

Management:
Science and Education

Slovak Scientific Journal

Slovak Scientific Journal **Management: Science and Education ~ m:se** is the scientific journal aimed at the presentation of selected theoretical and practical knowledge and experience of general management issues.

The journal focuses on publishing original results of theoretical and applied research and also verified the practical experience of the authors and collectives. It should be focused on the latest trends and theories, current approaches and view on complexity of the management issue and its individual parts. Specific scientific journal portfolio is:

Management as a professional socio-economic problem (general management, business management, strategic management, knowledge management, innovation management, financial management, quality management, human resources management, marketing-management and other management functions, processes and tools).

Management as a problem of ***science***, the subject of scientific research (methods tools, models, solutions to the knowledge base of Management Science).

Management as an ***education*** discipline, the subject of teaching and professional education (educational approaches, methods and techniques).

Journal Title: **Management: Science and Education ~ m:se**

Editor-in-Chief

prof. Ing. Štefan Hittmár, PhD., DBA

Executive Editor

assoc. prof. Ing. Viliam Lendel, PhD.

Scientific Board

prof. emeritus Wladimir Andreff	University Paris 1 Panthéon Sorbonne, France
assoc. prof. Ing. Vladislav Bína, Ph.D.	University of Economics in Prague, Czech Republic
prof. Ing. Ivan Brezina, CSc.	University of Economics in Bratislava, Slovakia
dr. Frederick Duncan	St. Paul University N.Y., USA
prof. Ing. Jaroslav Ďaďo, PhD.	Matej Bel University in Banská Bystrica, Slovakia
prof. Ing. Štefan Hittmár, PhD., DBA	University of Žilina, Slovakia
prof. Dr. MA Ing. Július Horváth, PhD.	Central European University, Budapest, Hungary
prof. Ing. Vojtěch Koráb, Dr., MBA	Brno University of Technology, Czech Republic
prof. Ing. Milan Kubina, PhD.	University of Žilina, Slovakia
assoc. prof. Ing. Viliam Lendel, PhD.	University of Žilina, Slovakia
prof. Ing. Dr. Róbert Štefko, PhD.	University of Prešov in Prešov, Slovakia
assoc. prof. Ing. Michal Varmus, PhD.	University of Žilina, Slovakia

Editorial Board

prof. Ing. Štefan Hittmár, PhD., DBA	Faculty of Management Science and Informatics, University of Žilina e-mail: stefan.hittmar@fri.uniza.sk
Ing. Michal Kuběnka, Ph.D.	Faculty of Economics and Administration, University of Pardubice e-mail: michal.kubenka@upce.cz
assoc. prof. Ing. Viliam Lendel, PhD.	Faculty of Management Science and Informatics, University of Žilina e-mail: viliam.lendel@fri.uniza.sk
assoc. prof. Ing. Michal Varmus, PhD.	Faculty of Management Science and Informatics, University of Žilina e-mail: michal.varmus@fri.uniza.sk

Assistant of the Editorial Office

assoc. prof. Ing. Michal Varmus, PhD.	e-mail: michal.varmus@fri.uniza.sk

Published by

Faculty of Management Science and Informatics, University of Žilina
Univerzitná 8215/1, 010 26 Žilina, Slovakia

&

Institute of Management by University of Žilina
Veľký diel 3792, 010 26 Žilina, Slovakia

Production

EDIS – Editing Centre, University of Žilina
Univerzitná blok HB, 010 26 Žilina, Slovakia

INTRODUCTION

Modern management based on applying new management models and methods and using progressive management techniques, methods and procedures has got special importance in current period of continuous transformation and progress of our economy within market conditions of European Union. With arise of theoretical base, knowledge of science and scientific approaches this approach is more actual and interesting.

Management in the meaning of "manage" is applied in conditions of social-economical systems management. All known rules, guides, models and techniques of so-called common management are applied here. This universality is practically essential with regard to activity and progress of businesses in challenging market environment and need of its suitable implementation within different economical and social situations.

Management represents from the most common view complex of universally applied models, approaches, methods and techniques used by assessing resources and reaching goals of business oriented system, which products are material products or intangible services. Management is aimed on creating functional conditions and progress of technically, organizationally, economically and socially independent and operable system, acting and evolving in competitive environment.

By applying management in specific conditions of different systems, more concrete approaches, methods and techniques are finding. These basically arise from common knowledge, are transformed and mainly adapted to more real condition of routine. Therefore also in management, practical solutions and simultaneously also theoretical knowledge should be evolving. Developing the theoretical and practical background is therefore very important. Determination of scope and rate of these two procedures cannot be exactly specified – it will always depend on specific applications.

Scientific articles in this journal present selected actual development trends in management principally in theoretical level. In the some cases it reacts on actual needs of businesses to improve their management activities in order to gain particular competitive advantage within their market. Therefore scientific papers are mapping the newest theoretical trends but in area of practical use of managerial work.

The effort to prepare and publish the scientific papers is to point to chosen process and tool solutions, which cover the complexity and levels of management science.

Scientific articles are based on successful scientific endeavors of particular authors acting on different colleges and universities. Authors describe, evaluate and propose various approaches, models and techniques to immediate applying or as management task support. It is thereby created consistent enough material for explanation, understanding and evolving theoretical questions in these established problems.



Editor-in-Chief

CONTENTS

KATARÍNA DOMANICKÁ – JAKUB SOVIAR – MARTIN HOLUBČÍK – DOMINIKA TOMAN
Explainable AI in Multitenant Cloud-Based Security Operations Centers 5

DOMINIKA DUPÁKOVÁ – MILAN KUBINA – VILIAM LENDEL
Continuity Management with Connection to the Security Operations Center 11

LINDA FILIPOVIČOVÁ – JAKUB SOVIAR – MARTIN HOLUBČÍK – MARTIN MIČIAK
Theoretical-Analytical Framework of a Multi-tenant SOC Cloud Service
with ML Elements for Sustainable Digital Risk Management 16

IVANA GABRIŠOVÁ – GABRIEL KOMAN – LUCIE LENDELOVÁ
Modern Information Systems as a Tool for Managerial Decision Support 24

ADAM JACKO – MICHAL VARMUS – RADOSLAV JANKAL
An Integrated Framework for Identifying and Prioritising Cybersecurity Risks in Sports Management 30

SILVIA KRÚPOVÁ – GABRIEL KOMAN – ONDREJ STOPKA
The Practical Deployment of UAVs: A Market Analysis and Case Study Approach 37

ALŽBETA KUCHARČÍKOVÁ – IVANA POMPUROVÁ
Status of People with Disabilities in the Labor Market 43

ALŽBETA KUCHARČÍKOVÁ – IVANA POMPUROVÁ
Employment of People with Disabilities in the Labor Market – Analysis of Research Studies 50

EXPLAINABLE AI IN MULTITENANT CLOUD-BASED SECURITY OPERATIONS CENTERS

KATARÍNA DOMANICKÁ – JAKUB SOVIAR – MARTIN HOLUBČÍK – DOMINIKA TOMAN

Abstract: *The increasing adoption of multitenant cloud-based Security Operations Centers (SOCs) and the growing integration of machine learning into security operations have introduced new challenges related to transparency, trust, privacy protection, and governance. While advanced artificial intelligence techniques enhance detection capabilities and operational scalability, many models operate as opaque systems, limiting interpretability and auditability in security-critical environments. This tension is particularly significant in multitenant infrastructures, where strict requirements for tenant isolation, data protection, and continuous verification coexist with high levels of automation. The purpose of this article is to develop a conceptual framework for Explainable AI in Multitenant Cloud-Based Security Operations Centers. The study is conceptual in nature and is based on a structured literature review conducted across major academic databases. An initial corpus of 36 peer-reviewed publications was identified, of which 12 studies met predefined inclusion criteria and formed the analytical foundation of the paper. The selected literature was qualitatively synthesized to identify recurring themes related to explainability, federated learning, privacy-preserving machine learning, Zero Trust principles, and AI governance in SOC environments. The results indicate that explainability should not be understood solely as a technical feature of machine learning models, but rather as a cross-layer design principle interconnected with data protection mechanisms, tenant isolation requirements, and governance structures. Based on this synthesis, the article proposes a multilayer conceptual framework integrating data, model, explainability, and governance layers within multitenant SOC architectures. The study contributes to the theoretical advancement of AI-driven cybersecurity operations by systematically linking explainability with privacy, operational control, and governance in multitenant cloud environments. The proposed framework extends existing fragmented discussions and provides a structured conceptual basis for future empirical validation and implementation-oriented research in explainable AI for cloud-based security operations.*

Keywords: *Explainable Artificial Intelligence, Multitenant Cloud Security, Security Operations Center (SOC), Federated Learning, AI Governance*

JEL Classification: *D8, L8, M15, M21*

1. INTRODUCTION

The rapid expansion of cloud computing and the increasing adoption of Security Operations Center services in multitenant environments have fundamentally transformed the way cybersecurity operations are organized and delivered. In parallel, machine learning and artificial intelligence techniques are progressively integrated into SOC workflows in order to improve detection capabilities, automate repetitive tasks, and support analysts in managing growing volumes of security events. However, the increasing reliance on complex machine learning models, particularly in shared cloud infrastructures, raises critical concerns regarding explainability, trust, privacy protection, and governance. The central problem addressed in this article lies in the tension between automation and transparency in multitenant cloud based SOC environments. While advanced machine learning techniques enhance detection performance and scalability, many of these systems operate as black box models, limiting analysts' ability to understand, verify, and justify security decisions. In multitenant settings, this challenge is further amplified by strict requirements for tenant isolation, data protection, and continuous verification within shared infrastructures.

The main objective of this article is to develop a conceptual framework for Explainable AI in Multitenant Cloud Based Security Operations Centers. The framework integrates insights from the literature on SOC architectures, machine learning in cybersecurity, federated and privacy preserving learning, Zero Trust principles, and AI governance. By synthesizing these domains, the article seeks to clarify how explainability can be systematically embedded into multitenant SOC design not only at the technical model level but also at the architectural and governance levels.

Readers can expect a structured theoretical and analytical synthesis of existing research followed by the formulation of a multilayer conceptual model that connects explainability, privacy protection, tenant isolation, and governance mechanisms. The contribution of this article lies in bridging previously fragmented discussions including SOC operational design, explainable artificial intelligence, federated learning, and AI governance into a unified conceptual perspective. The study is conceptual and based on secondary literature. It does not aim to provide empirical validation but rather to refine and extend the theoretical understanding of explainability within complex multitenant SOC ecosystems.

2. METHODOLOGY

This study adopts a structured literature review approach and is conceptual in nature. The data used in this research consist exclusively of secondary sources obtained from peer-reviewed scientific publications. The literature search was conducted using major academic databases, including Web of Science, Scopus, IEEE Xplore, and SpringerLink. The search strategy combined the keywords "Security Operations Center", "multitenant cloud", "machine learning",

"explainable artificial intelligence", "federated learning", and "AI governance".

The initial search process resulted in a corpus of 36 relevant publications. Duplicate records were removed prior to screening, and titles and abstracts were evaluated to assess thematic alignment with the defined research objective. The publications were screened according to the following criteria: English language, peer reviewed status, full text availability, and thematic relevance to multitenant SOC environments, machine learning integration, and explainability in cybersecurity. After full text assessment and relevance evaluation, 12 publications were retained as the primary analytical basis of this article.

The selected studies were qualitatively analyzed and synthesized to identify recurring conceptual themes related to explainability, privacy protection, tenant isolation, governance mechanisms, and operational constraints in multitenant cloud-based SOC environments. The findings form the foundation of the proposed conceptual framework.

3. THEORETICAL BACKGROUND

This chapter summarizes the theoretical foundations relevant to multitenant cloud based Security Operations Centers that utilize machine learning and explainable artificial intelligence. It focuses on three key areas: architectural and organizational SOC models, the integration of machine learning methods into security operations, and the issue of explainability and trustworthiness of algorithmic decision making. The objective is to establish a conceptual foundation for the subsequent design of the proposed framework.

Security Operations Center (SOC) can be defined, based on the available literature, as a centralized organizational unit responsible for the continuous monitoring, detection, analysis, and response to cybersecurity incidents within an organization's information systems. A systematic study by Vielberth et al. emphasizes that an SOC should not be understood as a single technical tool, but rather as a complex socio technical system integrating human resources, processes, technologies, and governance mechanisms (Vielberth et al., 2020). At the same time, multiple publications highlight the absence of a unified, generally accepted definition of an SOC in academic literature. Authors concur that this terminological ambiguity complicates both the comparison of SOC solutions and the systematic research of this domain (Vielberth et al., 2020; Chamkar et al., 2024). Despite these definitional inconsistencies, the literature repeatedly reflects a consensus that the core functions of an SOC include the collection and correlation of security events, incident detection, investigation, escalation, and support for incident response.

Several SOC models are distinguished in the literature, differing in their degree of centralization, organizational placement, and service delivery model. In addition to traditional in house SOCs, virtualized and outsourced models are described, frequently operated by managed security service providers serving multiple clients simultaneously (Chamkar et al., 2024; Gnanasekaran et al., 2025). These models enable the scaling of security operations; however, they also introduce new requirements related to architectural design, data isolation, and responsibility management.

From a historical perspective, the evolution of SOCs is characterized by a transition from predominantly reactive models based on signature driven mechanisms and manual incident handling to proactive approaches emphasizing continuous behavioral analytics, threat hunting, and automation (Nagar, 2018). This evolution is closely associated with the increasing complexity of IT environments and the growing volume of security related data. With the expansion of cloud services and the outsourcing of security functions, SOC models providing security services to multiple organizations via shared infrastructure have become increasingly prevalent in practice (Chamkar et al., 2024).

Based on an empirical study, Gnanasekaran et al. identify multiple SOC models, including in house, outsourced, and integrated SOCs serving multiple clients through a centralized platform. The authors highlight inherent trade offs among scalability, cost efficiency, contextual knowledge of the client environment, and detection accuracy that characterize these models (Gnanasekaran et al., 2025). Multitenant SOC solutions are closely intertwined with shared cloud infrastructure. The literature emphasizes that, in such environments, ensuring tenant isolation at the levels of data, identity, application logic, and network resources is a critical prerequisite (Hariharan, 2025). Insufficient isolation may enable lateral movement by attackers, data breaches, and violations of regulatory requirements. Hariharan further argues that in shared infrastructure environments, no system component can be implicitly trusted, and that continuous authentication, authorization, and monitoring are essential for tenant protection (Hariharan, 2025).

With the increasing volume of security data and the accelerating pace of cyberattacks, machine learning techniques have been progressively adopted within SOC environments. The literature documents the application of ML for event correlation, anomaly detection, alert prioritization, and decision support for security analysts (Nagar, 2018; Srinivas et al., 2025). Srinivas et al. argue that traditional rule based and signature driven approaches are insufficient to effectively address dynamic and sophisticated threats, which has led to the integration of advanced ML models, large language models, and autonomous agents into SOC workflows. These technologies are presented as mechanisms for automating routine tasks, supporting analysts, and reducing detection and response times (Srinivas et al., 2025). In the context of anomaly detection, particularly in cloud and distributed environments, the literature identifies limitations of centralized cloud based ML approaches and proposes federated learning as a method enabling collaboration among multiple entities without sharing raw data (Kumar and Idamakanti, 2025). This approach is especially relevant in multitenant environments, where requirements for privacy protection and data isolation are particularly stringent.

Despite the growing adoption of machine learning, the literature also highlights the challenge posed by so called black box models, whose decision making processes are difficult for users to interpret. This issue is particularly critical in security applications, where analysts must understand the rationale behind detections, verify their validity, and justify the decisions taken (Mohale and Obagbuwa, 2025). The work of Mohale and Obagbuwa analyzes the integration of explainable artificial intelligence in intrusion detection

systems and emphasizes that explainability is a key factor for analyst trust, system auditability, and the practical deployment of ML models in production environments. The authors identify several XAI techniques that enable local or global explanations of model decisions, while also noting trade offs between interpretability, accuracy, and computational overhead (Mohale and Obagbuwa, 2025). In the broader context of security operations, explainability is presented not merely as a technical property of ML models, but as part of a wider framework encompassing trust, accountability, and regulatory compliance. Some studies emphasize that in regulated environments and in security as a service delivery models, the ability to explain analytical decisions is essential for maintaining customer trust and meeting audit requirements (Srinivas et al., 2025).

4. ANALYTICAL PART

Building upon the theoretical foundations presented in the preceding chapter, this section focuses on the analytical integration of multitenant cloud based SOC environments, machine learning, and explainable artificial intelligence. The objective is to examine how the literature reflects requirements for explainability in security systems, what implications privacy protection and tenant isolation have for the design of machine learning models, and how explainability can be conceptualized within the context of the SOC pipeline. This chapter provides a synthesis of existing knowledge that establishes the basis for the subsequent development of a conceptual framework.

4.1 Requirements for Explainability in Multitenant SOC Environments

The literature addressing the integration of machine learning into security systems repeatedly highlights the problem of insufficient model interpretability. Mohale and Obagbuwa state that many intrusion detection systems utilizing machine learning operate as so called black box models, whose decision making processes are difficult for security analysts to interpret (Mohale and Obagbuwa, 2025). The authors further conclude that the lack of explainability reduces user trust and complicates the practical deployment of these systems in production environments (Mohale and Obagbuwa, 2025). In the same systematic review, the authors emphasize that explainability enables analysts to identify which attributes or features of the input data contributed to a specific model decision (Mohale and Obagbuwa, 2025). Explainable artificial intelligence is therefore presented in their work as an approach that supports transparency and the practical usability of machine learning models in security applications (Mohale and Obagbuwa, 2025).

Srinivas et al., in the context of AI augmented SOC environments, state that the automation of security processes through advanced models and agents is intended to support the work of security analysts within SOC workflows (Srinivas et al., 2025). At the same time, the authors discuss the necessity of maintaining control, oversight, and feedback mechanisms in processes supported by artificial intelligence tools (Srinivas et al., 2025). Based on an empirical study, Gnanasekaran et al. identify several SOC models, including in house, outsourced, and integrated models, and highlight trade offs among cost, organizational integration, and detection capability (Gnanasekaran et al., 2025). In the context of models serving multiple clients through a centralized platform, the authors emphasize that the nature of service delivery influences the operational configuration of the SOC and its associated processes (Gnanasekaran et al., 2025).

4.2 Tenant Aware Explainability

Hariharan, in a study focused on Zero Trust in multi tenant cloud environments, emphasizes that shared infrastructure creates increased requirements for access management, continuous verification, and tenant protection (Hariharan, 2025). The author highlights the insufficiency of traditional perimeter based approaches in such environments and stresses the principle of never trust, always verify (Hariharan, 2025). Kumar and Idamakanti, in their discussion of cloud based anomaly detection, address the limitations of centralized machine learning approaches, particularly from the perspective of privacy protection and scalability (Kumar and Idamakanti, 2025). As an alternative, they propose federated learning, which enables model training without sharing raw data among participating entities. The authors also consider the need for explainability in such machine learning settings and describe the use of explainable artificial intelligence techniques to enhance decision transparency (Kumar and Idamakanti, 2025).

