ТЕХНОЛОГИЧНИ РИСКОВЕ ОТ ДИГИТАЛИЗАЦИЯТА В НЕАКАДЕМИЧНА СРЕДА

TECHNOLOGICAL RISKS OF DIGITALIZATION IN NON-ACADEMIC ENVIRONMENT

Мариана Ковачева [1]
e-mail: mkovacheva@unwe.bg [1]

Абстракт

Дигитализацията се превръща в определяща характеристика на организационната трансформация, простирайки се отвъд академичните институции в бизнеса, правителството и секторите на обществените услуги. Макар че повишава ефективността, иновациите и свързаността, едновременно с това въвежда нови категории технологични рискове, които заплашват оперативната стабилност, целостта на данните и етичното управление. Този доклад разглежда технологичните рискове от дигитализацията в неакадемична среда чрез структурирана класификация на осем категории: заплахи за киберсигурността, рискове за поверителността на данните, системни повреди и прекъсвания, загуба на контрол над цифровите умения, етични и алгоритмични рискове, зависимост от доставчици и платформи, съкращения на работни места и правни и регулаторни предизвикателства. Въз основа на рамката за управление на риска ISO 31000:2018, изследването предоставя систематичен анализ на това как тези рискове могат да бъдат идентифицирани, анализирани и смекчени. Заключенията подчертават, че управлението на технологичните рискове изисква не само технически решения, но и социална, етична и организационна адаптация. Докладът предлага всеобхватна концептуална рамка, с което допринася за подобряване на осведомеността за риска, устойчивостта и отговорното цифрово управление в неакадемичните институции.

Abstract

Digitalization has become a defining characteristic of organizational transformation, extending beyon d academic institutions into business, government, and public service sectors. While it enhances efficie ncy, innovation, and connectivity, it simultaneously introduces new categories of technological risks th at threaten operational stability, data integrity, and ethical governance. This paper examines the tech nological risks of digitalization in non-academic environments through a structured classification of e ight categories: cybersecurity threats, data privacy risks, system failures and downtime, loss of digital skills control, ethical and algorithmic risks, dependency on vendors and platforms, job displacement, a nd legal and regulatory challenges. Drawing upon the ISO 31000:2018 risk management framework, t he study provides a systematic analysis of how these risks can be identified, analyzed, and mitigated. T he findings underscore that managing technological risks requires not only technical solutions but als o social, ethical, and organizational adaptation. By offering a comprehensive conceptual framework, t he paper contributes to improving risk awareness, resilience, and responsible digital governance in no n-academic institutions.

Ключови думи: digitalization, technological risks, non-academic environment

JEL: C88, L86

Introduction

In today’s fast developing world where new technologies emerge every day and integrate in more aspects of our lives, the risks connected to them are also expanding. Non-academic institutions

[1] Гл. ас. д-р към катедра ИТК, УНСС, email: mkovacheva@unwe.bg

are such that do not focus on education, research or some scholarly activities, but they operate in other important areas of society, business and public life.

The digitalization is happening in every sphere around us and helps immensely in developing and integrating digital technologies into all areas of a business. There is a great importance in studying the technological risks in non-academic environments because even that digitalization is offering innovation, efficiency and speed, also introduces threats, dependency and vulnerability that can threaten the stability of business organizations. Understanding these emerging risks will help balance the innovation with security, and will ensure that digital system will remain reliable, ethical and sustainable.

This paper explores eight categories of technological risks which are arising from digitalization outside of academia. The defined groups are as follows: cybersecurity threats, data privacy risks, system failures and downtime, loss of digital skills control, ethical and algorithmic risks, dependency on vendors and platforms, job displacement, and legal and regulatory challenges.

Conceptual background

Digital transformation has become a defining force in modern organizations, yet it is important to distinguish between digitization and digitalization. Digitization refers to the technical conversion of analog information into digital formats - for example, scanning documents or automating data entry. [1] Digitalization, on the other hand, involves a broader social and organizational process that integrates digital technologies into everyday operations, fundamentally altering how value is created, communicated, and managed.[2] In non-academic environments - such as business enterprises, government institutions, and healthcare systems - digitalization extends beyond technology adoption to include process redesign, data-driven decision-making, and cultural adaptation. While it offers efficiency and innovation, it simultaneously introduces new categories of technological risk that can disrupt operations, compromise data integrity, and create ethical or regulatory challenges.

