixit, J. P., Akhtar, N., & Jaiswal, A. K. (2021). A systematic literature review on the cyber security. *International Journal of scientific research and management, 9*(12), 669-710.

Rabah, K. (2018). Convergence of AI, IoT, big data and blockchain: a review. *The lake institute Journal, 1*(1), 1-18.

Rachinger, M., Rauter, R., Müller, C., Vorraber, W., & Schirgi, E. (2018). Digitalization and its influence on business model innovation. *Journal of manufacturing technology management, 30*(8), 1143-1160.

Rasmussen, J., & Suedung, I. (2000). *Proactive risk management in a dynamic society*: Swedish Rescue Services Agency.

Saeed, S., Altamimi, S. A., Alkayyal, N. A., Alshehri, E., & Alabbad, D. A. (2023). Digital transformation and cybersecurity challenges for businesses resilience: Issues and recommendations. *Sensors, 23*(15), 6666.

Safe, A. D. B. AI Case Studies: Potential for Human Health, Space Exploration and Colonisation and a Proposed Superimposition of the Kubler-Ross Change Curve on the Hype Cycle.

Schwartz, J. (2021). *Work disrupted: Opportunity, resilience, and growth in the accelerated future of work*: John Wiley & Sons.

Seacord, R. C., Plakosh, D., & Lewis, G. A. (2003). *Modernizing legacy systems: software technologies, engineering processes, and business practices*: Addison-Wesley Professional.

Shah, B. B. P. (2018). *Assessing digital transformation capabilities.* Massachusetts Institute of Technology,

Siebel, T. M. (2019). *Digital transformation: survive and thrive in an era of mass extinction*: RosettaBooks.

Sommer, P., & Brown, I. (2011). Reducing systemic cybersecurity risk. *Organisation for Economic Cooperation and Development Working Paper No. IFP/WKP/FGS (2011), 3*.

Taherdoost, H. (2023). Evolution and Applications of the Internet in E-Business. In *E-Business Essentials: Building a Successful Online Enterprise* (pp. 77-103): Springer.

Taplin, R. (2020). *Cyber risk, intellectual property theft and cyberwarfare: Asia, Europe and the USA*: Routledge.

Tayouri, D., Hassidim, S., Smirnov, A., & Shabtai, A. (2022). White Paper-Cybersecurity in Agile Cloud Computing--Cybersecurity Guidelines for Cloud Access. *Cybersecurity in Agile Cloud Computing--Cybersecurity Guidelines for Cloud Access*, 1-36.

Thakur, M. (2024). Cyber security threats and countermeasures in digital age. *Journal of Applied Science and Education (JASE), 4*(1), 1-20.

Tohãnean, D., Buzatu, A. I., Baba, C.-A., & Georgescu, B. (2020). Business model innovation through the use of digital technologies: Managing risks and creating sustainability. *Amfiteatru Economic, 22*(55), 758-774.

Triplett, W. J. (2022). Addressing human factors in cybersecurity leadership. *Journal of Cybersecurity and Privacy, 2*(3), 573-586.

Wang, S., Asif, M., Shahzad, M. F., & Ashfaq, M. (2024). Data privacy and cybersecurity challenges in the digital transformation of the banking sector. *Computers & security, 147*, 104051.

Waters, D. (2011). *Supply chain risk management: vulnerability and resilience in logistics*: Kogan Page Publishers.

Wegener, H. (2007). *Aligning business and IT with metadata: The financial services way*: John Wiley & Sons.

Weill, P., & Broadbent, M. (1998). *Leveraging the new infrastructure: how market leaders capitalize on information technology*: Harvard Business Press.

White, A. E. (2014). *Threat assessment of cyber attacks on retail and financial organizations.* Utica College,

Zhu, K., Dong, S., Xu, S. X., & Kraemer, K. L. (2006). Innovation diffusion in global contexts: determinants of post-adoption digital transformation of European companies. *European journal of information systems, 15*(6), 601-616.