The literature on privacy preserving and decentralized machine learning, including federated learning frameworks and associated security and privacy requirements, underscores the importance of protecting sensitive data during both training and inference in environments involving multiple collaborating entities (Hasan and Kudapa, 2021; Kucur et al., 2026). Kucur et al. systematically examine cryptographic approaches and open challenges in privacy preserving machine learning, including practical limitations and risks in distributed settings (Kucur et al., 2026). Similarly, Hasan and Kudapa present conceptual foundations of data privacy aware machine learning and federated learning as approaches for safeguarding data in distributed processing environments (Hasan and Kudapa, 2021). Based on the referenced sources, it can be concluded that the literature links requirements for privacy protection, the restriction of raw data sharing, and the need for transparent decision making, particularly in distributed and cloud based environments (Kumar and Idamakanti, 2025; Hasan and Kudapa, 2021; Kucur et al., 2026).

4.3 Explainability in the SOC Pipeline

Vielberth et al. describe the SOC as a socio technical system that integrates human resources, processes, technologies, and governance elements, while emphasizing the importance of coordinating activities from detection to incident response (Vielberth et al., 2020). Chamkar et al. further elaborate architectural SOC models, procedural workflows, and detection coverage practices, thereby providing a framework for analyzing how detection and response mechanisms are organized within an SOC (Chamkar et al., 2024). Srinivas et al. state that modern SOC environments increasingly integrate artificial intelligence and machine learning components, as well as automation mechanisms, into security workflows in order to support event processing and incident response. The authors discuss the necessity of monitoring the behavior and performance of such systems during operation and emphasize the

importance of feedback mechanisms within the operational activities of analysts (Srinivas et al., 2025).

Mohale and Obagbuwa distinguish between global and local approaches to explainability and underline their relevance for interpreting both overall model behavior and individual detections in security systems. The authors also highlight practical limitations of certain explainable artificial intelligence approaches, including computational demands that may be significant in environments requiring operational event processing (Mohale and Obagbuwa, 2025). Based on the referenced sources, it can be concluded that the literature supports the consideration of explainability as a property relevant to the processing of security events and decision making within an SOC. At the same time, it emphasizes the necessity of accounting for practical implementation constraints associated with explainable artificial intelligence techniques (Mohale and Obagbuwa, 2025; Srinivas et al., 2025; Vielberth et al., 2020; Chamkar et al., 2024).

5. PROPOSED CONCEPTUAL FRAMEWORK

This chapter builds upon the theoretical foundations and analytical synthesis presented in the preceding sections of the article. Its objective is to systematically organize the identified insights into a conceptual framework that reflects the requirements for explainability in multitenant cloud based Security Operations Centers. The chapter progressively addresses design principles derived from the literature, potential architectural layers of the framework, the integration of governance and accountability, and finally the positioning of explainability within the SOC life cycle.

5.1 Conceptual Design Principles

The available literature indicates that explainability in security systems is closely associated with user trust and the practical usability of models. Mohale and Obagbuwa (2025) note that many intrusion detection systems based on machine learning operate as so called black box models. Their decision making processes are difficult for security analysts to understand, which, according to the authors, reduces trust and complicates real world deployment in production environments (Mohale and Obagbuwa, 2025). The authors further emphasize that explainable artificial intelligence enables a clearer understanding of which specific input data attributes led to a given model decision, thereby supporting transparency in system operation (Mohale and Obagbuwa, 2025). Within so called AI augmented SOC environments, the need to maintain control over the level of automation is also emphasized. Srinivas et al. (2025) describe the use of advanced models, large language models, and autonomous agents as tools intended to support the work of analysts. At the same time, they stress that such systems must be complemented by mechanisms for oversight, control, and feedback in processes supported by artificial intelligence (Srinivas et al., 2025).

The issue of privacy protection and the limitation of data sharing is repeatedly linked in the analyzed sources to federated learning and broader privacy preserving approaches (Kumar and Idamakanti, 2025; Hasan and Kudapa, 2021; Kucur et al., 2026). Kumar and Idamakanti (2025) point to the limitations of centralized cloud based machine learning solutions and present federated learning as a method for training models without sharing raw data among participating entities. Hasan and Kudapa (2021) elaborate the concept of data privacy aware machine learning and federated learning as mechanisms for protecting sensitive information in distributed environments (Hasan and Kudapa, 2021). Kucur et al. (2026) complement this perspective with an analysis of cryptographic techniques, open challenges, and practical limitations of privacy preserving machine learning in distributed settings. In multitenant cloud environments, the need to protect individual tenants and to ensure continuous verification is particularly emphasized (Hariharan, 2025, Kucur et al., 2026). In the context of Zero Trust architecture, Hariharan (2025) states that shared infrastructure increases demands on access management, continuous identity verification, and tenant protection. The author highlights the inadequacy of traditional perimeter based approaches and stresses the principle of never trust, always verify as a foundation for protection in multi tenant cloud environments (Hariharan, 2025).

5.2 Architectural Layers of the Framework

The analyzed publications do not provide a unified architectural model of a multitenant SOC with explicitly defined layers such as data, model, explainability, and governance (Vielberth et al., 2020; Chamkar et al., 2024; Kumar and Idamakanti, 2025; Mohale and Obagbuwa, 2025; Kucur et al., 2026). However, several works describe elements that may be understood as distinct functional layers of the system (Vielberth et al., 2020; Chamkar et al., 2024).

Vielberth et al. (2020) characterize the SOC as a socio technical system that connects people, processes, technologies, and governance mechanisms. This perspective enables the consideration of the SOC not only as a technical platform but also as an organizational and managerial framework (Vielberth et al., 2020). Chamkar et al. (2024) further elaborate architectural SOC models and describe workflows and detection coverage approaches that shape the technological and procedural structure of security operations (Chamkar et al., 2024).

At the level of models and explainability, Kumar and Idamakanti (2025) discuss federated learning and describe the integration of explainable artificial intelligence techniques to increase the transparency of detection decisions. Mohale and Obagbuwa (2025) distinguish between global and local explanations and discuss their relevance for interpreting overall model behavior as well as individual detections. Kucur et al. (2026) analyze cryptographic and privacy preserving mechanisms relevant to data protection in distributed processing environments. Based on these sources, it is possible to conceptualize a multilayer SOC structure that distinguishes between a data processing layer, a model layer, an explainability layer, and a governance and control layer (Vielberth et al., 2020; Chamkar et al., 2024; Kumar and Idamakanti, 2025; Mohale and Obagbuwa, 2025; Kucur et al., 2026).

5.3 Integration of Governance and Accountability

Issues of governance and accountability are linked in the literature primarily to the operation of artificial intelligence systems in regulated and organizationally complex environments. Otunlape (2026) analyzes governance frameworks for enterprise artificial intelligence and

emphasizes the need for systematic risk management, transparency, and control mechanisms in the implementation and operation of artificial intelligence solutions (Otunlape, 2026).Finch and Butt (2025) highlight gaps in existing governance frameworks and emphasize that their implementation must take into account actual organizational capacities and operational constraints. This aspect is also relevant for service delivery models in which processes and controls must be established under conditions of limited resources (Finch and Butt, 2025).

In security applications, governance is closely interconnected with explainability. Mohale and Obagbuwa (2025) associate explainability with auditability and the practical usability of machine learning models in production security systems, emphasizing the importance of decision transparency for the verifiability of detections (Mohale and Obagbuwa, 2025). Srinivas et al. (2025) underline the need for oversight, control, and feedback mechanisms in artificial intelligence supported SOC workflows, which is relevant from the perspective of operational management of machine learning components (Srinivas et al., 2025).

5.4 Positioning Explainability in the SOC Life Cycle

In the literature, the SOC is understood as a coordinated system of processes extending from detection to incident response, integrating both technical and organizational elements. Vielberth et al. (2020) emphasize the socio technical nature of the SOC and the need to coordinate activities related to detection and incident response (Vielberth et al., 2020). Chamkar et al. (2024) complement this perspective by elaborating workflows and detection mechanisms within the SOC (Chamkar et al., 2024).

Srinivas et al. (2025) state that modern SOC environments increasingly integrate artificial intelligence and machine learning components into their processes and highlight the necessity of monitoring the performance of these systems during operation, including feedback mechanisms from analysts (Srinivas et al., 2025). Mohale and Obagbuwa (2025) distinguish between global explanations of overall model behavior and local explanations of individual detections, both of which are relevant for interpreting security outputs. The authors also note the computational demands of certain explainable artificial intelligence techniques, which may constitute a limitation in the operational processing of large volumes of events (Mohale and Obagbuwa, 2025). Kumar and Idamakanti (2025), in the context of federated learning, describe the use of explainable artificial intelligence techniques to support transparency in decision making for cloud based anomaly detection (Kumar and Idamakanti, 2025).

6. DISCUSSION

The proposed conceptual framework is derived from a synthesis of literature on SOC architectures, multitenant cloud environments, machine learning, and explainable artificial intelligence. The analyzed studies consistently indicate that the SOC should be understood as a socio technical system integrating people, processes, technologies, and governance mechanisms (Vielberth et al., 2020). In this context, explainability does not emerge solely as a technical property of a model, but as a factor directly influencing trust, auditability, and the practical usability of security solutions (Mohale and Obagbuwa, 2025).

The problem of black box models identified in the field of intrusion detection (Mohale and Obagbuwa, 2025) is amplified in multitenant cloud environments by requirements for tenant isolation, access control, and continuous verification within shared infrastructure (Hariharan, 2025). At the same time, the literature highlights the limitations of centralized machine learning approaches and proposes federated and privacy preserving mechanisms as alternatives that enable model training without sharing raw data (Kumar and Idamakanti, 2025; Hasan and Kudapa, 2021; Kucur et al., 2026). The proposed framework connects these findings by conceptualizing explainability, privacy protection, and governance mechanisms as interrelated design principles.

Studies on AI augmented SOC environments further emphasize the need for oversight, control, and feedback in automated processes (Srinivas et al., 2025). Governance literature in the domain of enterprise artificial intelligence underlines the importance of systematic risk management, transparency, and organizational capacity in the implementation of artificial intelligence systems (Otunlape, 2026; Finch and Butt, 2025). Within this context, the proposed model can be interpreted as a conceptual integration of technical and organizational requirements into the structure of a multitenant cloud based SOC.

The limitations of the article lie primarily in its conceptual nature. The framework is derived from secondary literature and has not been empirically validated on a specific multitenant SOC implementation. The article does not include experimental comparisons of explainable artificial intelligence techniques, quantitative measurement of the impact of explainability on detection performance, or an organizational analysis of the implementation of governance mechanisms under real operational conditions. In addition, regional or sector specific regulatory differences that could affect the applicability of the model are not examined. Future research should therefore incorporate primary data from production multitenant SOC environments and provide empirical validation of the relationship between explainability, data protection, and operational efficiency.

7. CONCLUSIONS

This article set out to address the challenge of integrating explainable artificial intelligence into multitenant cloud-based Security Operations Centers. Building upon a structured literature review and analytical synthesis, it developed a conceptual framework that connects architectural, technical, and governance dimensions of explainability within SOC environments.

The findings suggest that explainability in multitenant SOCs cannot be reduced to a purely technical property of machine learning models. Instead, it must be understood as a cross-layer principle that interacts with privacy-preserving mechanisms, tenant isolation requirements, Zero Trust security principles, and organizational governance structures. By conceptualizing explainability across data, model, explainability, and governance layers, the article extends existing discussions that often treat these domains separately. The proposed framework contributes to theoretical development by positioning explainability as an integrative design principle within multitenant cloud security operations rather than as an auxiliary feature of individual

detection models. This perspective refines the understanding of SOC evolution in AI-augmented environments and highlights the interdependence between transparency, operational efficiency, and regulatory accountability.

At the same time, the conceptual nature of the framework calls for empirical validation. Future research should examine its applicability in real multitenant SOC implementations and assess how explainability mechanisms affect detection performance, analyst decision-making, and governance effectiveness in practice. By articulating the structural interconnections between explainability, privacy, and governance, this article contributes to advancing the theoretical foundations for trustworthy AI-driven security operations in cloud-based multitenant contexts.

Acknowledgement

Funded by the EU NextGenerationEU through the Recovery and Resilience Plan for Slovakia under the project No. 09I05-03-V02-00010.

REFERENCES

[1] NAGAR, G. (2018). The Evolution of Security Operations Centers (SOCs): Shifting from Reactive to Proactive Cybersecurity Strategies. ***International Journal of Scientific Research and Management***, 6(9), EC-2018-100–EC-2018-115. Available online: https://doi.org/10.18535/ijsrm/v6i9.ec03 (accessed on 16 February 2026).

[2] HARIHARAN, R. (2025). Zero Trust Security in Multi-Tenant Cloud Environments. ***Journal of Information Systems Engineering and Management***, 10(45s). Available online: https://doi.org/10.52783/jisem.v10i45s.8899 (accessed on 16 February 2026).

[3] SRINIVAS, S.; KIRK, B.; ZENDEJAS, J.; ESPINO, M.; BOSKOVICH, M.; BARI, A.; DAJANI, K.; ALZAHRANI, N. (2025). AI-Augmented SOC: A Survey of LLMs and Agents for Security Automation. ***Journal of Cybersecurity and Privacy***, 5, 95. Available online: https://doi.org/10.3390/jcp5040095?urlappend=%3Futm_source%3Dresearchgate.net%26utm_medium%3Darticle (accessed on 16 February 2026).

[4] KUMAR, P.; IDAMAKANTI, R. (2025). Cloud Network Anomaly Detection using Federated Learning and Explainable AI. ***International Journal on Science and Technology (IJSAT),*** 16(3), IJSAT25037336. Available online: https://doi.org/g9vzfp (accessed on 16 February 2026).

[5] MOHALE, V. Z.; OBAGBUWA, I. C. (2025). A systematic review on the integration of explainable artificial intelligence in intrusion detection systems to enhancing transparency and interpretability in cybersecurity. ***Frontiers in Artificial Intelligence***, 8, 1526221. Available online: https://doi.org/10.3389/frai.2025.1526221 (accessed on 16 February 2026).

[6] OTUNLAPE, O. (2026). Governance Frameworks for Enterprise AI Systems Operating in Regulated Environments. International ***Journal of Computer Applications***, 187(74), 13–21. Available online: https://www.ijcaonline.org/archives/volume187/number74/otunlape-2026-ijca-926244.pdf (accessed on 16 February 2026).

[7] FINCH, W. W.; BUTT, M. (2025). Gaps in AI-Compliant Complementary Governance Frameworks' Suitability (for Low-Capacity Actors), and Structural Asymmetries (in the Compliance Ecosystem)—A Systematic Review. ***Journal of Cybersecurity and Privacy***, 5, 101. Available online: https://doi.org/10.3390/jcp5040101 (accessed on 16 February 2026).

[8] KUCUR, E. N.; BUYUKTANIR, T.; UGURELLI, M.; YILDIZ, K. (2026). Privacy-Preserving Machine Learning Techniques: Cryptographic Approaches, Challenges, and Future Directions. ***Applied Sciences***, 16, 277. Available online: https://doi.org/10.3390/app16010277 (accessed on 16 February 2026).

[9] HASAN, M. T.; KUDAPA, S. P. (2021). Data Privacy-Aware Machine Learning and Federated Learning: A Framework for Data Security. ***American Journal of Interdisciplinary Studies***, 2(3), 01–34. Available online: https://doi.org/10.63125/vj1hem03 (accessed on 16 February 2026).

[10] CHAMKAR, S. A.; MALEH, Y.; GHERABI, N. (2024). Security Operations Centers: Use Case Best Practices, Coverage, and Gap Analysis Based on MITRE Adversarial Tactics, Techniques, and Common Knowledge. ***Journal of Cybersecurity and Privacy***, 4, 777–793. Available online: https://doi.org/10.3390/jcp4040036 (accessed on 16 February 2026).

[11] VIELBERTH, M.; BÖHM, F.; FICHTINGER, I.; PERNUL, G. (2020). Security Operations Center: A Systematic Study and Open Challenges. ***IEEE Access***, 8, 227756–227773. Available online: https://doi.org/10.1109/ACCESS.2020.3045514 (accessed on 16 February 2026).

[12] GNANASEKARAN, V.; NILSEN, T. G.; HEEGAARD, P. E. (2025). A Comparative Study of Security Operations Center Models for Operational Technology. In: ***Proceedings of the Norwegian Information Security Conference (NIKT 2025),*** 1–16. Available online: https://doi.org/10.5324/yd7t8t20 (accessed on 16 February 2026).

Katarína DOMANICKÁ, Ing.
Jakub SOVIAR, prof. Mgr., PhD.
Martin HOLUBČÍK, Ing., PhD.
Dominika TOMAN, Ing., PhD.
University of Žilina, Faculty of Informatics and Management Science, Department of Managerial Theories
Univerzitná 8215/1, 010 26 Žilina, Slovakia
e-mail: katarina.domanicka@stud.uniza.sk; jakub.soviar@fri.uniza.sk; martin.holubcik@fri.uniza.sk;
dominika.toman@fri.uniza.sk

CONTINUITY MANAGEMENT WITH CONNECTION TO THE SECURITY OPERATIONS CENTER

DOMINIKA DUPÁKOVÁ – MILAN KUBINA – VILIAM LENDEL

Abstract: *Business continuity management (BCM) is an approach that enables organizations to systematically prepare for emergencies and limit their impact on business operations. The purpose of this management is to ensure that the company can keep its most important processes running even in times of crisis, technical failure, or security incidents. The basis is a thorough risk assessment and business impact analysis (BIA), which are used to identify critical activities and set recovery limits - such as maximum tolerated downtime (RTO) or acceptable data loss (RPO). These findings are followed up with specific documents, in particular business continuity plans (BCP) and disaster recovery plans (DRP), which describe procedures in the event of a disruption to normal operations. In an environment where the functioning of organizations is closely linked to information and communication technologies, it is increasingly important to link business continuity with cybersecurity. The Security Operations Center (SOC) plays an important role here, ensuring continuous monitoring of systems, evaluation of security events, and management of incident response. While BCM creates a strategic framework and sets recovery priorities, SOC ensures operational response and real-time situation resolution. If these areas are interconnected and the organization regularly verifies its preparedness through tests, simulations, or exercises, its ability to handle crisis situations is significantly increased. Such a systematic approach strengthens operational and cyber resilience, promotes trust among business partners and customers, and contributes to the long-term stability and competitiveness of the organization.*

Keywords: *business continuity management, business impact analysis, cybersecurity, security operations center, enterprise*

JEL Classification: *M15, M21*

1. INTRODUCTION

Nowadays, with new cyber threats constantly evolving and emerging, it is very important for businesses to have a plan in place for how to operate and how to restore their operations in the event of a security incident. Business continuity management (BCM) is a systematic process focused on ensuring the resilience of a business against new threats and unforeseen events. The goal of this process is to identify critical areas and processes in the company, assess the impact of their disruption, and implement measures that will enable the company to quickly restore its key activities.

Today, BCM is viewed as more comprehensive than the traditional approach to disaster recovery planning. Greater emphasis is placed on proactive risk management, business impact analysis (BIA), and the establishment of recovery parameters such as RTO and RPO. This modern approach combines strategic management, risk management, crisis management, and information security.

The Security Operation Center (SOC) also plays an important role in this regard, ensuring continuous monitoring and detection of security incidents. This makes it possible to identify threats in a timely manner and respond to incidents. This connection strengthens the company's resilience to cyber threats.

2. METHODOLOGY

This article was written as a literature review in the field of business continuity management and its connection to the Security Operation Center.

Sources were searched in scientific databases such as Web of Science, Science Direct, and IEEE Xplore. Keywords such as business continuity management, business impact analysis, security operations center, cyber resilience, and combinations thereof were used.