On the other hand, technological risk refers to the potential for adverse outcomes resulting from the design, implementation, or use of technology. It encompasses failures of systems or infrastructures as well as unintended human, ethical, or organizational consequences. These risks often stem from the uncertainty that accompanies innovation and from the interdependence of digital systems within complex socio-technical environments. In non-academic contexts, technological risks include technical failures, cybersecurity incidents, data privacy breaches, and ethical issues arising from algorithmic decision-making. They also encompass human factors such as skill obsolescence, organizational dependency on external vendors, and social effects like job displacement. Recognizing these diverse dimensions underscores that technological risk is not purely a technical matter but a multidimensional issue combining social, ethical, and operational factors.

When digital transformation progresses more rapidly than organizational structures or human competencies can adjust, this equilibrium is disrupted, leading to a higher probability of system failures, human errors, and the decomposition of digital skills. Consequently, managing technological risk extends beyond implementing technical safeguards - it also requires social adaptation, continuous training, and inclusive design practices that ensure people and technology evolve together. [11]

The ISO 31000:2018 framework offers a globally recognized standard for systematic risk management. It defines risk as the effect of uncertainty on objectives and outlines a continuous process of identification, analysis, evaluation, and treatment. Applying ISO 31000 principles to technological risks ensures a structured and comparable approach to their management. Within non-academic environments, this process enables organizations to identify digital vulnerabilities, assess their potential impact, and implement appropriate mitigation strategies - ranging from cybersecurity protocols to vendor oversight and employee training. [3]

In non-academic environments, digitalization transforms how organizations operate, interact with stakeholders, and deliver services. Businesses leverage digital tools for analytics and automation, governments deploy digital platforms for public service delivery, and healthcare institutions integrate electronic systems for patient management. However, these benefits also amplify exposure to technological uncertainty - manifesting as cybersecurity threats, data privacy violations, or system dependencies.

Unlike academic institutions, non-academic organizations face direct market pressures, competitive dynamics, and regulatory obligations. These contextual factors heighten the significance of managing technological risk not only to protect assets but also to ensure operational resilience and legal compliance. Effective risk governance thus requires integrating technological foresight with ethical, legal, and social considerations, supported by international frameworks such as ISO 31000.

Classification of technological risks

All types of organizations increasingly rely on technologies and are becoming more digitalized. The eight categories of technological risks were defined through a literature-based classification review. The method of definition involved a review of academic publications – papers, articles, industry reports, etc. which addressed the technological risks associated with digitalization in non-academic environment. Similar groups were grouped under broader conceptual categories. The classification reflects both theoretical insights and practical observations taken from various non-academic sectors and organizations in them.

