UNEC Journal of Computer Science and Digital Technologies
Volume 1, № 1, 2025, pp. 83-89
https://doi.org/10.30546/UNECCSDT.2025.01.083

Section:
Digital Transformation &
Emerging Technologies

Working methodology for assessing digital transformation risks

Rasul Balayev[1], Sevda Hajizada[2*]

[1, 2*]*Department of Digital Technologies and Applied Informatics, UNEC, Baku, Azerbaijan*
0000-0001-7642-1635, rasul.balayev@unec.edu.az
0000-0001-7191-2718, s.hajizade@unec.edu.az

Abstract

The intensification of digital transformations increases risk situations and raises the issue of their assessment. Although these issues are the focus of researchers, there are still no working risk assessment tools that would gain the trust of users, especially representatives of micro and small businesses. To ensure competitiveness and overall business efficiency, it is advisable to create a working methodology for assessing the risks of digital transformation. The purpose of the study is to formulate a methodological approach designed to become a working tool for identifying the factors that determine the risk situation in the digital market and characterize their impact. For this purpose, the results of existing studies are commented on and a comparative description of methodological approaches to assessing the risks of digital transformation is given. The need for an urgent solution to the risk management problems associated with digital transformations was emphasized. Strategic measures to be taken to address the relevant problems were explained. The initial approach assumed a relatively easy-to-understand and implement methodological approach involving the creation of a bank of relevant risks for assessing cyber risks. From a methodological point of view, in the network implementation of multi-level business models, great importance is attached to the fact that digital business entities operating at the same level compete with each other and also enter into partnerships.

Keywords: digital transformations, risks, cyber risks, work methodology, business

Received:	*Revised:*	*Accepted:*	*Published:*
26/05/2025	*01/06/2025*	*05/06/2025*	*14/06/2025*

1. Introduction

The digital market presents surprises and new risks for market participants. It is difficult to determine whether these risks are related to the market, the economy or digital transformation. As with traditional risks [1], the initial approach can distinguish the manifestations of digital transformation risks in the digital market and in the digital economy (Figure 1). It is considered that [2] the risks of digital transformation primarily affect the functioning of market participants (business entities). To study the nature of risks in the digital economy, it is necessary to conduct a comparative characterization of digital and traditional economic relations. In the relevant sources [3], the following are mentioned as characteristics that distinguish the considered economic relations, determine risks and ultimately generate crises: decreasing utility and decreasing profitability. The decrease in utility is caused primarily by the fact that the benefits of using digital technologies are not directly related to material

production, but to the conditions of use. If the number of producers does not increase and the provider of digital services does not diversify its activities, marginal costs approach zero, and utility decreases.

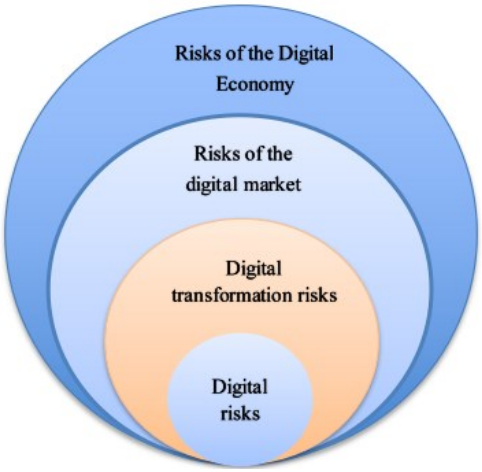


Figure 1. Classification of risks posed by digitalization
Compiled by the author.

The situation described leads to a decrease in profitability. We consider it possible to accept a simplified territorial distribution of the relationship to digital risks that arise during the manifestation of digital transformation, the digital market and the digital economy, presented in Figure 1.