The process of selecting relevant sources took place in several steps. First, the articles were assessed based on their titles. This was followed by selection based on abstracts, given that this article looks at the issue from a managerial perspective and the combination of these keywords often yielded highly technical articles that would not be suitable in terms of content. In the final step, the articles were reviewed in their entirety and those that were current and relevant to the topic were selected.

The selected sources formed the theoretical basis for the creation of this article.

3. BUSINESS CONTINUITY MANAGEMENT AND SECURITY OPERATIONS CENTER

Business continuity management is one of the important steps in business management. BCM itself is a complex management process. Its goal is to ensure that the organization is sufficiently resilient to risks, threats, and other unforeseeable events. It is a systematic process focused on identifying threats, assessing their impact, and designing and implementing measures that will enable the organization to continue its key activities in the event of a security incident. The goal is to minimize the consequences of incidents and return to normal operations as quickly as possible.

Business continuity management can be defined as a comprehensive management process that identifies potential threats to an organization and builds frameworks for resilience and effective response to protect the interests of stakeholders, reputation, and activities that create value for the organization [1].

BCM is the ability of an organization to continue delivering products or services at pre-agreed levels even after a serious incident [2].

According to some authors, BCM represents a shift from traditional disaster recovery planning, with the focus shifting from post-event recovery to proactive prevention or minimization of the impact of failure. Other authors agree with this statement, arguing that rather than focusing solely on information systems, business continuity management is about ensuring critical business functions and their continuity during any disruption that may affect many information assets. It combines concepts from organizational strategy, information systems, and crisis management, offering different perspectives beyond traditional disaster recovery models [3].

In an environment of intensive digitization and increasing technological interconnectedness of organizations, it is necessary to consider business continuity management from the perspective of cybersecurity. Today, the operation of key processes is closely linked to information and communication systems, which increases the importance of effective monitoring and management of security incidents. In this context, the Security Operations Center (SOC) plays an important role, providing continuous monitoring of security events, their identification, evaluation, and coordination of response measures. While BCM formulates strategic principles and continuity priorities, SOC is an operational mechanism that enables immediate response to incidents. Their mutual integration contributes to strengthening the organization's ability to cope with cyber and technological disruptions [4].

This is an increasingly important concept for the sustainability of an organization, especially in view of supply chain disruptions, economic uncertainties, climate change, and pandemics. Implementing this concept requires a systematic approach, including risk assessment, business continuity planning, and crisis management strategies, while some aspects are governed by legislation and industry standards [5].

It can therefore be said that business continuity management is a comprehensive set of planned and interconnected activities carried out in the event of an unplanned interruption to the normal operation of an organization, in the event of an accident or other crisis.

Within the framework of BCM objectives, each organization determines its own main objective, as each organization has different priorities. The strategic imperative of the business continuity management process is determined about the interests of individuals, the prevention of further losses or the inability to perform priority activities, and the impact on the environment. In general, however, the main objectives ensure:

- protection of priority activities
- stabilization and restoration of priority activities, their dependencies, and supporting resources,
- mitigation of impacts and response to negative effects caused by the crisis.

In the context of cyber incidents, these objectives are closely related to the activities of the SOC, which ensures the timely identification of security events, their evaluation, and escalation in accordance with the priorities set out in the BCM. The SOC thus represents an operational mechanism through which continuity objectives can be met, especially in scenarios of technological and information disruptions [6].

The most important thing to understand about BCM is that every organization faces certain risks. These may not only be cyber attacks, but also natural disasters, various technological failures, or internal problems. Given that BCM deals with risks, it is logical that it is based on risk analysis and business impact analysis.

The BCM process is a continuously evolving cycle consisting of various steps, such as understanding the business, creating a continuity strategy, defining recovery action plans, creating a continuity management culture, and testing and improving continuity plans.

The process is described as the BCM life cycle and consists of several basic steps:

- Strategy setting
- Planning
- Implementation
- Testing
- Continuous improvement

The SOC also plays an important role in implementation and testing, participating in cyber incident simulations, verifying response procedures, and testing the organization's preparedness for technological failures. SOC participation in BCP and DRP testing allows for verification not only of documented preparedness, but also of actual detection, response, and recovery coordination capabilities [6].

Proper and effective continuity planning is essential for BCM, resulting in a business continuity plan (BCP). In the event of technological disruptions, the BCP is closely linked to the Disaster Recovery Plan (DRP). In the event of cyber incidents, it is the SOC that identifies and classifies the incident and initiates the activation of the DRP, thereby directly supporting the achievement of the specified recovery parameters.

The scenario of sudden technology failure includes IT infrastructure outages, cyber attacks, and software failures. In such cases, the SOC provides continuous system monitoring, anomaly detection, forensic analysis, and response coordination. Its activities significantly influence the organization's ability to meet the RTO and RPO defined in the BIA. The RTO and RPO parameters also serve as a prioritization mechanism for SOC activities, as they determine which systems and processes must be restored first [7].

The strategy determines how the organization will respond to potential incidents and disruptions. Planning translates the strategy into specific measures that are recorded in continuity plans. Implementation represents the practical introduction of measures into the organization's activities. Testing is an important part of BCM. It verifies the effectiveness of plans in simulated conditions. This makes it possible to identify weaknesses before an incident occurs. Continuous improvement means that the BCM process is always considered incomplete. It needs to be constantly updated and adapted to changing conditions.

Technical measures alone are not enough to make BCM effective. The organization must have the right internal settings and culture. The point is that risks in the organization

should not be ignored or left unaddressed simply because they have been identified. It is about actively managing them. From this perspective, BCM can be seen as a competitive advantage, as a well-prepared organization has satisfied employees who know that they are prepared in the event of an incident, and customers know that their data and cooperation are safe.

BCM is also related to crisis management and risk management. Risk management is about preventing risks and reducing the likelihood of threats occurring. Business continuity management assumes that some incidents cannot be avoided and will occur. It is important to be prepared and able to recover in the event of incidents. Crisis management, on the other hand, deals with managing current situations during a crisis, while BCM ensures that critical functions of the organization continue to function during and after a crisis.

Figure 1 shows how BCM is linked to standards and frameworks that govern how it works.

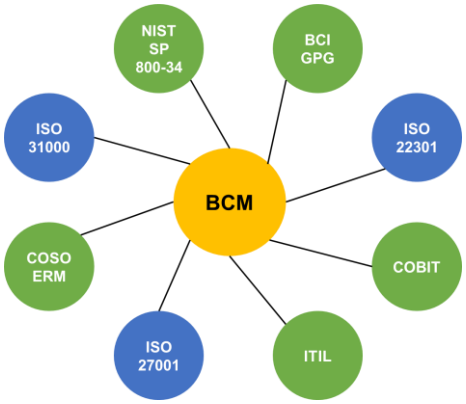


Figure 1 BCM and standards and frameworks

BCM is at the center, acting as a central system to which standards and frameworks are subsequently linked, helping with its development.

Blue indicates standards that must be implemented, and green indicates frameworks that describe how this should be done in practice.

Proper and effective continuity planning is essential in BCM to prepare for various scenarios that may occur and have a negative impact on the normal activities of the organization. For this reason, the output of business continuity management is a business continuity plan (BCP), which is a document containing details designed to ensure that the immediate consequences of a business interruption are managed.

BCP is a comprehensive framework designed to maintain critical business functions and operations during a disaster or disruptive event. Its primary goal is to minimize the impact of disasters on organizations and facilitate a rapid return to normal operations [8, 9].

Scenarios or business continuity plans have four typical categories defined [8]:

1. Sudden unavailability of personnel – this scenario covers situations in which the organization lacks key personnel or a larger number of employees (absences for various reasons, such as contagious disease, strikes, official closure of the building, injury/death of critical personnel, transport restrictions, etc.). The plan should therefore include measures such as staff transfers, crisis teams, cross-training, external replacements, or simplification of processes for the necessary period.
2. Sudden unusability of the workplace/building – certain situations (such as fire, flood, power failure, engineering network failure, road closure, bomb attack, mandatory evacuation of the area, or physical damage to the building) make it impossible to use part or all the organization. The plan should define alternative workplaces (so-called hot sites, warm sites, cold sites), as well as the possibility of working from home, shared spaces with partners, and logistics for moving equipment.
3. Sudden unusability of technology – this is a scenario involving IT infrastructure failure (cyber attacks, power outages, internet outages, software errors, etc.). The BCP must therefore include procedures for system recovery (disaster recovery plan, DRP), data backup and recovery, and communication with the IT department or cloud service providers.
4. Sudden media unavailability – a scenario in which access to physical and digital media containing key information or data is lost (e.g., database damage, loss and destruction of archives, backup failure, etc.). Possible solutions include having multiple backups, geographically diversifying backups, ensuring access to backups from alternative locations, and having defined procedures for restoring and verifying data integrity.

Within the framework of BCP scenarios, an organization does not need to include natural disasters, armed conflicts, or civil unrest, as it cannot influence them. However, in view of the 2019/2020 pandemic (Covid), it is advisable to have scenarios prepared for such situations (at least for pandemics such as Covid-19).

It is equally important to note that the organization's management decides which scenario will be included in the BCP, as each organization has its own limitations that significantly influence the creation of the BCP.

When planning, which is at the core of the entire BCM concept, the organization must determine the requirements for the various resources needed to implement individual business continuity strategies. According to ISO/IEC 22301, it is important to consider the following categories of resources that should be assessed and allocated in the BCP [2]:

- People – consideration of the necessary number of employees (minimum, maximum), their competencies, distribution of tasks, and deadlines for their deployment. Within the BCP, it is important to consider the availability of personnel during crisis situations and the possibility of their substitution, whether by internal or external employees/organizations.
- Information and data – include the identification of critical data and information that is essential for the performance of activities, considering availability, confidentiality, and integrity (the so-called CIA triad), including backup and recovery after an incident.
- Buildings, working environment, and related engineering networks – the BCP must also plan for the availability of premises that will be suitable for the organization to continue operating and the necessary infrastructure (energy, air conditioning, internet, etc.).

- Facilities, equipment, and consumables – the availability of technical equipment (e.g., computers, servers, machinery, and devices, etc.) and necessary materials that are essential for the proper operation of the organization is determined.
- Information and communication technology (ICT) systems (ICT) – critical IT infrastructure must be identified in the BCP, and a method for its protection and recovery within a specified time (recovery time objective, RTO) and with a specified level of data recovery (recovery point objective, RPO) in the event of a disaster/crisis must also be proposed.
- Transport and logistics activities – ensuring the availability of transport and logistics services necessary for the operation of the organization.
- Financing – planning within BCM also includes identifying sources for obtaining funds and subsequently securing them so that the objectives set out in the BCP can be achieved.
- Partners and suppliers – the organization should not forget to assess its dependencies on third parties, as their failure for any reason can significantly affect the organization's operations. Therefore, backup scenarios and alternatives should be defined in the case of suppliers of key components.

The BCM strategy should also include the approval of priority time frames for business recovery and the assessment of third-party capabilities to ensure the continuity of supply chain activities.

The resources identified in ISO 22301 (people, information, buildings, technology, finance, partners) are also relevant to the functioning of SOCs. Personnel capacity, the technological infrastructure of monitoring tools, data availability, and cooperation with external security service providers are essential prerequisites for the effective functioning of security oversight. [10].

To develop a BCM and BCP, it is necessary to analyze the organization's processes, and a business impact analysis (BIA) is used to identify the most important ones that must continue to function. BIA is a key process for identifying and evaluating the business processes necessary to ensure the continuity of the organization. It involves examining business processes to determine the critical operations that are necessary to maintain business operations and assessing the impact of disruptions over time on individual resources. The process requires an understanding of the business environment, data collection, and the preparation of comprehensive reports for review by senior management. Effective implementation of BIA depends on management commitment in terms of resources and agreement to support business continuity management systems. Organizations must regularly review and adapt their BIAs, especially when circumstances change and to remain competitive. Traditional BIA methods rely heavily on qualitative analysis and expert judgment, lacking sufficient theoretical support and quantitative calculations. To address these limitations, researchers have proposed applying the analytical hierarchy process (AHP) to BIA, which provides scientific calculation methods and index systems for more effective business continuity management planning. [11].

It can therefore be said that BIA identifies, qualifies, and quantifies the potential impacts and possible losses in the event of an interruption or disruption of operations across all an organization's processes to identify the organization's key/critical processes. This involves assessing the impacts (economic, reputational, regulatory), threats, and costs of restoring processes in the event of an outage at various intervals from the start of the outage.

According to ISO 22301, ISO/TS 22317, and ISO/IEC 27031, the basic parameters of BIA analysis include [2, 12, 13]:

- Recovery time objective (RTO) – the maximum acceptable time in which a critical process, activity, service, or system must be restored to an acceptable level after a disruption. In other words, the period during which it is necessary to restore the activity, service, or system to minimize the negative impact on the organization.
- Recovery point objective (RPO) – the maximum amount (in terms of time and data volume) that an organization is willing and able to lose. It expresses the data delay that can be expected during recovery. Simply put, how much data can be lost in an incident without unacceptable consequences.

Both parameters are basic outputs of BIA and define the extent to which recovery strategies and infrastructure need to be prepared to ensure business continuity. BIA thus enables the identification of critical processes and the determination of RTO and RPO for them.

For an organization to be sure that what it has stated in its BCP or DRP (disaster recovery plan) can be implemented, it must test these plans. There are several types of testing [2, 12, 14]:

- Failover test – the most realistic and riskiest test, in which the production environment is completely interrupted and planned backup systems and workstations are activated. A complete failure is simulated, and the organization begins to follow the BCP/DRP and use backup systems.
- Parallel tests – the test consists of running the production system concurrently with the backup system, testing the backup system's ability to take over full operation without disrupting the organization's operations.
- Simulation tests – these involve testing using a scenario in which specific incidents are simulated (cyber attack, fire in the server room, network outage, etc.) and a team of people responds to the situation in accordance with the BCP/DRP.
- Theoretical walkthrough – participants (crisis team, cybersecurity manager, IT department, etc.) formally go through all the steps of the BCP/DRP without physical implementation.
- Plan completeness check (table-top) – a less formal test, usually conducted in the form of a discussion exercise at a table, during which various incidents are discussed and how they would be resolved according to the BCP/DRP.

The frequency of testing plans depends on the criticality of activities, systems, and processes; BIA results; regulatory requirements; and the results of previous tests. It is generally recommended to perform control tests in the form of

simulations once a year and after each significant change, and a full interruption test every 2 or 3 years [15].

Testing of continuity plans (failover tests, parallel tests, simulation exercises, table-top tests) should also include the active participation of the SOC. Simulations of cyber incidents, such as ransomware attacks or network compromises, allow for testing not only the functionality of recovery mechanisms, but also the effectiveness of security monitoring detection and response [16].

The integration of BCM and SOC thus creates a comprehensive organizational resilience management system, in which BCM represents a strategic framework for continuity and SOC an operational tool for ensuring it. This connection enables organizations to respond more effectively to modern threats, minimize the impact of incidents, and ensure the stability of critical processes even in conditions of increased uncertainty.

5. CONCLUSION

Business continuity management is now an essential part of managing an organization that wants to be prepared for unexpected situations. It is not just about creating plans, but about a systematic approach to identifying risks, setting priorities, and establishing measures that will enable the organization to continue its key activities even during a crisis.

In the context of increasing digitalization, it is important to link BCM with the activities of the Security Operations Center. While BCM determines the strategic direction and priorities for recovery, SOC ensures a practical and immediate response to cyber incidents. Their cooperation thus increases the organization's ability to cope with technological and security disruptions and contributes to its long-term stability and credibility.

Acknowledgement

Funded by the EU NextGenerationEU through the Recovery and Resilience Plan for Slovakia under the project No. 09I05-03-V02-00010.

REFERENCES

[1] SPEIGHT, P. 2011. ***Business Continuity. Journal of applied security research***, 6(4). https://doi.org/10.1080/19361610.2011.604021

[2] ISO/IEC 22301. (2019). Security and resilience — Business continuity management systems — Requirements. https://www.iso.org/standard/75106.html

[3] HECHT, J. A. 2002. ***Business Continuity Management. Communications of the Association for Information Systems***, vol. 8, 444-450 s. https://doi.org/10.17705/1CAIS.00830

[4] SAVOLAINEN, T. et al. 2024. ***Business Continuity Management of Critical Infrastructures from the Cybersecurity Perspective***. 2024 IEEE Global Engineering Education Conference (EDUCON), Kos Island, Greece, 2024, pp. 1-6, doi: 10.1109/EDUCON60312.2024.10578811.

[5] SRIVASTAVA, K., GHANEM AL HASHMI, W. S. 2023. ***Business continuity management – Significant insights from practice.*** 1., New York, Routledge, pp. 14, https://doi.org/10.4324/9781003304678

[6] VIELBERTH, M. 2020. ***Security Operations Center: A Systematic Study and Open Challenges.*** IEEE Access, vol. 8 pp. 227756-227779, doi: 10.1109/ACCESS.2020.3045514.