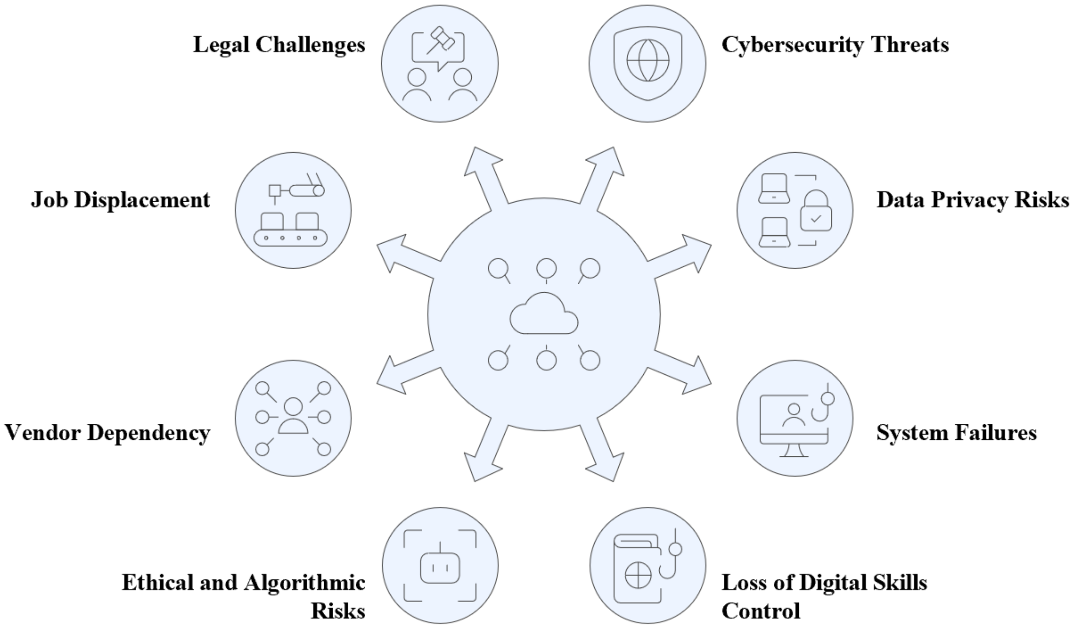

Figure 3 Categories of technological risks

The eight categories of technological risks in non-academia shown on Figure 1 are the following: cybersecurity threats, data privacy risks, system failures and downtime, loss of digital skills control, ethical and algorithmic risks, dependency on vendors and platforms, job displacement, and legal and regulatory challenges.

The classification of technological risks in this paper aligns with the ISO 31000:2018 risk management process, which emphasizes the systematic steps of risk identification, analysis, and evaluation. Each of the eight categories - such as cybersecurity, data privacy, and technological dependency, etc. - represents a key dimension of uncertainty that can affect organizational objectives in non-academic environments. By structuring the classification according to ISO 31000 principles, the framework ensures that risks are recognized in a comprehensive and comparable manner, supporting both academic analysis and practical application within established international risk management standards. [3]

Table 1 illustrates how the eight identified technological risk categories align with the stages of the ISO 31000:2018 risk management process. This integration ensures that the classification not only organizes risks conceptually but also provides a structured approach for identifying, analyzing, and managing them within non-academic environments. [3]

ISO 31000:2018 Process Stage	**Description (according to ISO 31000)**	**Application to the Eight Technological Risk Categories**
1.Risk Identification	Recognize and describe risks that could affect the achievement of objectives.	Identify the main sources of technological risk: **cybersecurity threats**, **data privacy risks**, **system failures and downtime**, **loss of digital skills control**, **ethical and algorithmic risks**, **dependency on vendors and platforms**, **job displacement**, and **legal and regulatory changes**.
2. Risk Analysis	Understand the nature, sources, likelihood, and potential consequences of each risk.	Analyse how each risk operates and interacts - for instance, the likelihood of **cyberattacks**, the severity of **data breaches**, the operational impact of **system failures**, or the social implications of **algorithmic bias** and **job displacement**.
3.Risk Evaluation	Compare analysed risks against defined criteria to determine their significance.	Prioritize which risks require the most urgent response. For example, **cybersecurity** and **data privacy** may pose immediate high-impact threats, while **dependency on vendors** and **legal changes** may represent longer-term strategic risks.
4.Risk Treatment	Develop and implement measures to mitigate, transfer, accept, or avoid risks.	Apply appropriate mitigation strategies: enhance **cybersecurity protocols**, strengthen **data governance**, establish **redundancy for system continuity**, provide **continuous digital skills training**, ensure **ethical AI oversight**, and plan for **regulatory compliance** and **workforce transition**.
5.Monitoring and Review	Continually assess the effectiveness of risk controls and adapt to change.	Regularly review and update controls as technologies evolve - for example, reassessing **vendor dependencies**, **AI ethics compliance**, and **cyber defence mechanisms**.
6.Communication and Consultation	Maintain stakeholder engagement and transparency throughout the risk process.	Ensure clear communication across technical teams, management, legal advisors, and employees to build a shared understanding of each technological risk and its mitigation.

Table 4 Technological risks aligned with ISO 310000:2018

- **Cybersecurity Threats**

Definition:

Cybersecurity threats refer to malicious digital actions that compromise the confidentiality, integrity, or availability of data and systems. These include cyberattacks such as phishing, ransomware, and unauthorized access that exploit vulnerabilities in networks and digital infrastructures.