The following are some of the risks faced by businesses in the digital marketplace [2]:

- Economic risks: monopoly, barriers that limit competition, isolation from external markets, financial difficulties.
- technological risks (serious discrepancies between technological innovation priorities and national innovation priorities; ergonomic problems);
- electronic risks, expressed in the encounter with theft of personal information, online fraud, spam attacks, virus attacks, spyware and other similar situations.
- risks associated with the use of artificial intelligence (increasing possibilities of disinformation, erroneous overestimation of AI capabilities and actions under its influence, distortion of reality, detachment from reality, control of AI by malicious entities);
- natural and environmental risks (damage to equipment and digital infrastructure, problems with energy supply as a result of natural disasters, as well as for environmental reasons).

The following risks associated with the digital economy should be highlighted [4]:

- oligopoly in the information market.
- limited opportunities for public and state control.
- displacement of live labor, reduction in wages for unskilled labor.
- the education system chronically lags the needs of the labor market.
- direct dependence on economic entities on the Internet.

2. Metodology

The purpose of creating a digital risk detection model is to redirect funds that would otherwise be spent on mitigating low-probability cyber risks to managing other risks. In practice, risk assessment models are complex, and the lack of clarity about which factors influence the results makes it difficult for business entities to use them when making decisions. According to business entities, especially small and medium-sized businesses, these models should be understandable to them and to experts. In other words, a working risk assessment tool is needed in the context of the prevalence of small and medium-sized businesses. In this regard,

in our opinion, the following approach deserves attention. According to the classical approach, the risk detection model (R) assumes that the probability of an incident (E) is calculated as the product of the damage (Z) that would be caused if the incident occurred [5].

The probability and loss indicators can be represented as the following functions:

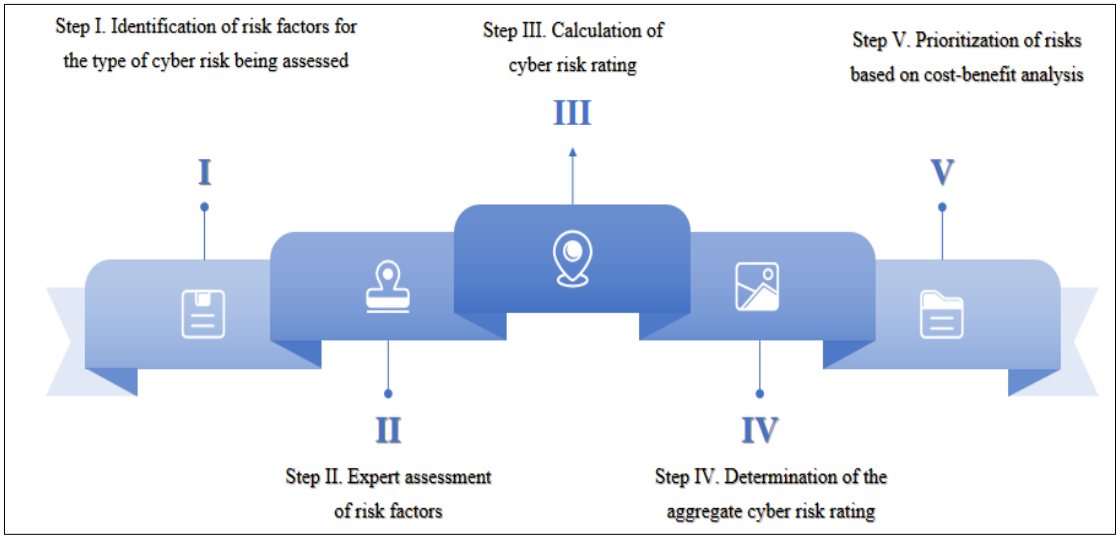
$$\boldsymbol{R = E \times Z}$$

$$\boldsymbol{E = \alpha \sum H + \beta \sum B + \gamma \sum Q + \delta \sum S}$$

$$\boldsymbol{Z = \nu \sum A + \lambda \sum P + \omega \sum R + ↄ \sum T + \mu \sum N}$$

Here,
H-threats;
B-weaknesses (gaps);
Q-potential for violation of the rules (malfunction);
S-effectiveness of protective measures;
A-losses from asset depreciation;
P-losses from process disruption;
T-costs of ineffective regulatory measures;
N – represents losses due to dissatisfaction of partners and customers.
$\boldsymbol{\alpha, \beta, \gamma, \delta, \nu, \lambda, \omega}$, ↄ, μ -are the corresponding coefficients.