[7] SARAIVA, M., MATEUS-COELHO, N. 2022. ***CyberSoc Framework a Systematic Review of the State-of-Art.*** Procedia Computer Science, Volume 204, pp. 961-972, https://doi.org/10.1016/j.procs.2022.08.117

[8] HOLLCROFT, B., LYON, B. 2021. ***Business Continuity Plan, capitol 19 in: Risk Assessment: A Practical Guide to Assessing Operational Risks.*** 2. https://doi.org/10.1002/9781119798323.ch19

[9] KUMAR, A. 2020. ***Business continuity plan.*** South Asian Journal of Engineering and Technology, 10(2), https://doi.org/10.26524/sajet.2020.2.2

[10] FORSBERG, J., FRANTTI, T. 2023. ***Technical performance metrics of a security operations center.*** Computer & Security, Volume 135, https://doi.org/10.1016/j.cose.2023.103529

[11] SKIDAR, P. 2011. ***Alternate Approaches to Business Impact Analysis.*** Information Security Journal: A Global Perspective, 20(3). 128-134 s. https://doi.org/10.1080/19393555.2010.551274

[12] ISO/IEC 27031. (2025). Cybersecurity — Information and communication technology readiness for business continuity. https://www.iso.org/standard/27031#:~:text=ISO/IEC%2027031%20provides%20guidance%20on%20ensuring%20that,ICT%2Drelated%20disruptions%20that%20could%20impact%20critical%20operations

[13] ISO/TS 22317. (2021). Security and resilience — Business continuity management systems — Guidelines for business impact analysis. 2. vydanie. https://www.iso.org/standard/79000.html

[14] NIST SP 800-34. (2010). NIST Special Publication 800-34 Rev. 1. Contingency Planning Guide for Federal Information Systems. https://csrc.nist.gov/pubs/sp/800/34/r1/upd1/final

[15] ZENG, Z., ZIO, E. 2017. ***An integrated modeling framework for quantitative business continuity assessment.*** Process Safety and Environmental Protection, Volume 106, pp. 76-88, https://doi.org/10.1016/j.psep.2016.12.002

[16] ALI, Q. S. A., HANAFIAH, M. H., MOGINDOL, S. H. 2023. ***Systematic literature review of Business Continuity Management (BCM) practices: Integrating organisational resilience and performance in Small and medium enterprises (SMEs) BCM framework.*** International Journal of Disaster Risk Reduction, Volume 99, 104135, https://doi.org/10.1016/j.ijdrr.2023.104135c

Dominika DUPÁKOVÁ, Ing.
Milan KUBINA, prof., Ing., PhD.
Viliam LENDEL, doc., Ing., PhD.
Department of Management Theories, Faculty of Management Science and Informatics, University of Zilina
Univerzitná 8215/2, 010 26 Zilina, Slovak Republic
e-mail: dominika.dupakova@fri.uniza.sk; milan.kubina@fri.uniza.sk; viliam.lendel@fri.uniza.sk

THEORETICAL-ANALYTICAL FRAMEWORK OF A MULTI-TENANT SOC CLOUD SERVICE WITH ML ELEMENTS FOR SUSTAINABLE DIGITAL RISK MANAGEMENT

LINDA FILIPOVIČOVÁ – JAKUB SOVIAR – MARTIN HOLUBČÍK – MARTIN MIČIAK

Abstract: *The advancement of Industry 4.0 increases organizational reliance on cloud-based and interconnected digital infrastructures while significantly intensifying cyber risks. For small and medium-sized enterprises (SMEs), limited financial and human resources make effective cybersecurity management particularly challenging. This paper proposes a theoretical–analytical framework for a multitenant Security Operations Center (SOC) implemented as an open cloud service with integrated machine learning (ML) capabilities, aimed at strengthening cyber resilience, risk management, value creation, and sustainability. The study synthesizes recent research in cloud security, multitenant architectures, artificial intelligence, and managerial perspectives on human capital and stakeholder value. The analysis addresses technological, process, organizational, and economic dimensions of multitenant SOC operation. The findings suggest that cloud-based multitenant SOCs enable SMEs to access advanced security monitoring and incident response capabilities, while ML improves anomaly detection, alert prioritization, and automation efficiency. The paper concludes that a multitenant cloud SOC represents a scalable and sustainable cybersecurity model aligned with the strategic demands of Industry 4.0.*

Keywords: *Multitenant Security Operations Center (SOC), Cloud Computing, Cybersecurity, Machine Learning, Industry 4.0, Risk Management, Sustainability*

JEL Classification: *D8, L8, M15, M21*

1. INTRODUCTION

The development of the Industry 4.0 concept is fundamentally transforming how organizations manage data, processes, and technological infrastructures. Cloud services and artificial intelligence (AI) have become core pillars of digital transformation, while organizations' exposure to cyber risks is increasing rapidly. [1]The transition from isolated information systems to interconnected cyber–physical systems, IoT, and data-driven decision-making significantly raises requirements for the availability, integrity, and confidentiality of information assets. Recent studies confirm that threat complexity in industrial digital ecosystems is growing primarily due to IT/OT integration, extensive connectivity, and the increasing volume of data flows, which elevates cybersecurity to one of the key managerial challenges of Industry 4.0. [2][3][4]

According to Lee & Lim [5] and Jimeno-Morenilla et al. [6], digital transformation is increasingly built upon cloud services, artificial intelligence (AI), and platformization, which accelerate innovation and enable the integration of processes across the value chain. Yaqub & Alsabban [7] and Afrin et al. [8] demonstrate that Industry 4.0 technologies—including cloud computing, data analytics, and intelligent automation—are becoming key enablers of competitiveness and the scalability of business models. However, cloud environments also introduce specific security risks related to virtualization, multitenancy, and shared infrastructure, including challenges associated with tenant isolation, identity and access management, and data protection. [9]

These challenges are particularly pronounced for small and medium-sized enterprises (SMEs), which typically lack the financial and human resources required to operate dedicated security teams and continuous 24/7 monitoring. As cyber threats grow in complexity, SMEs face a tension between technological demands and limited access to specialized expertise. Prior research highlights shortages of cybersecurity skills, constrained budgets, and unclear role distribution when relying on external security providers, emphasizing the increasing importance of human capital management in the context of Industry 4.0. [1][10]

In this context, a multitenant Security Operations Center (SOC) implemented as an open cloud-based service represents a promising cybersecurity model. Such an approach enables multiple organizations to share security infrastructure while maintaining logical (data) tenant isolation, centralized detection management, and standardized protection, response, and reporting capabilities. Research on multitenant and multi-domain security operations architectures suggests that traditional perimeter-based models are no longer sufficient, creating a need for scalable and adaptive SOC-as-a-Service solutions built on SIEM, monitoring platforms, and integrated analytics. [11] At the same time, practical SOC operation relies on a combination of technologies, processes, and people, with a growing need to standardize use-case coverage and detection mapping (e.g., against the MITRE ATT&CK framework) in order to scale monitoring capabilities and service quality across multiple customers. [12]

The effectiveness of cloud-based SOCs is further enhanced by the integration of machine learning (ML), which supports the detection of anomalous behavior and previously unknown attacks in distributed environments where signature-based approaches are insufficient. [13][14] Practical deployments demonstrate that the integration of ML with Security Information and Event Management (SIEM) systems and Intrusion Detection Systems (IDS) and automation tools can improve threat detection, alert

prioritization, and operational efficiency, thereby strengthening organizational resilience. From an economic perspective, this multitenant cloud-based model is significantly more feasible for SMEs than building and operating an in-house SOC. [15]

The objective of this paper is therefore to develop a theoretical–analytical framework that explains how multitenant cloud-based SOCs with AI components support value creation, risk management, and organizational sustainability in the Industry 4.0 environment, while simultaneously linking technological aspects with organizational and managerial determinants. [1] [8]

2. THEORETICAL BACKGROUND

The following theoretical section develops three interrelated dimensions: (1) the technological shift toward multitenant cloud-based security services, (2) the role of machine learning in incident detection and response, and (3) managerial determinants—human capital, risk management, value creation, and sustainability. This framework makes it possible to explain why multitenant cloud-based SOCs make sense not only from a technical perspective, but also from economic and organizational viewpoints—particularly for small and medium-sized enterprises (SMEs).

2.1 Multitenant Cloud-Based SOCs as a New Cybersecurity Model

In recent years, cloud security architectures have increasingly shifted toward Security-as-a-Service models, enabling organizations to leverage advanced security technologies without the need for high capital expenditures or the establishment of fully staffed in-house 24/7 security teams. This trend is particularly relevant for small and medium-sized enterprises (SMEs), which typically lack sufficient human and financial resources to operate their own SOC, yet simultaneously face pressure from Industry 4.0 to digitize processes, integrate data, and adapt rapidly. [1]

A multitenant SOC enables multiple organizations to share a single cloud-based security platform while maintaining logical separation of data, identities, alerts, and incidents. The primary advantages of this approach include scalability, standardized security processes, and economic efficiency achieved through shared infrastructure and centralized operations. These characteristics significantly lower entry barriers to advanced cybersecurity services for SMEs. [17][18]

At the same time, multitenancy introduces specific security and governance challenges, particularly related to tenant isolation, access control, and configuration management across shared environments. Research on cloud-native and multitenant architectures highlights secure isolation and governance of shared components as key challenges that must be addressed to ensure trustworthy SOC operation. [16][19]

From a security operations management perspective, it is important to note that SOC performance is no longer assessed solely by the "number of alerts," but also through measurable technical performance metrics (e.g., detection effectiveness, correlation quality, triage latency, and the ability to validate incidents), which are also critical for performance comparison in SOC-as-a-Service (SOCaaS) models. [20] Consequently, the effectiveness of a multitenant cloud-based SOC depends not only on its infrastructure, but also on its ability to analyze large volumes of security data efficiently, which motivates the integration of machine learning techniques.

2.2 Machine Learning in Cyber Threat Detection

Machine learning (ML) enables the automated analysis of large volumes of security data in real time and supports the identification of behavioral patterns that are difficult to detect using traditional rule- or signature-based approaches. Big Data and artificial intelligence (AI) solutions have also proven effective in other domains—such as education and performance management—where they support personalized decision-making and more accurate predictions. [21] In the SOC context, "personalization" can be interpreted as the adaptation of models and rules to the tenant's specific context (infrastructure, operational characteristics, and risk profile), while a multitenant platform is able to share common knowledge (global attack patterns) and simultaneously preserve tenant-specific deviations. The same principle applies to cybersecurity, where algorithms enable the predictive identification of attacks before their escalation. In cloud-based and multitenant SOC environments, ML is particularly important due to the scale and heterogeneity of generated telemetry data—such as logs, network flows, endpoint events, and cloud audit records—which exceed the capacity of manual analysis. [14]

In security operations, ML techniques are primarily applied to anomaly detection, identification of novel attacker tactics, techniques, and procedures (TTPs), reduction of alert noise, to the detection of anomalous user and system behavior, which is critical for uncovering insider threats and compromised accounts; and to the early identification of advanced persistent threats (APTs) and support for a predictive (rather than purely reactive) security posture. By correlating events across heterogeneous data sources, ML contributes to improved incident contextualization and prioritization within SOC environments. [13]

At the same time, Yan et al. [22] repeatedly emphasize that the practical deployment of ML in cybersecurity must address not only accuracy, but also interpretability, robustness, and operational sustainability of models (e.g., data drift, false positives, and labeling quality). Explainable ML is therefore critical in SOC operations, as it enhances analysts' trust in model outputs and supports the auditability of security decisions.

In practice, ML is commonly integrated with Security Information and Event Management (SIEM) and Security Orchestration, Automation, and Response (SOAR) platforms to translate analytical outputs into automated correlation, triage, and response recommendations. This integration contributes to the emergence of "AI-augmented SOCs," in which AI supports human analysts by improving efficiency and decision-making rather than replacing expert judgment. [23] Nevertheless, effective SOC operation continues to depend on qualified professionals who are able to configure, interpret, and govern ML-driven security processes. Therefore, it is essential to integrate the technological dimension of the SOC with human capital and risk management.

2.3 Human Capital and Risk Management in the Digital Environment

Cybersecurity is not only a technological issue, but also an organizational one. Staffenová et al. [1] emphasize that the effective utilization of human capital in the context of Industry 4.0 is essential for managing complex digital systems. Koman et al. [24] similarly highlight the importance of risk management in human resources information systems, which is directly applicable to SOC environments, where a combination of technological tools and skilled analysts is indispensable.

Cybersecurity represents a complex socio-technical system in which technology and human decision-making mutually influence one another. Key factors include human competencies, process design, governance, accountability, and decision-making under pressure. Staffenová et al. [1] point out that in Industry 4.0 environments, human capital becomes a critical success factor, as organizations must possess digital, analytical, and security-related competencies.

At the same time, Koman et al. [24] stress that risk management in human resources information systems is essential for ensuring data integrity, personal data protection, and the credibility of decision-making processes. This principle directly translates into SOC operations, where the combination of analysts, automated tools, and decision-making workflows determines an organization's ability to manage security incidents effectively.

In small and medium-sized enterprises (SMEs), this dimension is even more pronounced, as a single individual often covers multiple roles (IT, security, compliance). Consequently, it is crucial that externally provided security services (SOC-as-a-Service, Security Operations Center as a Service – SOCaaS) are designed with the client's actual operational capacity in mind. In the SOC context, this translates into the need for clearly defined roles (who performs triage, who escalates, who approves responses), as well as training and incident-handling routines. Moreover, Hoong and Rezania [10] demonstrate that SMEs face a significant shortage of cybersecurity experts, which further increases the importance of outsourcing and cloud-based SOC models as a means of accessing advanced expertise.

Research on Security-as-a-Service adoption further indicates that post-adoption effectiveness depends on how well organizations integrate external security services with their internal resources and decision-making practices. For multitenant SOCs, this highlights the importance of structured provider–client interfaces, including Service Level Agreements (SLAs), communication mechanisms, and shared situational awareness. [25] Ultimately, the integration of technology and human capital determines an organization's ability to manage cyber risks, build stakeholder trust, and ensure long-term resilience.

2.4 Value Creation and Sustainability through Security

In contemporary business environments, cybersecurity is increasingly perceived as an integral component of organizational value creation rather than merely as a cost factor. Kusnirova et al. [26] demonstrate that managerial activities focused on value creation and stakeholder relationship management increase value for both suppliers and customers; cybersecurity directly contributes to this process as a mechanism for risk reduction and increased process transparency (e.g., incident response, reporting, and auditing). Effective security practices support customer and partner trust, reduce operational disruptions, and protect digital assets that form the core of products and services in the context of Industry 4.0.

From the perspective of corporate value, empirical findings also suggest that cybersecurity governance can be positively associated with firms' market value, operating through a reputational mechanism based on investor and partner trust. [28] This is particularly important for SMEs operating within supply chains, where cybersecurity maturity increasingly becomes a prerequisite for collaboration, driven by compliance requirements imposed by larger partners.

Demjanovicová and Varmus [27] further argue that the shift in corporate value orientation toward environmental sustainability is transforming how firms perceive risk management, including digital risks that may have secondary environmental impacts (e.g., operational disruptions, inefficiencies, and incidents in operational technology environments). From a sustainability perspective, Demjanovicová and Varmus [27] emphasize that the protection of digital assets and the reduction of operational risks are integral components of responsible business conduct. Cloud-based SOCs, as noted by Kurunthachalam [29], also contribute to environmental sustainability, as shared infrastructure leads to lower energy consumption and more efficient resource utilization compared to isolated, enterprise-specific solutions. The linkage between security and sustainability is further reflected in academic research on "green" cloud computing and data centers, which systematically examine energy efficiency and techniques for reducing environmental impact. [30]

3. ANALYTICAL PART

While the theoretical section explained why a multitenant cloud-based SOC (SOC-as-a-Service) with AI/ML elements appears to be a suitable response to the challenges of Industry 4.0, the following analytical chapter examines how these principles are reflected in practice. The analysis therefore integrates a technological perspective (architecture, automation, detection), an economic perspective (cost efficiency, scalability), and an organizational–managerial perspective (competencies, processes, human factors, and performance measurement).

3.1 Analytical Framework and Dimensions

The analysis examines multitenant SOCs as open cloud-based services through four interrelated dimensions: the technological dimension (secure multitenancy, continuous monitoring, correlation, and automation), the process dimension (standardization of detection use cases, triage, and incident response), the human and competency dimension (the transformation of analyst roles through automation and AI), and the economic and sustainability dimension (cost efficiency, scalability, and resource utilization). [1][31][32][33] Together, these dimensions provide a structured framework for evaluating how multitenant SOCs scale security operations while maintaining service quality and organizational feasibility.

3.2 Analysis of Multitenant SOCs as Open Cloud-Based Services

The analysis indicates that multitenant SOCs combine technological efficiency with economic and organizational sustainability by operating a unified security platform for multiple organizations, while ensuring tenant isolation and access control at both architectural and governance levels.

From a technological perspective, in cloud environments, the volume of telemetry data (logs, audit records, network flows, endpoint events) is so high that manual oversight becomes unsustainable. A modern cloud-based SOC therefore relies on the integration of Security Information and Event Management (SIEM) systems (data collection, normalization, and correlation) with Security Orchestration, Automation, and Response (SOAR) platforms (orchestration and automated playbooks), and increasingly also with Extended Detection and Response (XDR) and Endpoint Detection and Response (EDR) solutions. Research on cloud security automation emphasizes that modular architectures integrating SIEM, SOAR, and threat intelligence can improve detection capabilities while simultaneously reducing response times in dynamic cloud infrastructures. [34]

Machine learning further supports SOC efficiency by enabling automated triage, anomaly detection, and alert prioritization. By reducing the volume of routine decisions handled by analysts, ML lowers the risk of missed incidents during periods of overload. At the same time, Tilbury and Flowerday [35] and Tariq et al. [36] caution that automation also introduces risks—most notably alert fatigue, automation bias, and complacency. For this reason, automation must be designed as a model of human–automation collaboration rather than as a blind replacement of analysts.

From a process perspective, multitenant SOCs must scale not only the number of clients, but also the consistency and quality of detection and response. This requires standardized detection use cases, systematic mapping of coverage to attacker tactics and techniques (e.g., MITRE ATT&CK), and continuous identification of coverage gaps. Without structured use-case management, detection quality across tenants may become uneven, which is particularly critical in SOC-as-a-Service models subject to Service Level Agreements (SLAs). [37]

The demonstrability of SOC value is closely linked to performance measurement. Effective SOC evaluation therefore relies on technical performance metrics—such as detection capability, correlation quality, and triage efficiency—rather than on alert volumes alone. These metrics are essential for assessing the real contribution of SOC operations to organizational security posture and for ensuring comparability across tenants. [20]

3.3 Organizational and HR Perspective: Shifting from "Operations" to Strategic Competencies

From an organizational and human resource perspective, cloud-based SOCs enable a shift from routine operational tasks toward more strategic cybersecurity competencies. Automated monitoring, correlation, and response activities reduce the need for continuous manual intervention, allowing organizations to focus internal capacities on risk prioritization, security governance, compliance, and the development of a security-oriented organizational culture. Tilbury and Flowerday [35], in their work on human–automation collaboration in SOC environments, further emphasize that the maximum benefits of automation are achieved when analysts are involved in the design of automation and when clear boundaries of autonomy are defined (i.e., when the system recommends actions versus when it executes them). This shift toward strategic competencies aligns with the concepts of intelligent innovation systems, which support rapid adaptation and continuous innovation within organizations. [17]

3.4 Synthesis of Analytical Findings

The analytical findings suggest that multitenant cloud-based SOCs represent a feasible and effective model for enhancing cybersecurity resilience in SMEs. Technologically, this model enables scalable monitoring, event correlation, and incident response through the integration of SIEM, SOAR, ML-based analytics and threat intelligence tools. [34] From a process perspective, standardized detection use cases and systematic performance measurement contribute to consistent service quality across multiple tenants. Organizationally, the multitenant SOC model allows SMEs to reallocate limited human resources from routine operational tasks toward strategic risk management and governance activities. [35] The value of multitenant SOCs is also more readily demonstrable through technical SOC performance metrics, such as detection effectiveness, response time, and the degree of response automation. [20] Analyzing multitenant SOCs as open cloud-based services shows that this model combines technological efficiency with economic and organizational sustainability. The use of machine learning enables the automation of security processes, thereby reducing reliance on manual interventions, increasing the consistency of responses, and minimizing the risk of human error. From a human resource management perspective, cloud-based SOCs allow organizations to focus on strategic competencies rather than operational tasks, which aligns with the concepts of intelligent innovation systems. [17]

4. DISCUSSION

The findings of the theoretical and analytical sections indicate that multitenant cloud-based SOCs represent a significant instrument for strengthening the digital resilience of organizations. In the context of small and medium-sized enterprises (SMEs), these solutions help overcome barriers related to costs, the shortage of cybersecurity experts, and technological complexity, as identified by Staffenová et al. [1]. From a value creation perspective, cloud-based SOCs enhance stakeholder trust, improve business continuity, and support sustainable managerial decision-making. [26][27]

The analytical part demonstrated that multitenant cloud-based SOCs (as open services) combine the advantages of scalability, shared infrastructure, and the automation of security processes. This discussion interprets these findings in the broader context of Industry 4.0 and focuses on their implications for SME digital resilience, SOC process maturity, the human factor, and stakeholder value.