Causes and Contributing Factors:

Key contributors include increased connectivity, inadequate security protocols, outdated software, and limited employee awareness. The rise of remote work in non-academic environment and the Internet of Things (IoT) has expanded attack surfaces, making organizations more exposed. [4] [5]

Impacts and Consequences:

Cyber incidents can cause data breaches, financial losses, operational disruptions, and reputational damage. In critical sectors, they may endanger service continuity or public safety, and often result in legal liabilities and regulatory penalties. [4]

- **Data Privacy Risks**

Definition:

Data privacy risks arise from the improper collection, storage, sharing, or use of personal or sensitive information. They concern both compliance with privacy laws and the ethical handling of digital data.

Causes and Contributing Factors:

Contributors include weak data governance, lack of transparency, and excessive data collection by organizations. Inadequate encryption, third-party data sharing, and poor user consent practices also elevate the risk. [5]

Impacts and Consequences:

Privacy violations lead to loss of individual trust, legal sanctions under regulations such as GDPR, and reputational harm. For organizations, breaches may disrupt operations and erode customer relationships. [5]

- **System Failures and Downtime**

Definition:

System failures and downtime refer to interruptions in digital infrastructure that halt or degrade the performance of critical systems, applications, or services.

Causes and Contributing Factors:

Common causes include software bugs, power outages, hardware malfunctions, or human error. Overreliance on automated systems and lack of redundancy amplify the likelihood and duration of failures. [6]

Impacts and Consequences:

Consequences include productivity loss, revenue reduction, and service unavailability. In sectors like healthcare or finance, system downtime can have severe operational or safety implications. It may also expose weaknesses in business continuity planning. [6]

- **Loss of Digital Skills Control**

Definition:

Loss of digital skills control refers to the decline or mismatch of employees’ technological competencies relative to rapidly changing digital tools and systems.

Causes and Contributing Factors:

Rapid digital transformation, insufficient training, and reliance on outsourced IT functions reduce in-house skill retention. Frequent software updates or platform shifts can outpace employee adaptation. [7]

Impacts and Consequences:

A digital skills gap limits innovation increases dependency on vendors, and heightens vulnerability to misuse or error. It can lower productivity, employee confidence, and the overall resilience of the organization. [7]

- **Ethical and Algorithmic Risks**

Definition:

Ethical and algorithmic risks emerge from the design and use of automated systems, especially those employing artificial intelligence or machine learning, which may produce biased or opaque outcomes. [8]

Causes and Contributing Factors:

These risks arise from biased training data, lack of ethical oversight, and insufficient transparency in algorithmic decision-making. Pressure for efficiency can override ethical considerations.

Impacts and Consequences:

Consequences include unfair treatment, discrimination, and loss of public trust. Biased algorithms can damage reputations, violate regulations, and produce social inequalities or ethical controversies.[8]

- **Dependency on Vendors and Platforms**

Definition:

Dependency on vendors and platforms occurs when organizations rely heavily on external technology providers for essential services such as cloud storage, software, or maintenance.

Causes and Contributing Factors:

Outsourcing IT operations, using proprietary software, and engaging in long-term vendor contracts reduce flexibility. Limited interoperability and switching costs reinforce dependency. [9]

Impacts and Consequences:

Vendor dependency can cause disruptions if providers experience failures, price increases, or data breaches. It restricts control over data and technology decisions, posing operational and strategic risks. [9]

- **Job displacement**

Definition:

Job displacement refers to the reduction or transformation of employment caused by automation, artificial intelligence, or other digital technologies that replace or redefine human tasks. [10]

Causes and Contributing Factors:

Advances in robotics, AI, and process automation reduce demand for routine tasks. Lack of upskilling initiatives and resistance to organizational change further amplify the problem. [7]

Impacts and Consequences:

Displacement can lead to workforce instability, social inequality, and resistance to technological change. It may harm employee morale and increase public criticism of digitalization practices. [10]

- **Legal and Regulatory Challenges**

Definition:

Legal and regulatory changes represent the evolving laws and compliance requirements governing technology use, data protection, and digital transactions.