In cases where it is not possible to obtain data on the quantitative assessment of the probability and damage indicators (which is indeed the case in this particular case), it is necessary to use expert approaches to assessing cyber risks. In this case, the calculation algorithm includes the following steps (Scheme 1):



Scheme 1. Sequence of steps for cyber risk assessment

At Step I, described in Scheme 1, it is considered appropriate to create a bank of cyber risks and their determinants [6]. A certain amount of subjectivity is allowed in the expert assessment of risk factors (Step III) [7]. To reduce the negative impact of the subjective approach, it is advisable to narrow the scope of application of expert technologies and use them as an additional tool for assessing risk factors. The results obtained in studies [8], where the overall cyber risk rating is calculated at Step III, can be more clearly demonstrated using machine learning. At Step IV, it is advisable to calculate the overall cyber risk rating using the matrix method. In IoT projects, this approach provides more reliable results, as shown in the

relevant sources [9]. We believe that at this step, the generalization of expert opinions should be accompanied by the ability to appeal to different opinions before the end of the process. In this case, each responsible employee of the company will be able to qualitatively assess the impact of risk factors. The appropriateness of the recommended approach is due to the need to assess the subjects, rules, mechanisms and agreements involved in risk management from a single point of view [10].

The results obtained in the prioritization of digital risks based on cost-benefit analysis should be re-evaluated in terms of compliance with sustainable performance criteria. Compared with existing approaches [11], the recommended approach to assessing cyber risks is more flexible and understandable. As a next step, it is advisable to apply a transversal approach for a more reliable risk assessment. Thus, a broad-based approach to risk management in the context of digital transformation is considered promising. A transversal approach, expressed in attempts to take into account the interests of all key stakeholders, yields certain results, as noted in the relevant sources [12].

3. Results and discussion

In the relevant sources [13], the risks of digital transformation are classified according to various criteria. Using these classifications, the risks faced by digital business can be interpreted as follows:

- lack of a strategy that unites stakeholders to manage changes;
- increasing complexity of technologies and software created without taking into account network feedback;
- lack of emphasis on the ease of use criteria when developing digital tools;
- lagging behind the pace of business digitalization and the pace of change in consumer demand;
- inability to develop skills in data analysis, software integration, application architecture, cybersecurity and other areas due to the high frequency of changes;
- making a decision between ensuring information security and developing integration processes to the detriment of the latter;
- limitation of financial allocations due to failures in digital transformation.

Managing the risks associated with digital transformation requires addressing various issues that arise during these transformations. The sources that study these issues [14] mention the following as strategic measures to address them:

- increasing investment in digital technology platforms.
- creating a change (transformation) management working group.
- engaging a digital transformation consultant.
- taking into account the prospects for using digital platforms when developing and implementing business models, etc.

Digital transformations expand the scope of risk management by adding risks to economic activity. The growing dynamics of the business environment increases the diversity of approaches used to neutralize risks in value chains.

Corporate digital transformations are accompanied by risks that affect company revenues. As shown in the source below, ever-increasing investments in these transformations increase the likelihood of operational risks [15]. In this case, the question of which risks at the company level are more serious and which require greater costs to eliminate becomes relevant.