The results of the theoretical analysis confirm that the shift toward Industry 4.0 (IT/OT convergence, Industrial Internet of Things – IIoT, and pervasive connectivity) creates an environment in which cybersecurity becomes not only a

technical issue, but also a managerial and strategic one. In this context, an organization's ability to maintain operational continuity during security incidents represents a key component of digital resilience. The concept of "cyber resilience" in recent literature has evolved from isolated security controls toward a holistic approach encompassing preparedness, detection, response, and recovery, which aligns with the role of SOCs as mechanisms of continuous monitoring and operational incident management. [38]

From a practical perspective, the discussion highlights that multitenant cloud-based SOCs are particularly valuable for SMEs when they reduce three major barriers: costs, shortage of experts, and technological complexity. [1] This value is especially evident in the shortened time required to implement core SOC functions (log collection, correlation, triage) and in the accessibility of advanced capabilities (e.g., automated response), which SMEs would otherwise deploy much more slowly—or not at all—when operating an in-house SOC. Aproyable et al. similarly focus on SMEs and demonstrate that cybersecurity resilience in practice depends on a combination of technological and organizational mechanisms—namely, the ability to learn from incidents, understand risk, and develop procedures for managing it. [39]

The process dimension of multitenant SOCs is also critically important. The objective is not merely to "scale the number of clients," but to scale a consistent quality of detection and response. Research on SOC use-case management (coverage and gap analysis) shows that without systematic governance of detection scenarios and coverage mapping (e.g., to MITRE ATT&CK), detection gaps and uneven service quality emerge—an issue that is particularly critical in the SOC-as-a-Service model due to Service Level Agreements (SLAs) and provider credibility. The analytical findings further indicate that the integration of AI and ML significantly enhances SOC efficiency, particularly in triage, correlation, and noise reduction (alert fatigue). At the same time, Giarimpampa et al. [40] caution that AI in SOCs should not be understood merely as increased automation, but rather as an augmentation of analysts' work and decision-making—especially through interpretability of outputs, controlled autonomy, and sound process integration. Systematic reviews of AI applications in SOCs confirm the growing importance of AI for security operations, while also identifying persistent challenges such as model validation, reliability in production environments, data drift, explainability, and the risk of false positives. [41]

Finally, this study emphasizes that a multitenant cloud-based SOC is not only a technical architecture, but also a governance model that must be designed to support clear role separation between the service provider and the client, tenant isolation mechanisms, auditability and reporting, process anchoring of incident response (escalation paths, playbooks, post-incident learning), and measurable SOC performance. Key performance indicators include metrics such as Mean Time to Detect (MTTD) and Mean Time to Respond (MTTR), the accuracy of correlation rules, and the success rate of automated responses. SOC performance measurability is essential not only for justifying investments, but also for ensuring service comparability across tenants; systematically applied, technically oriented SOC metrics enable organizations to link "what the SOC does" with "its impact on risk." [41][42]

From a value creation perspective, cloud-based SOCs enhance stakeholder trust, improve business continuity, and support sustainable managerial decision-making. [26][27] This argument is further supported by empirical research indicating that cybersecurity governance can be positively associated with firms' market value, operating through reputational effects and increased trust among investors and supply chain partners—particularly in contexts where trust and legitimacy are critical. [28]

Despite these benefits, several limitations of this study must be acknowledged. First, the multitenant SOC concept presupposes robust tenant isolation mechanisms and a high level of governance; if these elements are not strictly implemented, risks may increase (e.g., data leakage between tenants or erroneous sharing of incident context). Second, the integration of AI and ML within SOCs is highly sensitive to data quality and operational conditions (such as data drift, availability of labeled data, and interpretability of outputs), which—if insufficiently managed—may lead to false positives or "blind spots" in detection. [40][41]

Additional limitations should also be considered. Third, the effectiveness of multitenant SOCs may vary significantly depending on the maturity of the client organization; SMEs with low security awareness or poorly defined internal processes may not fully benefit from advanced SOC capabilities, even when these are technically available. Fourth, the reliance on standardized detection use cases and shared threat intelligence, while beneficial for scalability, may reduce sensitivity to highly specific or sector-specific threats if tenant-level customization is insufficient. Finally, regulatory and legal constraints—particularly related to data residency, cross-border data processing, and compliance requirements—may limit the applicability of multitenant SOC models in certain industries or jurisdictions.

Based on these findings, several relevant directions for future research emerge. Future studies could focus on quantifying the benefits of multitenant SOCs for SMEs using measurable indicators such as Mean Time to Detect (MTTD), Mean Time to Respond (MTTR), detection accuracy, reduction of alert fatigue, and costs associated with incident handling. [39] Another promising research direction involves the design of a standardized framework for evaluating security use-case coverage and gap analysis in the SOC-as-a-Service model, including systematic mapping to the MITRE ATT&CK framework and the definition of recommended Key Performance Indicators (KPIs). Further attention should also be devoted to empirical validation of organizational success factors for multitenant SOCs, particularly in the areas of competency models, interfaces between SOC providers and clients, governance structures, and mechanisms for post-incident organizational learning. [38] Finally, a particularly promising avenue for future research is the evaluation of "AI-augmented SOC" approaches in production environments, with a focus on their reliability, decision explainability, and the security of the AI components themselves. [40]

5. CONCLUSION

The objective of this article was to develop a theoretical–analytical framework explaining how a multitenant

cybersecurity operations center (SOC), implemented as an open cloud-based service with machine learning components, can support digital resilience, risk management, value creation, and organizational sustainability in the context of Industry 4.0. This objective was achieved through a synthesis of contemporary scientific knowledge from the domains of cloud security, artificial intelligence, human capital management, and value-oriented management.

The theoretical part demonstrated that the digitalization of industrial and business systems significantly increases organizations' dependence on the availability, integrity, and confidentiality of digital assets. In this context, cybersecurity shifts from a purely technical support function toward the level of strategic risk management. Cloud-based and multitenant architectures simultaneously enable a new model of security service delivery—as a scalable, economically accessible, and technologically advanced alternative to traditional on-premises SOC solutions.

The analytical part subsequently showed that a multitenant cloud-based SOC can effectively combine technological efficiency (automated data collection, event correlation, and incident response), process standardization (use-case management, threat coverage, and performance metrics), and organizational sustainability (the reallocation of human resources from routine operational tasks toward strategic cybersecurity management). The integration of machine learning further enhances detection accuracy and reduces analyst workload, thereby improving organizations' ability to respond to dynamic and evolving threats.

As a result, a multitenant cloud-based SOC can be interpreted as a mechanism of digital resilience that is particularly relevant for small and medium-sized enterprises (SMEs). These organizations gain access to security capabilities that would otherwise exceed their financial and human resource capacities, while simultaneously increasing their credibility toward customers, partners, and regulators. From a value management perspective, SOCs support business continuity, transparency, and stakeholder trust, which translate into long-term competitiveness and sustainability.

A multitenant cybersecurity operations center delivered as an open cloud-based service with machine learning components represents a strategic instrument of digital transformation in the era of Industry 4.0. It integrates technological innovation (scalable cloud platforms, automated triage and response), effective risk management (continuous monitoring, standardized use cases, performance measurement), human capital development (a shift from routine operations toward strategic competencies), and value creation for stakeholders (trust, reputation, and continuity).

From a scientific perspective, this article contributes to the expansion of knowledge by linking SOC technological architecture with organizational and value-oriented dimensions of enterprise management. It demonstrates that cybersecurity in the context of Industry 4.0 is not an isolated IT function, but an integral part of strategic management, human capital development, and value creation. The findings further confirm that the benefits of cloud-based SOCs for SMEs are maximized when SOCs are designed as a combination of technology and processes—supported by systematic use-case management and gap analysis, as well as a clearly defined governance interface between the service provider and the client. Cyber resilience is increasingly becoming a decisive factor of sustainable organizational performance and may directly influence an organization's reputation and value.

From a practical perspective, this article provides a conceptual foundation for the design and evaluation of multitenant SOC solutions that can be utilized by security service providers, SME managers, and policymakers involved in digital transformation initiatives. In this way, the article fulfills its objective not only theoretically but also in applied terms—as a framework for understanding and implementing cloud-based SOCs as a key element of a secure and sustainable digital economy.

Acknowledgement

Funded by the EU NextGenerationEU through the Recovery and Resilience Plan for Slovakia under the project No. 09I05-03-V02-00010.

REFERENCES

[1] STAFFENOVÁ, N., KUCHARCIKOVÁ, A., FALÁT, L. Using of human capital management in small and medium-sized enterprises in context of Industry 4.0. 2025. [online]. [cit. 19-01-2026]. Available at: https://journals.plos.org/plosone/article?id=10.1371/journal.pone.0320568

[2] CORALLO, A. et al. Cybersecurity awareness in the context of the Industrial Internet of Things: A systematic literature review. 2022. [online]. [cit. 19-01-2026]. Available at: https://www.sciencedirect.com/science/article/pii/S0166361522000094

[3] HARKAT et al. Cyber-physical systems security: A systematic review. 2024. [online]. [cit. 19-01-2026]. Available at: https://www.sciencedirect.com/science/article/pii/S0360835224000123

[4] OKS, S.J. et al. Cyber-Physical Systems in the Context of Industry 4.0: A Review, Categorization and Outlook. 2022. [online]. [cit. 19-01-2026]. Available at: https://link.springer.com/article/10.1007/s10796-022-10252-x

[5] LEE, C.; LIM, C. From technological development to social advance: A review of Industry 4.0 through machine learning. 2021. [online]. [cit. 19-01-2026]. Available at: https://www.sciencedirect.com/science/article/pii/S0040162521000858

[6] JIMENO-MORENILLA, A. et al. Technology enablers for the implementation of Industry 4.0 to traditional manufacturing sectors: A review. 2021. [online]. [cit. 19-01-2026]. Available at: https://www.sciencedirect.com/science/article/pii/S0166361520306242

[7] YAQUB, M.Z.; ALSABBAN, A. Industry-4.0-Enabled Digital Transformation: Prospects, Instruments, Challenges, and Implications for Business Strategies. 2023. [online]. [cit. 19-01-2026]. Available at: https://www.mdpi.com/2071-1050/15/11/8553

[8] AFRIN, S. et al. Industrial Internet of Things: Implementations, challenges, and potential solutions across various industries. 2025. [online]. [cit. 19-01-2026]. Available at: https://www.sciencedirect.com/science/article/pii/S016636152500082X
[9] PARAST, F.K. et al. Cloud computing security: A survey of service-based models. 2022. [online]. [cit. 19-01-2026]. Available at: https://www.sciencedirect.com/science/article/pii/S0167404821003977
[10] HOONG, Y.; REZANIA, D. Balancing talent and technology: Navigating cybersecurity and privacy in SMEs. 2024 [online]. [cit. 19-01-2026]. Available at: https://www.sciencedirect.com/science/article/pii/S2772503024000379
[11] REPETTO, M. et al. An architecture to manage security operations for digital service chains. 2021. [online]. [cit. 19-01-2026]. Available at: https://www.sciencedirect.com/science/article/pii/S0167739X20303290
[12] CHAMKAR, S.A. et al. Security Operations Centers: Use Case Best Practices, Coverage, and Gap Analysis Based on MITRE Adversarial Tactics, Techniques, and Common Knowledge. 2024. [online]. [cit. 19-01-2026]. Available at: https://www.mdpi.com/2624-800X/4/4/36
[13] HE, Z. Machine Learning for Cybersecurity: A Survey of Applications, Adversarial Challenges, and Future Research Directions. 2025. [online]. [cit. 19-01-2026]. Available at: https://www.mdpi.com/2079-9292/14/23/4563
[14] KHAN, A.Q. Knowledge-based anomaly detection: Survey, challenges, and future directions. 2024. [online]. [cit. 19-01-2026]. Available at: https://www.sciencedirect.com/science/article/pii/S0952197624011540
[15] MUHAMMAD, A.R et al.. Integrated Security Information and Event Management (SIEM) with Intrusion Detection System (IDS) for Live Analysis based on Machine Learning. 2023. [online]. [cit. 19-01-2026]. Available at: https://www.sciencedirect.com/science/article/pii/S1877050922024243
[16] THEODOROPOULOS, T. et al. Security in Cloud-Native Services: A Survey. 2023. [online]. [cit. 19-01-2026]. Available at: https://www.mdpi.com/2624-800X/3/4/34
[17] LENDEL, V., SPALEKOVÁ, D., LENDELOVÁ, L., SOTEK, M. The Innovative Intelligence System—A Tool for Discovering Innovative Opportunities and for Ensuring the Sustainability and Business Prosperity. 2021. [online]. [cit. 19-01-2026]. Available at: https://www.mdpi.com/2071-1050/13/21/12305
[18] KUMAR, R. Multi-Tenant SaaS Architectures: Design Principles and Security Considerations. 2020. [online]. [cit. 19-01-2026]. Available at: https://www.researchgate.net/publication/391673039_Multi-Tenant_SaaS_Architectures_Design_Principles_and_Security_Considerations
[19] OLABANJI, D.O. et al. Multi-tenancy in cloud-native architecture: a systematic mapping study. 2023. [online]. [cit. 19-01-2026]. Available at: https://researchportal.port.ac.uk/en/publications/multi-tenancy-in-cloud-native-architecture-a-systematic-mapping-s/
[20] FORSBERG, J; FRANTTI, T. Technical performance metrics of a security operations center. 2023. [online]. [cit. 19-01-2026]. Available at: https://www.sciencedirect.com/science/article/pii/S016740482300439X
[21] MICIAK, M., TOMAN, D., ADÁMIK, R., KUFOVÁ, E., SKULEC, B., MOZOLOVÁ, N., HOFEROVÁ, A. Effective Education System for Athletes Utilising Big Data and AI Technology. 2025. [online]. [cit. 19-01-2026]. Available at: https://www.mdpi.com/2306-5729/10/7/102
[22] YAN, F. et al. Explainable machine learning in cybersecurity: A survey. 2022. [online]. [cit. 19-01-2026]. Available at: https://dl.acm.org/doi/abs/10.1002/int.23088
[23] SRINIVAS, S. et al. AI-Augmented SOC: A Survey of LLMs and Agents for Security Automation. 2025. [online]. [cit. 19-01-2026]. Available at: https://www.mdpi.com/2624-800X/5/4/95
[24] KOMAN, G., TOMAN, D., JANKAL, R., BORSOS, P. Risk management in a human resources information system. 2023. [online]. [cit. 19-01-2026]. Available at: https://www.researchgate.net/publication/374330778_Risk_management_in_a_human_resources_information_system
[25] VEDADI, A. et al. Investigating the role of internal security resources in post-adoption satisfaction with the Security-as-a-Service model: an organizational mindfulness perspective. 2023. [online]. [cit. 19-01-2026]. Available at: https://www.sciencedirect.com/org/science/article/abs/pii/S1741039823000013
[26] KUSNIROVA, D., DURISOVA, M., BUBELINY, O. Enhancing Stakeholder Value: Managerial Activities in the Value Creation Process for Suppliers and Buyer—Evidence from Slovak Enterprises. 2024. [online]. [cit. 19-01-2026]. Available at: https://www.mdpi.com/2076-3387/14/8/186
[27] DEMJANOVICOVÁ, M., VARMUS, M. Changing the Perception of Business Values in the Perspective of Environmental Sustainability. 2021. [online]. [cit. 19-01-2026]. Available at: https://www.researchgate.net/publication/351420187_Changing_the_Perception_of_Business_Values_in_the_Perspective_of_Environmental_Sustainability
[28] TAN, W. et al. Cybersecurity governance and corporate market value: Perspectives from investor trust and supply chain trust. 2025. [online]. [cit. 19-01-2026]. Available at: https://www.sciencedirect.com/science/article/pii/S0927538X24003986
[29] KURUNTHACHALAM, A. Sustainable Cloud Computing: Energy Efficiency and Environmental Impact. 2025. [online]. [cit. 19-01-2026]. Available at: https://www.researchgate.net/publication/399099909_Sustainable_Cloud_Computing_Energy_Efficiency_and_Environmental_Impact
[30] KATAL, A. et al. Energy efficiency in cloud computing data centers: a survey on software technologies. 2022. [online]. [cit. 19-01-2026]. Available at: https://pmc.ncbi.nlm.nih.gov/articles/PMC9424070/
[31] PANDI, M. AI-Enhanced Cloud Security Operations Center for Automated Cyber Threat Defense. 2025. [online]. [cit. 19-01-2026]. Available at: https://www.researchgate.net/publication/396214645_AI-Enhanced_Cloud_Security_Operations_Center_for_Automated_Cyber_Threat_Defense
[32] VIELBERTH, M. Security Operations Center: A Systematic Study and Open Challenges. 2020. [online]. [cit. 19-01-2026]. Available at: https://www.researchgate.net/publication/347520429_Security_Operations_Center_A_Systematic_Study_and_Open_Challenges
[33] ALBANESE, M. Towards AI-Driven Human-Machine Co-Teaming for Adaptive and Agile Cyber Security Operation Centers. 2025. [online]. [cit. 19-01-2026]. Available at: https://arxiv.org/abs/2505.06394

[34] PITKAR, H. Cloud Security Automation Through Symmetry: Threat Detection and Response. 2025. [online]. [cit. 19-01-2026]. Available at: https://www.mdpi.com/2073-8994/17/6/859
[35] TILBURY, J.; FLOWERDAY, S. Humans and Automation: Augmenting Security Operation Centers. 2024. [online]. [cit. 19-01-2026]. Available at: https://www.mdpi.com/2624-800X/4/3/20
[36] TARIQ, S. et al. Alert Fatigue in Security Operations Centres: Research Challenges and Opportunities. 2025. [online]. [cit. 19-01-2026]. Available at: https://dl.acm.org/doi/10.1145/3723158
[37] CHAMKAR, S.A. et al. Security Operations Centers: Use Case Best Practices, Coverage, and Gap Analysis Based on MITRE Adversarial Tactics, Techniques, and Common Knowledge. 2024. [online]. [cit. 19-01-2026]. Available at: https://www.mdpi.com/2624-800X/4/4/36
[38] World Economic Forum. Unpacking Cyber Resilience. White Paper. 2024. [online]. [cit. 19-01-2026]. Available at: https://www3.weforum.org/docs/WEF_Unpacking_Cyber_Resilience_2024.pdf
[39] ARROYABLE, J.C.F. et al. Cybersecurity Resilience in SMEs. A Machine Learning Approach. 2023. [online]. [cit. 19-01-2026]. Available at: https://www.tandfonline.com/doi/full/10.1080/08874417.2023.2248925
[40] GIARIMPAMPA, D. et al. Exploring the Role of Artificial Intelligence in Enhancing Security Operations: A Systematic Review. 2025.[online]. [cit. 19-01-2026]. Available at: https://dl.acm.org/doi/10.1145/3747587
[41] FORSBERG, G. Situational Awareness in a Multi-Tenant Security Operations Center - The Role of Information Flow during Alert Investigations: A Qualitative Analysis. 2025. [online]. [cit. 19-01-2026]. Available at: https://www.diva-portal.org/smash/get/diva2%3A1981730/FULLTEXT01.pdf
[42] VAHTERI, K. Framework for SOC performance metrics and enhancement. 2025 [online]. [cit. 19-01-2026]. Available at: https://www.utupub.fi/bitstream/10024/194608/1/Vahteri_Kari_Thesis.pdf

Linda FILIPOVIČOVÁ, Ing,
Jakub SOVIAR, prof. Mgr., PhD.
Martin HOLUBČÍK, Ing., PhD.
Martin MIČIAK, Ing., PhD.
University of Žilina, Faculty of Informatics and Management Science, Department of managerial theories
Univerzitná 8215/1, 010 26 Žilina, Slovakia
e-mail: linda.filipovicova@stud.uniza.sk; jakub.soviar@stud.uniza.sk; martin.holubcik@fri.uniza.sk; martin.miciak@stud.uniza.sk

MODERN INFORMATION SYSTEMS AS A TOOL FOR MANAGERIAL DECISION SUPPORT

IVANA GABRIŠOVÁ – GABRIEL KOMAN – LUCIE LENDELOVÁ

Abstract: *The increasing complexity and dynamism of the contemporary business environment place growing demands on organizations to process information efficiently and support managerial decision-making with timely, reliable insights. Modern information systems are therefore evolving from traditional tools for data processing into intelligent, integrated platforms that actively support strategic and operational decisions. This article aims to analyze the theoretical foundations of information systems and to identify key technological trends shaping modern information systems, with particular emphasis on their role in managerial decision support. The study adopts a qualitative research design based on structured content analysis of selected academic and professional sources in the field of information systems. The analyzed corpus includes thirteen relevant publications meeting predefined criteria of thematic relevance, academic quality, timeliness, and geographical diversity. Identified trends were evaluated based on their frequency of occurrence across sources and subsequently synthesized into broader thematic categories. The findings indicate that cloud-based solutions represent the dominant trend in modern information systems, reflecting a shift toward service-oriented, scalable, and flexible architectures. Other significant trends include the Internet of Things, artificial intelligence and machine learning, big data analytics, mobile compatibility, and cybersecurity. Together, these trends highlight the transformation of information systems into intelligent, data-driven platforms capable of real-time analysis and adaptive behavior. The results underscore the growing importance of cloud-based information system architectures as foundational enablers of advanced decision support, including cybersecurity-oriented solutions integrating machine learning capabilities. The study contributes to existing literature by providing an integrative overview of key information system trends and their implications for managerial decision-making in modern organizations.*

Keywords: *Information Systems, Managerial Decision Support, Cloud-Based Systems, Digital Transformation, Artificial Intelligence, Cybersecurity*

JEL Classification: *M15*

1. INTRODUCTION

The contemporary business environment is characterized by a high degree of dynamism, globalization, and continuously changing market conditions. Organizations are under increasing pressure to remain flexible, respond rapidly, and process information effectively, whether due to unexpected events such as the COVID-19 pandemic or the impact of gradually evolving customer behavior. In this context, the ability to work with data has become a key prerequisite for sustaining long-term organizational competitiveness (Li & Liu, 2014; Batra, 2022).