Causes and Contributing Factors:

Rapid innovation often outpaces legislation. Differences in international regulations, unclear compliance standards, and inconsistent enforcement create uncertainty for organizations.[12]

Impacts and Consequences:

Non-compliance can lead to penalties, operational restrictions, or loss of licenses. Constant regulatory evolution increases compliance costs and strategic uncertainty, particularly in data-driven sectors. [12]

Conclusion

Digitalization represents both an opportunity and a challenge for non-academic environments. As organizations adopt new technologies to enhance efficiency and competitiveness, they also become increasingly exposed to a wide range of technological risks. This paper has identified and classified eight major categories of such risks - ranging from cybersecurity and data privacy concerns to ethical, social, and regulatory issues - providing a structured approach to understanding their causes, consequences, and interconnections. Applying the ISO 31000:2018 risk management framework has demonstrated that technological risk management must be continuous, systematic, and multidimensional. Beyond deploying technical safeguards, organizations must foster digital literacy, maintain ethical oversight, and ensure compliance with evolving legal standards. Building resilience requires a balance between innovation and control, where human, organizational, and technological elements are integrated within a comprehensive governance structure. Ultimately, effective management of technological risks in non-academic settings enables organizations to harness the benefits of digital transformation while safeguarding their integrity, reliability, and public trust. As digital ecosystems continue to evolve, proactive risk governance will remain essential for achieving sustainable and secure digital growth.

Acknowledgement

The paper is prepared as a part of the research activities under the project Models and Instruments for Transforming Higher Education System through Transnational Multi-Sector Links - STUDIES – DIG (Project N: 101131544), funded by the European Union.

References

1. ‘Digitization’, Gartner. [Online]. Available: https://www.gartner.com/en/information-technology/glossary/digitization
2. ‘Digitalization’, Gartner. [Online]. Available: https://www.gartner.com/en/information-technology/glossary/digitalization
3. *ISO 31000:2018 Risk management — Guidelines*. [Online]. Available: https://www.iso.org/standard/65694.html
4. S. Saeed, S. Altamimi, N. Alkayyal, E. Alshehri, and D. Alabbad, ‘Digital Transformation and Cybersecurity Challenges for Businesses Resilience: Issues and Recommendations’, vol. 23, no. 15, July 2023.
5. R. Malik, ‘Data Privacy & Cybersecurity: A Governance Imperative’, Mar. 2025, [Online]. Available: https://www.icsi.edu/media/webmodules/CSJ/March-2025/18.pdf
6. S. Jagarlamudi, ‘LESSONS LEARNED FROM CRITICAL SYSTEM FAILURES: A TECHNICAL OVERVIEW’, vol. 9, no. 2, pp. 358–367, Oct. 2024, doi: https://doi.org/10.5281/zenodo.13843406.
7. L. Patrick Willcocks, ‘Automation, digitalization and the future of work: A critical review’, vol. 3, no. 2, pp. 184–199, Feb. 2024, doi: https://doi.org/10.1108/JEBDE-09-2023-0018.
8. M. Bhatia and S. Kumar, ‘Ethical Implications of Biased Algorithms in Business Analytics’, Dec. 2024, [Online]. Available: https://www.researchgate.net/publication/394086631_Ethical_Implications_of_Biased_Algorithms_in_Business_Analytics
9. M. Vedenkannas, ‘Many ways of avoiding dependence on information system vendors’. [Online]. Available: https://www.vtv.fi/en/blog/many-ways-of-avoiding-dependence-on-information-system-vendors/
10. C. Peiwen, N. Sulaiman, and S. Zhenglong, ‘The Impact of Artificial Intelligence Application on Job Displacement and Creation: A Systematic Review’, vol. 9, no. 4, pp. 2495–2517, May 2025, doi: https://dx.doi.org/10.47772/IJRISS.2025.90400185.
11. Y. Luo, ‘A general framework of digitization risks in international business’, vol. 53, pp. 344–361, May 2021, doi: 10.1057/s41267-021-00448-9.
12. J. Paul Onoja, O. Hamza, A. Collins, U. Bright Chibunna, A. Eweja, and A. Ifesinachi Daraojimba, ‘Digital Transformation and Data Governance: Strategies for Regulatory Compliance and Secure AI-Driven Business Operations’, vol. 2, no. 1, pp. 43–55, Jan. 2021, doi: 10.54660/.IJFMR.2021.2.1.43-55.