The choice or formulation of a methodological approach to assessing digital risks requires characterizing the risks in the digital environment and answering a number of questions. We limited ourselves to the following questions:

a) What changes do modern transformations, including digital ones, bring to the concept of risk? Relevant sources [16] distinguish between risks threatening business, social, economic and information security, as well as investment, military, political and other risks. Digital

transformations bring information risks to the forefront, putting cybersecurity issues on the agenda.

b) How does digitalization affect traditional risks and how do digital risks differ from traditional risks? Although digital transformations partially eliminate problems such as incompleteness and asymmetry of information, their ability to reduce the likelihood of traditional risks remains a subject of discussion. Risks in the digital market and in the digital economy are directly related to information relations and technologies, network modes. Rapid digitalization causes radical and large-scale changes in people, society and the environment, increasing the likelihood of new risks. In the documents of authoritative international organizations, technological factors that determine technological risks include new technologies, materials, production networks, policies, and measurement difficulties, the characteristics of which are uncertain in the near future [17]. We agree with this approach that it is necessary to distinguish between the impact of technological development or its problems on digital risks [18]. The fact is that in practice, technological risks are often associated not with digital technologies, but with problems in their application.

c) What are the dynamics of risk management costs in the digital market?

In this regard, the results of relevant studies [19] show that companies perceive the risks associated with digitalization as follows:

- the costs of implementing digital technologies are disproportionate to the income received (35%);
- difficulties with recruiting personnel (34%);
- information security problems (33%);
- possible losses (31%).

Observations show that companies around the world are forced to take various preventive measures to combat expected cybersecurity threats. These measures significantly increase the costs of ensuring cybersecurity. In other words, the share of cybersecurity costs in the total investment in digital development tends to increase.

It should also be noted that among the growing variety of theoretical approaches, the transversal approach used to characterize and manage risks is considered more productive in terms of sustainable development requirements. The already mentioned source [12] puts forward the following argument in favor of using a transversal approach when defining the main steps of digital risk management: when identifying risks, a holistic view of factors such as the relationships between the company's structural units and the negative consequences of the risks that have occurred allows for the perception of expectations. In this process, the possibilities for the use of innovative technologies are expanded, and the company feels more confident in making decisions.

4. Conclusion

The transformation of the proposed, easy-to-understand methodological approach to assessing the risks of digital transformation into a working tool should be accompanied by the creation of a cyber risk bank. Another necessary condition is the formation of the necessary database with the participation of digital service providers and business entities. At present, when implementing a multi-level (network, transport and application) business model on the Internet, the possibility of cooperation between digital companies operating at the same level, while competing, should be considered. It is very likely that the proposed approach will be promising for use in decision support systems.

Acknowledgment

We would like to express our gratitude to the staff of the Department of Digital Technologies and Applied Informatics of the Azerbaijan State University of Economics for their assistance in researching materials on the problem.

Authors' Declaration

Conflicts of Interest: There were no conflicts of interest between the authors during the preparation of the article.

Authors' Contribution Statement

The authors contributed equally to all steps of the preparation of the article.

Authors' Contribution Statement

- Balayev Rasul Enver: Provided academic supervision and methodological guidance throughout the research process; reviewed and edited the final manuscript.
- Hajizada Sevda Mammadjafar: Contributed to the development of the research concept, conducted data analysis, and participated in the writing of the manuscript.

All authors have read and approved the final version of the manuscript and agree to be accountable for all aspects of the work.