Information systems are an integral part of organizational management in the modern economy. They not only enable the collection, storage, and processing of data but, more importantly, transform it into relevant information that can be used in managerial decision-making processes (Aminuddin Hamdat et al., 2024). The role of information systems is gradually shifting from operational process support to strategic decision support, while their functionality is increasingly influenced by current technological trends, particularly cloud-based architectures, advanced analytics, and intelligent data-processing capabilities. These developments are a primary driver of modern information systems, which are evolving from traditional tools for data recording and processing into intelligent systems that actively support managerial decision-making. This evolution is characterized by the intensive integration of emerging technologies that enhance system responsiveness to changing conditions and enable the provision of relevant information in real time (Taherdoost, 2022; Selvarajan & Guru, 2022).

Despite extensive research on managerial information systems, there remains a lack of integrative studies systematically linking technological trends with managerial decision support. To address this gap, the aim of this article is to analyze the theoretical foundations of information systems and to identify the key trends shaping modern information systems, with a focus on supporting managerial decision-making in organizations.

2. THEORETICAL BACKGROUND

2.1 Information Systems

Information systems can be conceptualized as socio-technical systems that integrate both technical and human elements to support organizational activities. In this perspective, an information system consists of interrelated components, including hardware, software, data, people, and procedures, which work together to collect, store, process, and disseminate information that supports organizational functions and decision-making processes (Gantz & Philpott, 2013). Such systems are deliberately structured to organize information into a coherent whole, enabling effective interpretation and application of data across different functional areas of an organization. The socio-technical view emphasizes that information systems are not merely technological artefacts, but complex

combinations of technology, people, and processes in which human, organizational, and technical factors are closely linked (Polojärvi et al., 2023). The integration of these components allows organizations to streamline processes, reduce operational costs, eliminate redundant administrative activities, and improve the quality of managerial decision-making by providing timely and relevant information. As organizations increasingly leverage information systems to support planning, control, and decision processes, the ability of these systems to transform raw data into actionable insights has become a key determinant of competitive advantage and operational efficiency. This integrated view underscores the role of information systems not only as support mechanisms for routine operations, but also as enablers of strategic information use in organizational contexts (Hananiya et al., 2024).

For information systems to function effectively, they must satisfy a range of qualitative criteria that extend beyond basic data processing. An important dimension of system quality, as identified in established IS evaluation frameworks, includes the capacity to integrate data from multiple heterogeneous sources into a unified view that supports coherent analysis and decision-making (Delone & McLean, 2003). Closely related to this is the ability to present information through multiple data views tailored to different user roles, which enhances system usefulness across organizational layers by ensuring that users see information in formats relevant to their specific tasks. Information systems provide advanced analytical and reporting tools that assist in interpreting complex datasets and generating actionable insights. The quality of information produced, in terms of relevance, timeliness, and completeness, is crucial for supporting managerial decisions and evaluating organizational performance (Petter et al., 2008). Advanced analytical and reporting capabilities further enable managers to interpret complex datasets and generate actionable insights, especially in dynamic and time-sensitive environments (Watson et al., 2009). Information systems provide mobile access to data and decision-support functionalities, enabling ubiquitous information use and timely responses regardless of location (Gebauer et al., 2010).

2.2 Management Information Systems

Management information systems play a fundamental role in supporting managerial control, planning, and decision-making within organizations. Their primary purpose is to transform data generated by transaction processing systems into structured and summarized information that enables managers to monitor organizational performance, analyze trends, and make informed decisions (Filip, 2007). By providing timely, accurate, and relevant information, management information systems serve as an essential link between operational activities and managerial decision processes. Management information systems are characterized by their ability to aggregate data from multiple organizational sources, support multidimensional analyses, and provide analytical tools for performance evaluation and decision support. They increasingly incorporate forecasting functions, scenario analysis, and simulations of decision impacts, thereby supporting both tactical and strategic planning activities (Dursun, 2010). Management information systems extend beyond basic operational reporting and contribute to higher-level managerial insight and organizational learning.

Management information systems are commonly conceptualized as an analytical layer built upon existing organizational information systems. They integrate data from various functional areas, such as finance, production, marketing, and human resources, into a unified analytical environment that supports consistent interpretation and coordinated decision-making across management levels. They enhance managerial visibility, improve coordination, and support evidence-based decision-making in complex organizational settings (Alter, 2008).

2.3 Cloud-Based Information Systems

Cloud-based information systems represent a significant evolutionary step in the development of management information systems. Unlike traditional on-premise solutions, cloud-based systems deliver information system functionality as a service, enabling flexible access to data and applications through internet-based platforms. This deployment model supports scalability, resource optimization, and cost efficiency, while reducing the need for extensive in-house infrastructure and capital investment (Marston et al., 2009; Armbrust et al., 2010).

The adoption of cloud-based information systems has been driven by the growing demand for real-time information, organizational agility, and the integration of advanced analytical capabilities. Cloud environments enable centralized data management, seamless system integration, and support for geographically distributed users, which are critical requirements for effective managerial decision-making in dynamic and uncertain business environments (Venters & Whitley, 2012; Oliveira et al., 2014). Cloud-based architectures facilitate the integration of emerging technologies such as big data analytics, artificial intelligence, and machine learning. The availability of scalable computing power and centralized data repositories enables organizations to apply advanced analytical and predictive techniques that would be difficult or costly to implement in traditional on-premise environments (Hashem et al., 2015).

In the context of managerial decision support, cloud-based information systems provide a foundation for intelligent, data-driven decision-making by enabling continuous data processing, real-time reporting, and adaptive system behavior. Consequently, cloud-based information systems are widely perceived as key enablers of digital transformation and as core components of modern organizational information infrastructures supporting strategic and operational decision-making (Vial, 2019).

3. METHODOLOGY

The aim of this article is to analyze the theoretical foundations of information systems and to identify the key trends shaping modern information systems, with a particular focus on their role in supporting managerial decision-making in organizations. Given the conceptual nature of the research objective and the emphasis on identifying and synthesizing existing knowledge, a qualitative research design based on secondary data analysis was adopted.

The identification of trends in the field of information systems was conducted through a structured content analysis of secondary academic and professional sources. The analyzed corpus consisted of 13 relevant publications, including peer-reviewed scientific articles, academic books, technology-oriented research reports, and selected professional sources from organizations operating in the field of information system development. This combination of sources ensured both theoretical depth and practical relevance.

The selection of sources was guided by four main criteria: (1) a thematic focus on information systems and their application in organizational contexts; (2) an academic or professional character of the publication; (3) relevance to contemporary technological developments and current trends in information systems; and (4) geographical diversity of authors, with sources originating from Europe, Asia, and North America. These criteria were applied to ensure the credibility, relevance, and diversity of perspectives represented in the analyzed material.

The content analysis focused on identifying recurring technological and functional trends related to modern information systems. As the primary analytical indicator, the frequency of occurrence of specific trends across the analyzed sources was used. Trends that appeared repeatedly in multiple independent publications were considered to be more significant and representative of broader developments in the field. This frequency-based approach enabled an objective comparison of individual trends across different authors and publication types and supported the systematic identification of dominant patterns.

To enhance analytical rigor, the identified trends were subsequently grouped and synthesized into broader thematic categories reflecting their functional role in managerial decision support. This methodological approach allowed the study to move beyond a descriptive overview of individual technologies and toward an integrative perspective on how contemporary information systems evolve in response to organizational and managerial requirements.

4. FINDINGS

Based on the content analysis, technological and functional trends were identified according to their frequency of occurrence across the analyzed sources. Trends that appeared repeatedly in multiple publications were considered more representative of broader developments in the field of information systems. The results of the analysis are summarized in the list below, where the identified trends are ranked in descending order based on their observed frequency:

1. Cloud-based solutions (Lenart, 2011; Kenge & Khan, 2020; Basl, 2016; Ogli, 2021; Razzaq et al., 2020; Qu et al., 2019; Dherman, 2023; Tadepalli, 2021; Eswaran, 2016; Jurik, 2021)
2. Internet of Things (IoT) (Basl, 2016; Ogli, 2021; Qu et al., 2019; Dherman, 2023; Tadepalli, 2021; Jurik, 2021; Al-MSloum & Alharbi, 2021; El Kadiri et al., 2016)
3. Artificial intelligence (AI) and machine learning (Kenge & Khan, 2020; Ogli, 2021; Dherman, 2023; Eswaran, 2016; Jurik, 2021; Al-MSloum & Alharbi, 2021; Margineanu, Nedelcu & Lixandroiu, 2020)
4. Big data analytics (Basl, 2016; Ogli, 2021; Qu et al., 2019; Jurik, 2021; El Kadiri et al., 2016)
5. Compatibility with mobile devices (Basl, 2016; Ogli, 2021; Tadepalli, 2021; Eswaran, 2016; Jurik, 2021)
6. Cybersecurity (Dherman, 2023; Jurik, 2021)

The analysis resulted in the identification of six major trends in the field of information systems that appeared in more than one of the analyzed publications. The most frequently mentioned trend was cloud-based solutions, with a frequency of occurrence of ten. This finding indicates a pronounced shift toward service-oriented models of information system delivery, reflecting the growing importance of flexibility, scalability, and on-demand access to system functionalities. The second most frequently identified trend was the Internet of Things (IoT), with a frequency of eight, followed by artificial intelligence (AI) and machine learning, which appeared in seven sources. These trends reflect a growing emphasis on intelligent data processing and the integration of information systems with physical business processes. Together, they point to the increasing role of automation, real-time data acquisition, and advanced analytics in contemporary organizational information systems. Big data analytics and compatibility with mobile devices were each identified in five sources, indicating their significant but slightly less dominant role compared to cloud computing and IoT. These trends highlight the increasing importance of analytical capabilities and ubiquitous access to information, enabling decision-makers to work with large datasets and access relevant information regardless of time or location. The lowest frequency was observed for cybersecurity, which reflects a more specialized focus or its implicit integration into modern information systems rather than a lower level of importance. The results of the content analysis indicate that the identified factors represent key indicators of the modernity of information systems, particularly in terms of their ability to support managerial decision-making in dynamic organizational environments.

Cloud-based solutions emerged as the dominant trend in modern information systems. Their significance lies primarily in reduced implementation and operational costs, increased accessibility and scalability, and the ability to rapidly adapt to changing organizational requirements. In the analyzed sources, cloud-based systems are most commonly associated with Software-as-a-Service and hybrid deployment models, which allow organizations to combine the advantages of cloud infrastructure with partial control over data and system components. Despite identified risks related to security and long-term cost considerations, cloud-based solutions remain a central pillar of modern information system development.

Artificial intelligence enables information systems to process complex and unstructured data and transform them into intelligent outputs applicable to managerial decision-making. When combined with machine learning techniques, information systems are able to identify patterns, predict future behavior, and automate complex processes. The analyzed sources indicate a growing adoption of AI-based functionalities in information systems, with expectations of widespread implementation in the near term. This trend significantly enhances the capacity of information systems to deliver context-aware and real-time decision support.

The Internet of Things extends information systems by enabling direct data collection from physical devices and sensors. The integration of IoT with organizational information systems allows real-time monitoring of production, logistics, and operational processes, thereby improving planning accuracy and control. When combined with management information systems, IoT technologies form the basis for intelligent operational and management systems that provide decision-makers with immediate insight into organizational conditions and support rapid response.

Big data analytics represent an integral component of modern information systems, particularly at the level of management information systems and strategic systems. Their primary objective is to transform large volumes of structured and unstructured data into meaningful information through business intelligence and analytical tools. The analyzed sources confirm that effective use of big data analytics substantially improves managerial decision quality and supports a transition from reactive to proactive organizational management.

Mobile compatibility ensures access to information systems regardless of time and location. This trend is particularly relevant in the context of remote work, decentralized organizational structures, and field-based activities, where immediate access to up-to-date information is essential. Mobile interfaces, when integrated with management information systems, enhance decision-making agility and support effective communication and coordination within teams.

The increasing integration and centralization of data within information systems have heightened their exposure to cyber threats. The analyzed sources emphasize the need for multi-layered security mechanisms and the integration of cybersecurity considerations from the system design phase onward. Cybersecurity thus emerges as a fundamental prerequisite for the reliability and trustworthiness of modern information systems and for their effective use in managerial decision-making contexts.

5. DISCUSSIONS

The evolution of information systems reflects broader technological and organizational changes driven by globalization, digitalization, and increasing managerial complexity. The identified trends illustrate a shift from traditional, internally focused systems toward intelligent, interconnected, and data-driven platforms that actively support managerial decision-making rather than merely recording operational data.

The dominance of cloud-based solutions confirms findings from previous studies emphasizing cost efficiency, scalability, and accessibility as primary drivers of information systems adoption, particularly among small and medium-sized enterprises. While concerns related to data security and customization persist, the overall benefits of cloud technologies significantly outweigh their limitations. Artificial intelligence and machine learning introduce a qualitative leap in decision support by enabling predictive analytics, pattern recognition, and automation of complex tasks. Unlike traditional Management information system functionalities, AI-enhanced systems provide contextual insights and proactive recommendations, aligning with contemporary demands for real-time, evidence-based decision-making. The integration of IoT expands the data ecosystem of organizations by enabling real-time monitoring of physical processes. When combined with Management information system platforms, IoT data enhances operational transparency and supports predictive maintenance, capacity planning, and performance optimization. Big data analytics and business intelligence tools address the growing challenge of information overload by transforming vast datasets into actionable knowledge. This trend underscores a transition from intuition-based to analytically driven managerial practices. Mobile compatibility further reinforces decision agility by enabling ubiquitous access to critical information, particularly for managers operating outside traditional office environments. Cybersecurity emerges as a foundational prerequisite rather than a supplementary feature of modern IS. Increasing system integration and data centralization necessitate advanced, multilayered security architectures embedded directly into system design.

The findings demonstrate that modern information systems are no longer passive repositories of data but active enablers of strategic and operational decision-making. The convergence of identified trends creates synergistic effects that amplify the value of IS within organizations. This study highlights the necessity of holistic system design, where technological innovation is aligned with managerial needs and organizational processes.

6. CONCLUSION

This study contributes to the existing literature by systematically identifying and synthesizing key technological trends that define modern information systems from a managerial decision-support perspective. By consolidating dispersed findings across multiple sources, the research addresses a gap in the literature concerning the integrative evaluation of information system trends.

The primary strength of the study lies in its structured analytical approach and its focus on decision support as a unifying theme across technological developments. However, the reliance on secondary data represents a limitation, as empirical validation within specific organizational contexts was beyond the scope of this research. Future research should focus on empirical case studies examining the real-world implementation of identified trends and their measurable impact on decision quality and organizational performance. Further exploration of ethical, organizational, and human factors associated with intelligent information systems would provide valuable insights.

In conclusion, modern information systems represent a strategic asset that fundamentally reshapes managerial decision-making. By integrating advanced technologies into cohesive platforms, organizations can enhance adaptability, resilience, and long-term competitiveness. The true value of information systems lies not in data accumulation, but in their ability to transform information into informed action.

Acknowledgement

Funded by the EU NextGenerationEU through the Recovery and Resilience Plan for Slovakia under the project No. 09I05-03-V02-00010.

REFERENCES

[1] AL-MSLOUM, A. S. H., & ALHARBI, I. M. 2021. ***Application and trends in information management system using artificial intelligence.*** Materials Today: Proceedings. https://doi.org/10.1016/j.matpr.2021.03.308.

[2] ALTER, S. 2008. ***Defining information systems as work systems: implications for the IS field***. European Journal of Information Systems, 17(5), 448–469. https://doi.org/10.1057/ejis.2008.37.

[3] AMINUDDIN HAMDAT, CESKAKUSUMADEWI B, SAMALAM, A. G., MUHAMMAD RIZAL, & IZAAC L.D LAWALATA. 2024. ***The Impact of Management Information Systems on Decision-Making Efficiency***. VIFADA MANAGEMENT and DIGITAL BUSINESS, 1(2), 56–74. https://doi.org/10.70184/qpw1rq78.

[4] ARMBRUST, M., STOICA, I., ZAHARIA, M., FOX, A., GRIFFITH, R., JOSEPH, A. D., KATZ, R., KONWINSKI, A., LEE, G., PATTERSON, D., & RABKIN, A. 2010. ***A View of Cloud Computing***. Communications of the ACM, 53(4), 50–58. https://doi.org/10.1145/1721654.1721672.

[5] BASL, J. 2016. ***Enterprise Information Systems and Technologies in Czech Companies from the Perspective of Trends in Industry 4.0***. Lecture Notes in Business Information Processing, 156–165. https://doi.org/10.1007/978-3-319-49944-4_12.

[6] BATRA, D. 2022. ***Antecedents of Organizational Agility During Business Uncertainty in Noninformation Technology Sectors***. Journal of Database Management, 33(1), 1–22. https://doi.org/10.4018/jdm.309433.

[7] DELEN, DURSUN. 2010. ***Decision Support and Business Intelligence Systems*** (9th Edition).

[8] DELONE, W. H., & MCLEAN, E. R. 2003. ***The DeLone and McLean Model of Information Systems Success: A Ten-Year Update***. Journal of Management Information Systems, 19(4), 9–30.

[9] DHERMAN, K. 2023. ***8 manufacturing ERP trends for 2023 | SYSPRO Blog***. SYSPRO Blog. https://www.syspro.com/blog/erp-and-technology/8-manufacturing-erp-trends-for-2023/.

[10] EL KADIRI, S., GRABOT, B., THOBEN, K.-D., HRIBERNIK, K., EMMANOUILIDIS, C., VON CIEMINSKI, G., & KIRITSIS, D. 2016. ***Current trends on ICT technologies for enterprise information systems.*** Computers in Industry, 79, 14–33. https://doi.org/10.1016/j.compind.2015.06.008.

[11] ESWARAN, CH. 2016. ***What Are the ERP Trends That Will Truly Matter in 2022?*** ERP News. https://erpnews.com/what-are-the-erp-trends-that-will-truly-matter-in-2022/.

[12] FILIP, F.-G. 2007. ***MANAGEMENT INFORMATION SYSTEMS: Managing the Digital Firm - 9th edition***, authors: Keneth C. Laudon and Jane P. Laudon (Book Review). International Journal of Computers Communications & Control, 2(1), 103. https://doi.org/10.15837/ijccc.2007.1.2342.

[13] GANTZ, S. D., & PHILPOTT, D. 2013. ***Thinking About Systems***. Elsevier EBooks, 79–103. https://doi.org/10.1016/b978-1-59-749641-4.00004-7.

[14] GEBAUER, J., SHAW, M. J., & GRIBBINS, M. L. 2010. ***Task-Technology Fit for Mobile Information Systems***. Journal of Information Technology, 25(3), 259–272. https://doi.org/10.1057/jit.2010.10.

[15] HANANIYA, PHILEMON & BADAU, KABIRU & OLAJIRE, FRANCIS & YIDAWI, MUSA. 2024. ***Information Systems in Organizations.***

[16] HASHEM, I. A. T., YAQOOB, I., ANUAR, N. B., MOKHTAR, S., GANI, A., & ULLAH KHAN, S. 2015. ***The Rise of "big Data" on Cloud computing: Review and Open Research Issues***. Information Systems, 47(1), 98–115. https://doi.org/10.1016/j.is.2014.07.006.

[17] JURIK, P. 2021. ***Aktuálne trendy v ERP aplikáciách***. https://www.researchgate.net/publication/348394002_Aktualne_trendy_v_ERP_aplikaciach.

[18] KENGE, R., & KHAN, Z. 2020. ***A Research Study on the ERP System Implementation and Current Trends in ERP***. Shanlax International Journal of Management, 8(2), 34–39. https://doi.org/10.34293/management.v8i2.3395.

[19] LENART, A. 2011. ***ERP in the Cloud – Benefits and Challenges***. Research in Systems Analysis and Design: Models and Methods, 93, 39–50. https://doi.org/10.1007/978-3-642-25676-9_4.

[20] LENART, A. 2011. ***Research in Systems Analysis and Design: Models and Methods***. University of Gdansk. 2011. [online]. [cit. 02.02.2023]. ISBN: 978-3-642-25675-2. Dostupné z: https://link.springer.com/chapter/10.1007/978-3-642-25676-9_4.

[21] LI, D., & LIU, J. 2014. ***Dynamic capabilities, environmental dynamism, and competitive advantage: Evidence from china***. Journal of Business Research, 67(1), 2793–2799. https://doi.org/10.1016/j.jbusres.2012.08.007.

[22] MARGINEANU, C. – NEDELCU, A. – LIXANDROIU, D. 2020. ***Evolutions and trends in information systems assisting managerial decision-making***. Study on erp systems. [online]. [cit. 02.02.2023]. Dostupné z: https://www.afahc.ro/ro/revista/2020_1/Review-No1-2020.pdf#page=23.

[23] MARSTON, S. R., LI, Z., BANDYOPADHYAY, S., GHALSASI, A., & ZHANG, J. 2009. ***Cloud Computing: The Business Perspective***. SSRN Electronic Journal, 51(1). https://doi.org/10.2139/ssrn.1413545.

[24] OLIVEIRA, T., THOMAS, M., & ESPADANAL, M. 2014. ***Assessing the determinants of cloud computing adoption: An analysis of the manufacturing and services sectors***. Information & Management, 51(5), 497–510. https://doi.org/10.1016/j.im.2014.03.006.

[25] PETTER, S., DELONE, W., & MCLEAN, E. 2008. ***Measuring information systems success: models, dimensions, measures, and interrelationships***. European Journal of Information Systems, 17(3), 236–263. https://doi.org/10.1057/ejis.2008.15.

[26] POLOJÄRVI, D., PALMER, E., & DUNFORD, C. 2023. ***A systematic literature review of sociotechnical systems in systems engineering. Systems Engineering***, 26(4). https://doi.org/10.1002/sys.21664.

[27] QU, Y. J., MING, X. G., LIU, Z. W., ZHANG, X. Y., & HOU, Z. T. 2019. Smart manufacturing systems: state of the art and future trends. ***The International Journal of Advanced Manufacturing Technology,*** 103(9-12), 3751–3768. https://doi.org/10.1007/s00170-019-03754-7.

[28] RAZZAQ, A., ASMAI, S. A., TALIB, M. S., IBRAHIM, N., & MOHAMMED, A. A. 2020. ***Cloud ERP in Malaysia: Benefits, Challenges, and Opportunities.*** International Journal of Advanced Trends in Computer Science and Engineering, 9(5), 7510–7516. https://doi.org/10.30534/ijatcse/2020/85952020.

[29] SELVARAJAN, GURU. 2022. ***Adaptive Architectures and Real-time Decision Support Systems: Integrating Streaming Analytics for Next- Generation Business Intelligence***. 5. 651-662.

[30] SOLIJONOV MIRODILJON MURALIMJON OGLI. 2021. ***Enterprise Resource Planning Implementation And Current Trends. The American Journal of Engineering and Technology***, 3(08), 1–10. https://doi.org/10.37547/tajet/Volume03Issue08-01.

[31] TADEPALLI, P. 2021. ***5 ERP Trends that Can Help Accelerate Your Digital Transformation***. (2021). Hitachivantara.com. https://www.hitachivantara.com/en-us/insights/5-enterprise-resource-planning-erp-trends-that-accelerate-digital-transformation.

[32] TAHERDOOST, H. 2022. ***An overview of trends in information systems: Emerging technologies that transform the information technology industry.*** Cloud Computing and Data Science, 4(1), 1–16. https://doi.org/10.37256/ccds.4120231653.

[33] VENTERS, W., & WHITLEY, E. A. 2012. ***A Critical Review of Cloud Computing: Researching Desires and Realities***. Journal of Information Technology, 27(3), 179–197. https://doi.org/10.1057/jit.2012.17.

[34] VIAL, G. 2019. ***Understanding Digital transformation: a Review and a Research Agenda***. The Journal of Strategic Information Systems, 28(2), 118–144. https://doi.org/10.1016/j.jsis.2019.01.003.

[35] WATSON, H. J., WIXOM, B. H., HOFFER, J. A., ANDERSON-LEHMAN, R., & REYNOLDS, A. M. 2009. ***Real-Time Business Intelligence: Best Practices at Continental Airlines1.*** EDPACS, 40(6), 1–16. https://doi.org/10.1080/07366980903484935.

Ivana GABRIŠOVÁ, Ing.
Gabriel KOMAN, doc. Ing., PhD.
Lucie LENDELOVÁ, Ing., Ph.D. MBA.
University of Žilina, Faculty of Management Science and Informatics, Department of Management Theories
Univerzitná 8215/1, 010 26 Žilina, Slovakia
e-mail: ivana.gabrisova@fri.uniza.sk; gabriel.koman@fri.uniza.sk; lucie.lendelova@fri.uniza.sk

AN INTEGRATED FRAMEWORK FOR IDENTIFYING AND PRIORITISING CYBERSECURITY RISKS IN SPORTS MANAGEMENT

ADAM JACKO – MICHAL VARMUS – RADOSLAV JANKAL

Abstract: *The digitalisation of the sports environment has increased the dependence of sports organisations on digital platforms, data infrastructures, analytical tools, and external services. Yet cybersecurity remains insufficiently embedded in managerial decision-making, which creates a gap between growing digital dependence and the organisational capacity to identify and prioritise risk. This article proposes an integrated framework for identifying and prioritising cybersecurity risks in sports management. The study is based on a synthesis and interpretation of eighteen scientific sources focused on cybersecurity, cybersecurity risk management, digital transformation, organisational resilience, and the sports environment. The findings show that cybersecurity risk in sports management is shaped across three interrelated dimensions: technological, organisational, and environmental. These dimensions are interpreted through a threat, vulnerability, and consequence logic and linked with a context-based approach to cybersecurity risk management. The analysis identifies three priority areas: risks affecting core digital operations, organisational vulnerabilities connected with communication, responsibility, and security culture, and dependencies on external partners and services. The article contributes by moving beyond a descriptive account of threats and by offering a structured framework that supports managerial decision-making in sports organisations. It also provides a basis for future empirical verification in sports clubs, sports facilities, and sports events.*

Keywords: *cybersecurity risk, sport management, digitalisation, risk prioritisation, organisational resilience, sports organisations*

JEL Classification: *M15, Z21, D81*

1. INTRODUCTION

The digitalisation of the sports environment is reshaping how sports organisations operate, communicate, and create value. It is no longer confined to the transfer of content to online platforms. Digital platforms, data services, analytical tools, and interconnected systems have become increasingly central to both operational processes and user interaction. In this context, Ivanova (2022) shows that digital sports platforms have become an integral part of the contemporary sports ecosystem.

As digitalisation intensifies, the importance of cybersecurity also grows. Bongiovanni et al. (2024) point out that sports events and sports organisations are becoming increasingly dependent on information management and intensive data sharing. At the same time, cybersecurity in the sports environment remains a comparatively underexplored area of research. Watchers et al. (2024) further suggest that, in practice, the cybersecurity dimension of protection is often perceived as less prominent than traditional forms of security. This creates a mismatch between growing digital dependence and a weaker managerial understanding of cybersecurity risk. Saeed et al. (2023) add that digital transformation improves efficiency and productivity, yet it also increases exposure to data breaches and cyberattacks. In a similar vein, Yaacob et al. (2023) show that emerging technologies expand the attack surface and create technical, organisational, and regulatory challenges that traditional protection measures do not fully address.

This situation suggests that cybersecurity cannot be reduced to technical measures alone. Setiawan et al. (2025) emphasise the need to integrate it into organisational management and leadership decision-making. Pollini et al. (2022) likewise show that vulnerability arises not only from technology, but also from human behaviour and organisational practice. Haque et al. (2025) complement this view by highlighting the importance of proactive risk management encompassing technical, process-related, human, and external factors. Familoni (2024) further indicates that artificial intelligence simultaneously strengthens threat detection and response while also enabling more sophisticated forms of attack and introducing new vulnerabilities that require adaptive defence and robust risk management.

The aim of this article is therefore to propose an integrated framework for the identification and prioritisation of cybersecurity risks in sports management. The framework combines the three-dimensional categorisation developed by Bongiovanni et al. (2024) with the decision logic of Ganin et al. (2020), which links threat, vulnerability, and consequence. It is further informed by context-based and dynamic approaches to risk management that emphasise organisational dependencies, evolving infrastructures, and transparent decision support. In this way, the article moves beyond a descriptive account of threats and offers a structured framework for managerial decision-making in sports organisations.

2. LITERATURE REVIEW

Cybersecurity in sports management extends beyond the technical protection of information systems. Within sports organisations, it is closely intertwined with risk management, operational organisation, and strategic decision-making. Genovard et al. (2025) show that sports organisations face multilayered risks affecting operational, legal, financial, and governance dimensions. Setiawan et al. (2025) likewise warn that a fragmented understanding of cybersecurity risk

reduces its visibility at the level of organisational leadership. For this reason, the theoretical foundations of this article are organised into three interconnected areas. The first concerns the digitalisation of the sports environment. The second addresses the integration of cybersecurity into risk management and organisational resilience. The third focuses on cybersecurity risk management frameworks that provide the basis for the article's own model.

2.1 Digitalisation as a Source of Cybersecurity Risk

Digitalisation has substantially expanded the range of activities that sports organisations perform through digital technologies. It is no longer limited to communication or content distribution. Increasing attention is now directed towards digital platforms, data repositories, analytical tools, payment modules, and services linked to external partners. Ivanova (2022) notes that digital sports platforms process personal data, financial data, system records, and real-time data. She also describes their architecture in terms of a user layer, an application layer, a data layer, a security layer, and an external service layer. Such an environment increases the functionality and accessibility of services, while simultaneously expanding the space of vulnerability.

This expansion is also visible in the technological transformation of sports events themselves. Principe et al. (2025) show that blockchain-based approaches are gradually entering sports event management and are associated with more decentralised governance structures, stronger transparency, higher operational efficiency, and broader stakeholder participation. At the same time, such implementation requires strategic infrastructure assessment, stakeholder engagement, and explicit risk management protocols. The growing complexity of digital event infrastructures therefore widens the field in which cybersecurity risk must be managed.

A similar line of argument is developed by Bongiovanni et al. (2024), who show that, in the context of sports events, cybersecurity is closely connected with the technological, organisational, and environmental dimensions of their functioning. According to the authors, the introduction of new technologies into infrastructure, event organisation, and data management increases demands for information protection and privacy. Sports events are also characterised by a high concentration of people, strong media attention, and significant economic value. This combination increases both their attractiveness to attackers and the potential scale of incident consequences.

This problem becomes even more visible in technologically intensive event settings. AL Dosari et al. (2023), in their work on mega sporting events, show that security arrangements increasingly rely on UAV-supported systems and broader digital security supply chains. Their model highlights the importance of traceability, security, privacy, trust, acceptability, and preparedness. These factors indicate that digitalisation in the sports environment does not merely expand technological infrastructure. It also increases dependence on secure coordination across multiple technologies, actors, and operating conditions.

Watchers et al. (2024) confirm this development in the setting of professional sports facilities. They show that sports venues are increasingly dependent on interconnected digital systems, while the cybersecurity dimension of protection remains less visible in practice than physical and personnel security. In this respect, digitalisation does not merely create new opportunities in the sports environment. It also generates new vulnerabilities that may not be recognised in time within organisational practice.

2.2 Cybersecurity as Part of Risk Management

If cybersecurity in sports management is to be addressed effectively, it must be embedded in a broader risk management framework. Genovard et al. (2025) show that sports organisations face a wide spectrum of risks and that governance and financial dimensions remain particularly underdeveloped in the literature. From the perspective of this article, this is important because cybersecurity risk affects more than information systems alone. It also has consequences for business continuity, resource protection, the allocation of responsibility, and the long-term stability of the organisation. Saeed et al. (2023) reinforce this view by linking digital transformation directly with business resilience and by arguing that organisations need structured cybersecurity readiness if they are to prevent disruptions during technological change.

This perspective is further developed by Setiawan et al. (2025), who emphasise the need for the strategic integration of cybersecurity into enterprise risk management. They point to a communication gap between IT teams and organisational leadership, the absence of standardised cybersecurity risk metrics, and siloed approaches to organisational governance. In the sports environment, this problem is especially significant. A sports organisation functions as an interconnected system of sporting, economic, operational, and communication processes. When cybersecurity risk is not visible at the leadership level, protective measures remain fragmented and their strategic relevance is weakened.

The human factor also plays an important role in this context. Pollini et al. (2022) conceptualise cybersecurity as part of a socio-technical system in which individual, organisational, and technological elements are interconnected. They warn that security culture and actual security behaviour do not necessarily coincide, and that tensions between formal rules and everyday working practice may create new vulnerabilities. In sports organisations, this issue is particularly pronounced because of time pressure, the high pace of decision-making, and the interaction of multiple groups of actors.

For this reason, cybersecurity naturally intersects with organisational resilience. Bostock and Breese (2023) understand resilience in sports management as a dynamic means of achieving objectives under conditions of pressure, change, and disruption. From this perspective, cybersecurity is not merely a matter of protecting technologies. It is also a matter of organisational preparedness to respond, adapt, and sustain operations when disruption occurs.

2.3 Cybersecurity Risk Management Frameworks

The previous subsections have shown that cybersecurity risk in the sports environment emerges at the intersection of technology, organisation, and wider external relationships. For this reason, it is not sufficient merely to identify risks. A more structured approach is needed, linking organisational context, risk identification, risk assessment, and subsequent decision-making on protective measures.

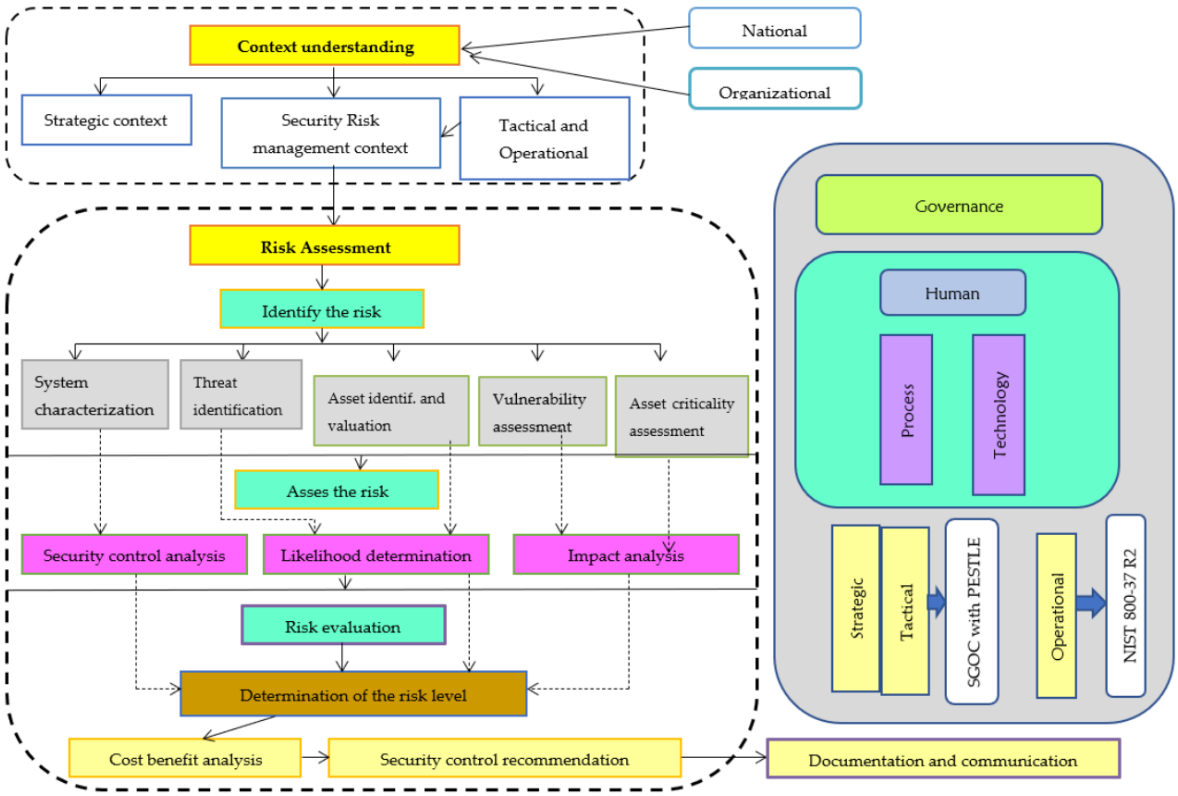


Figure 1 Context-Based Cybersecurity Risk Management Framework
Source: Melaku (2023)

Such an approach is important for this article because it creates a bridge between general theoretical reflection and a systematic understanding of cybersecurity risk management.