References

1. Hudakova, M., Gabrysova, M., Petrakova, Z., Buganova, K., & Krajcik, V. (2021). The Perception of Market and Economic Risks by Owners and Managers of Enterprises in the V4 Countries. Journal of Competitiveness, 13(4), 60–77. https://doi.org/10.7441/joc.
2. Timchuk, Oksana. (2020). Key Risks Of Digital Business Transformation. 635-640. 10.15405/epsbs.2020.12.82
3. Kaluzhsky, M. (2013). Новая экономика: от кризиса доткомов к виртуальному бизнесу. Информационные ресурсы России, 2, 27-32. https://nbn-resolving.org/urn:nbn:de:0168-ssoar-431561
4. Livshits, s.A. & Novikova, Olga & Yudina, N.A. & Nikolaeva, E.K. & Katz, David. (2019). Possible risks of the development of the digital economy. 10.2991/icdtli-19.2019.40
5. Kurmanova D.A., Sultangareev D.R., Khabibullina L.R. Models of financial technology risk management // Vestnik usntu. Science, education, economics. Series: Economics. 2020. No. 2 (32) in Russian URL: https://cyberleninka. ru/ article/n/modeli-upravleniya-riskami-finansovyh-tehnologiy
6. Huq N. TrendLabs Research. Follow the Data: Dissecting Data Breaches and Debunking Myths: Trend Micro Analysis of Privacy Rights Clearinghouse 2005–2015 Data Breach Records. Tokyo, Japan: Trend Micro, 2015. P. 51. URL: https://documents.trendmicro.com/assets/wp/wp-follow-the-data.pdf
7. Skjong, Rolf & Wentworth, Benedikte & Norske, Det & Hovik, Veritas & Norway,. (2011). Expert Judgment and Risk Perception
8. Sığırtmaç, Esma & Balta, Musa & Balta, Deniz. (2025). Determining the Cyber Risk Matrix and Actions Created by Company Employees with Machine Learning. Hittite Journal of Science and Engineering. 12. 1-14. 10.17350/HJSE19030000346
9. Pal, Ranjan & Huang, Ziyuan & Yin, Xinlong & Lototsky, S. & De, Swades & Tarkoma, Sasu & Liu, Mingyan & Crowcroft, Jon & Sastry, Nishanth. (2020). Aggregate Cyber-Risk Management in the IoT Age Cautionary Statistics for (Re)Insurers and Likes. IEEE Internet of Things Journal. PP. 1-1. 10.1109/JIOT.2020.3039254
10. Scardovi C. Digital Transformation in Financial Services. London: Springer International Publishing AG, 2017. 236 p. URL: https://doi:10.1007/ 978-3-319-66945-8

11. Cherdantseva, yulıa & Burnap, Pete & Blyth, Andrew & Eden, & Jones, & Soulsby, & Stoddart, Kristan. (2016). A Review of cyber security risk assessment methods for SCADA systems. Computers & Security. 56. pp. 1-27.. 10.1016/j.cose.2015.09.009
12. Vorontsova, Yu & Baranov, V.. (2021). Transversal approach to digital risk management. E-Management. 3. 49-56. 10.26425/2658-3445-2020-3-4-49-56
13. Brosnan, Andrew & McCarthy, Stephen & Carroll, Noel. (2024). Exploring the Nature of Risk in Digital Transformation: A Problematisation Perspective of Low-Code/ No-Code Platform Risk
14. Golovkov S. S., Kalinina I. A. Key risks of digital business transformation // Innovations and Investments. 2023. No. 3. (in Russian) URL: https://cyberleninka.ru/article/n/klyuchevye-riski-tsifrovoy-transformatsii-biznesa
15. Jiang, K., Chen, L., Li, J. *et al.* The risk effects of corporate digitalization: exacerbate or mitigate? *Humanit Soc Sci Commun* **12**, 317 (2025). https://doi.org/10.1057/s41599-025-04628-y
16. Ruan K. Cyber Risk Management: A New Era of Enterprise Risk Management. Digital Asset Valuation and Cyber Risk Measurement Principles of Cybernomics. Cambridge: Elsevier Inc., 2019. P. 49–73. URL: https://doi.org/10.1016/B978-0-12-812158-0.00003-X
17. Managing emerging technology-related risks. Standard Recommendation: CWA 16649:2013.URL:https://shop.standards.ie/preview/98705249998.pdf?sku=877230_SAIG_NSAI_ NSAI_2084853
18. Chernyakov Mikhail & Chernyakova, Maria. (2018). Technological Risks of the Digital Economy. Корпоративные финансы.12.99-109. 10.17323/j.jcfr.2073-0438.12.4. 2018. 99-109
19. Okrepilov, Vladimir. (2020). Approaches To Risk Management In Digital Economy: Corporate Risk Management. 543-552. 10.15405/epsbs.2020.10.03.61