Melaku (2023) proposes a context-based and adaptive cybersecurity risk management framework. The author states that the framework consists of four main parts: risk assessment, risk mitigation, the risk management programme, and process evaluation. Importantly, this approach does not begin with the technical threat itself, but with the internal and external context of the organisation, the identification of stakeholders, and the alignment of strategy with risk tolerance. Melaku (2023) further argues that such a model supports a more precise identification of vulnerable points, a better estimation of the possible consequences of incidents, and a more effective allocation of security investments. As shown in Figure 1, the individual components of the framework are arranged as an interconnected process in which assessment, mitigation, programme design, and ongoing evaluation are firmly embedded in the organisational context.

As Figure 1 shows, cybersecurity risk management is not a one-off intervention, but a continuous process grounded in feedback and aligned with organisational objectives. In this respect, Melaku's model is valuable for sports management because it links security-related decision-making with the broader functioning of the organisation. Islam et al. (2024) extend this perspective by showing that risk assessment should also reflect dynamic factors such as asset dependencies, exploitability, and attack complexity. Sarker et al. (2024) add that advanced assessment tools must remain explainable and trustworthy if they are to support managerial judgement in complex digital environments. Together, these approaches create a suitable conceptual basis for the analytical part of this article, in which cybersecurity risks are structured and prioritised from a managerial perspective.

3. METHODOLOGY

This article synthesises insights from eighteen scientific sources focused on cybersecurity, cybersecurity risk management, digital transformation, and the sports environment. Attention was directed towards studies that connect the security and managerial dimensions of the topic and, at the same time, offer applicable frameworks for sports management.

The individual studies were first reviewed and processed in terms of their main findings, applied frameworks, and key themes. They were then compared in order to identify common patterns and differences. This provided the basis for the synthesis of knowledge on the digitalisation of the sports environment, organisational vulnerabilities, and approaches to cybersecurity risk management. The methodological approach is based on the synthesis and interpretation of existing sources rather than on new empirical data collection.

The chosen approach is limited by the fact that the article works exclusively with secondary sources and does not verify the proposed framework in the setting of a specific sports organisation. Nevertheless, it provides a theoretically grounded basis for the analytical part of the article.

4. FINDINGS

The analytical part of the article is based on a synthesis of sources addressing the sports environment, digital platforms, cybersecurity risk management, and organisational resilience. The findings show that cybersecurity risk in sports management does not take a single form. It is shaped at the level of technology, organisation, and the wider environment

in which a sports organisation operates. For this reason, it was appropriate to structure the findings into three dimensions. They were then interpreted through the logic of threat, vulnerability, and consequence developed by Ganin et al. (2020).

4.1 Technological Dimension of Cybersecurity Risks

At the technological level, attention is focused on digital platforms, network environments, application layers, and data flows. Ivanova (2022) shows that digital sports platforms integrate the user interface, application services, data storage, the security layer, and external services. Such an arrangement enhances system functionality, while simultaneously creating multiple entry points for attack. Vulnerability is therefore distributed across the platform architecture rather than concentrated in a single location. From a technical perspective, the issue is not the protection of one isolated system, but of an interconnected digital environment.

The user and application layers are particularly sensitive in this respect. It is precisely here that the risks of unauthorised access, credential misuse, and weaknesses in interfaces between individual services emerge. Data flows are also of critical importance, since they carry personal data, payment information, and other system-relevant records.

This also implies that technical risk cannot be interpreted in purely static terms. Islam et al. (2024) show that its severity depends on dynamic parameters such as exploitability, asset dependencies, attack complexity, common attack points, and the likely impact on security objectives. In a sports organisation, this means that the criticality of a vulnerability is shaped not only by its existence, but also by how easily it can be exploited and how far its effects may propagate across connected systems.

A similar implication follows from Sarker et al. (2024), who argue that increasingly interconnected digital environments require automated and intelligent cybersecurity capabilities, but also trustworthy and interpretable decision support. This is relevant for sports settings because digital infrastructures are becoming more layered and data intensive. As technical complexity grows, the ability to detect threats, identify anomalies, and interpret alerts becomes part of technological resilience itself.

This line of argument is further developed by Bongiovanni et al. (2024), who emphasise that the expansion of technologies in sports events increases demands for cybersecurity. In their review, the technological dimension is associated with event-related digital infrastructure, Internet of Things devices, monitoring systems, and network environments. These elements extend the functionality of the sports setting, but at the same time increase its vulnerability. The technological layer in the sports environment therefore does not operate in isolation. It is closely linked to operations, visitor safety, user trust, and the protection of financial flows.

A similar picture is offered by Watchers et al. (2024), who focus on professional sports facilities. They show that sports venues are increasingly dependent on interconnected digital devices and on stable connectivity. Risk therefore does not arise solely within central systems. It also extends into everyday technical operations. The authors point to wireless networks, possible disruptions of connectivity, and the consequences of such incidents for personal data, financial data, and the operational stability of the facility.

4.2 Organisational Dimension of Cybersecurity Risks

Technology alone does not explain cybersecurity risk in its full scope. A substantial part of vulnerability arises from organisational arrangements, planning, communication, and security culture. Watchers et al. (2024) found that, in professional sport, physical and personnel security are often perceived as more important than cybersecurity. This imbalance is significant. It suggests that an organisation may possess well-developed traditional security measures while continuing to underestimate the digital dimension of threat.

This line of argument is reinforced by Setiawan et al. (2025), who draw attention to the separation of IT and risk management. When cybersecurity is addressed in isolation, gaps emerge in risk visibility, incident response, and strategic decision-making. The authors also emphasise the communication gap between technical teams and organisational leadership, the absence of standardised metrics, and the silo effect in organisational governance. It is precisely here that technical risk becomes a managerial problem. If leadership is unable to interpret risk accurately, it cannot assign it an adequate priority.

The significance of this dimension is further developed by Pollini et al. (2022). They show that cybersecurity forms part of a socio-technical system in which technological, individual, and organisational elements are interconnected. One of their key findings is that a stronger declared security culture does not automatically lead to a higher level of secure behaviour. Vulnerability may arise even when formal rules are properly designed, if everyday practice is shaped by time pressure, ambiguity, or routine circumvention of procedures.

Yaacob et al. (2023) add that organisational risk also grows when employee preparation, cybersecurity training, and compliance capacity do not keep pace with technological change. Familoni (2024) similarly argues that the current threat landscape requires interdisciplinary collaboration, adaptive defence mechanisms, and sustained investment in cybersecurity education and training. For sports organisations, this insight is particularly important. A security weakness does not necessarily take the form of a technical attack. It may emerge through unclear responsibilities, inadequate staff preparation, or poor communication between departments. The organisational dimension therefore shows that cybersecurity risk is also a matter of management, accountability, and everyday operational practice.

4.3 Environmental Dimension of Cybersecurity Risks

The third dimension is linked to the wider environment in which sports organisations operate. Bongiovanni et al. (2024) show that sports events occupy a distinctive position because they combine technological infrastructure, a high concentration of people, intense media attention, and sensitive operational dependencies. This combination increases the attractiveness of the environment to attackers and, at the same time, amplifies the impact of a possible incident. A cyberattack therefore does not affect only an information system. It may weaken public trust, affect partners and sponsors, and damage the economic outcomes of the organisation or the event.

Ivanova (2022) confirms the importance of this dimension in the context of digital sports platforms. She points out that external services, payment gateways, and application interfaces connected to third parties are major sources of vulnerability. Risk thus extends beyond the organisation itself. Even where internal protection is relatively well configured, a weak point may arise in an external integration or in a partner service. In the sports environment, this is particularly important, as organisations operate within a high degree of interdependence with suppliers, partners, and technological intermediaries.

This line of argument is also supported by Watchers et al. (2024), who highlight the dependence of sports facilities on external operational and security capacities. Organisations often rely on contractors and external staff. While this may be operationally efficient, it also broadens the space of uncertainty. Every external connection may represent a new entry point, a new communication gap, or a new ambiguity of responsibility.

A broader security reading of this dimension is provided by Mhammed (2025), who presents cyber intelligence as an important means of strengthening the resilience of vital infrastructures and of improving detection, analysis, and decision-making in the face of evolving cyber threats around future sporting events. His argument is relevant here because it shows that cyber incidents in sport may intersect not only with organisational operations, but also with wider questions of critical infrastructure protection and public security.

This environmental dependence also becomes concrete in mega event operations. AL Dosari et al. (2023) show that security arrangements linked to UAV-based systems rely on traceability, security, privacy, trust, acceptability, and preparedness. In such settings, the environment of risk is not limited to the focal organisation. It is distributed across technologies, service chains, and event ecosystems that require coordinated and reliable protection.

4.4 Prioritisation of the Identified Risks in Sports Management

Following the synthesis of the three dimensions, the next step is to determine which risks require the greatest managerial attention. A suitable point of departure is the framework proposed by Ganin et al. (2020), which operates with three basic elements: threat, vulnerability, and consequence. This approach makes it possible to move from the identification of risks to the evaluation of their severity. In sports management, this means that organisations need to understand not only what risks exist, but also which of them should be prioritised in decision-making. As shown in Figure 2, the individual criteria are arranged hierarchically and move from problem identification towards decision-making on priorities.

The first priority area can be identified as risks affecting the core of the digital operations of a sports organisation. These include the compromise of user accounts, disruption of data flows, attacks on authentication mechanisms, weaknesses in application interfaces, and incidents affecting services of high operational criticality. Ivanova (2022) shows that these layers carry personal data, financial transactions, and key system functions. When they are disrupted, not only the technical but also the operational and reputational severity of consequences increases.

The second priority area consists of organisational vulnerabilities. These include low levels of cybersecurity awareness, weak links between leadership and IT, unclear responsibilities, and insufficient planning. Watchers et al. (2024) and Setiawan et al. (2025) suggest that it is precisely within this dimension that technical risk becomes a strategic problem. An organisation may possess technical tools, yet without clear managerial understanding, staff preparedness, and internal coordination it cannot effectively position them among its priorities.

The third priority area concerns external relationships and dependence on third parties. Bongiovanni et al. (2024) and Ivanova (2022) show that the sports environment is strongly interconnected with partners, suppliers, and external services. In this dimension, the crucial factor is the combination of a higher degree of uncertainty and limited control. An organisation may not have full oversight of security processes beyond its internal boundaries, yet it still bears the consequences of an incident in its own operations and reputation.

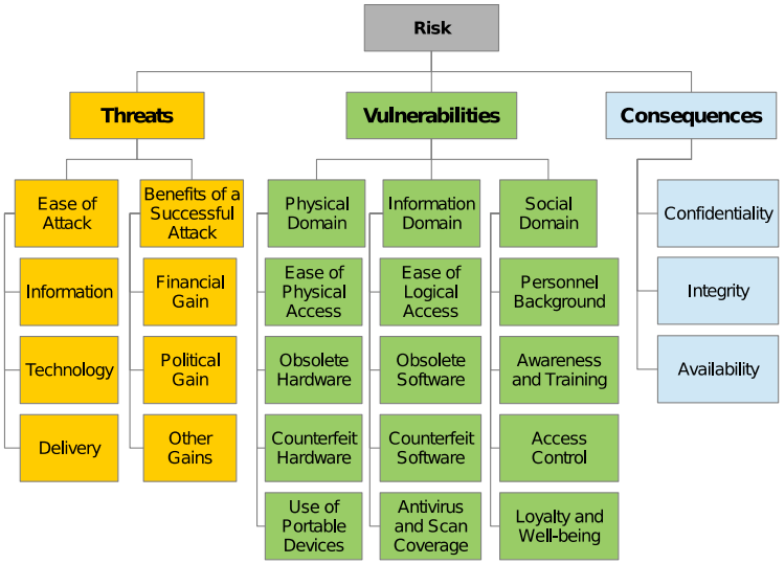


Figure 2 Hierarchy of Cybersecurity Risk Assessment Criteria
Source: Ganin et al. (2020)

5. DISCUSSION

The analysed sources suggest that the digital dependence of sports organisations is growing faster than their managerial capacity to integrate cybersecurity into decision-making. Ivanova (2022) demonstrates the complexity of digital sports platforms and their operational and data-related interconnectedness. Bongiovanni et al. (2024) extend this view by showing that sports events combine technological infrastructure, intensive information processing, and high reputational sensitivity. Watchers et al. (2024) further suggest that the cybersecurity dimension of protection often remains less visible in practice than physical and personnel security. Saeed et al. (2023) and Yaacob et al. (2023) reinforce this interpretation by showing that digital transformation and emerging technologies tend to advance faster than organisational preparedness, staff training, and compliance capacity. In this context, cybersecurity clearly becomes a sports management issue rather than a purely technical concern.

This also changes the way in which risk should be understood. Setiawan et al. (2025) warn that when cybersecurity remains isolated within the IT domain, both leadership decision-making and incident response are weakened. Pollini et al. (2022) likewise show that vulnerability emerges not only from technology, but also from human behaviour, working routines, and tensions between formal rules and everyday practice. Familoni (2024) adds that this challenge is intensified by the spread of artificial intelligence, which increases defensive possibilities while also enabling more sophisticated attacks. In sports organisations, such vulnerability carries particular weight because it can quickly affect operations, communication, and organisational reputation. Cybersecurity risk therefore cannot be reduced to system protection alone. It is also a matter of coordination, accountability, and organisational design.

Against this background, the integrated approach proposed in this article appears especially relevant. Melaku (2023) links cybersecurity risk management with organisational context, stakeholders, and risk tolerance. Ganin et al. (2020) add the decision logic of threat, vulnerability, and consequence. Islam et al. (2024) strengthen this reasoning by showing that prioritisation should also reflect exploitability, asset dependencies, and attack complexity. Sarker et al. (2024) complement this view by emphasising that advanced risk assessment tools must remain explainable and trustworthy if they are to support real organisational decisions. The value of combining these perspectives lies in the shift from descriptive reasoning to structured managerial judgement. Cybersecurity risk thus appears not as a set of isolated technical problems, but as a field of decision-making shaped by exposure, vulnerability, consequences, and the organisation's capacity to interpret them.

This interpretation is also consistent with the resilience perspective of Bostock and Breese (2023). Protection is not an end in itself. It forms part of an organisation's ability to function under pressure, adapt to disruption, and maintain continuity. From the perspective of sports management, this is particularly important because effective response depends not only on technical safeguards, but also on whether the organisation is able to recognise risk, assign it proper significance, and translate it into leadership action. In larger event settings, this relevance extends beyond the focal organisation, as Mhammed (2025) suggests in relation to cyber intelligence, resilience, and wider digital infrastructures.

At the same time, the proposed framework remains theoretical and requires empirical verification in specific sports organisations.

6. CONCLUSION

Cybersecurity in sports management should not be understood as a supplementary technical issue. It forms part of organisational management because it affects digital operations, internal processes, and external relationships across the sports environment. The synthesis of the analysed sources shows that its significance cannot be assessed solely in terms of threat, but must also be understood through organisational vulnerability, technological dependencies, and the consequences for continuity, trust, and reputation.

The contribution of this article lies in combining the three-dimensional view of cybersecurity risk in sports management with the prioritisation logic of Ganin et al. (2020), while drawing on context-based, dynamic, and explainable approaches to risk assessment. This integrated framework provides a structured basis for identifying and prioritising cybersecurity risks in sports management. Future research should focus on its empirical verification in sports organisations, sports facilities, and sports events.

Acknowledgement

Funded by the EU NextGenerationEU through the Recovery and Resilience Plan for Slovakia under the project No. 09I05-03-V02-00010.

REFERENCES

[1] AL-DOSARI, K., DEIF, A. M., KUCUKVAR, M., ONAT, N., & FETAIS, N. (2023). Security Supply Chain Using UAVs: Validation and Development of a UAV-Based Model for Qatar's Mega Sporting Events. ***Drones***, 7(9), 555. https://doi.org/10.3390/drones7090555

[2] BONGIOVANNI, I., HEROLD, D. M., & WILDE, S. J. (2024). Protecting the play: An integrative review of cybersecurity in and for sports events. ***Computers & Security***, 146, 104064. https://doi.org/10.1016/j.cose.2024.104064

[3] BOSTOCK, J., & BREESE, R. (2023). Theorising organisational resilience for sport management research and practice. ***Managing Sport and Leisure***, 28(4), 455–471. https://doi.org/10.1080/23750472.2021.1930113

[4] FAMILONI, B. T. (2024). Cybersecurity Challenges in the Age of AI: Theoretical Approaches and Practical Solutions. ***Computer Science & IT Research Journal***, 5(3), 703–724. https://doi.org/10.51594/csitrj.v5i3.930

[5] GANIN, A. A., QUACH, P., PANWAR, M., COLLIER, Z. A., KEISLER, J. M., MARCHESE, D., & LINKOV, I. (2020). Multicriteria Decision Framework for Cybersecurity Risk Assessment and Management. ***Risk Analysis***, 40(1), 183–199. https://doi.org/10.1111/risa.12891

[6] GENOVARD, F., MUÑOZ, J., PETCHAMÉ, J., & SOLANELLAS, F. (2025). Risk management approaches in sports organisations: A scoping review. ***Heliyon***, 11(3), e42270. https://doi.org/10.1016/j.heliyon.2025.e42270

[7] HAQUE, G. M. M., AKULA, D. K., MOHAMMED, Y. S., SYED, A. (2025). Cybersecurity Risk Management in the Age of Digital Transformation: A Systematic Literature Review. ***The American Journal of Engineering and Technology***, 7(08), 126–150. https://doi.org/10.37547/tajet/Volume07Issue08-14

[8] ISLAM, S., BASHEER, N., SILVESTRI, S., PAPASTERGIOU, S., & CIAMPI, M. (2024). Intelligent Dynamic Cybersecurity Risk Management Framework with Explainability and Interpretability of AI models for Enhancing Security and Resilience of Digital Infrastructure. In ***Review***. https://doi.org/10.21203/rs.3.rs-4796809/v1

[9] IVANOVA, S. (2022). Cybersecurity Challenges and Risk Management Strategies in Digital Sports Project Platforms. International ***Journal of Emerging Trends in Computer Science and Information Technology***, 3(2), 23–31. https://doi.org/10.63282/3050-9246.IJETCSIT-V3I2P103

[10] MELAKU, H. M. (2023). Context-Based and Adaptive Cybersecurity Risk Management Framework. ***Risks***, 11(6), 101. https://doi.org/10.3390/risks11060101

[11] MHAMMED, K. (2025). Cyber Intelligence & Moroccan National Security: What Strategy for Managing and Mitigating Cyber Threats against Future Sporting Events. ***Journal of Cyber Security and Risk Auditing***, 2025(4), 366–383. https://doi.org/10.63180/jcsra.thestap.2025.4.12

[12] POLLINI, A., CALLARI, T. C., TEDESCHI, A., RUSCIO, D., SAVE, L., CHIARUGI, F., & GUERRI, D. (2022). Leveraging human factors in cybersecurity: An integrated methodological approach. ***Cognition, Technology & Work***, 24(2), 371–390. https://doi.org/10.1007/s10111-021-00683-y

[13] PRINCIPE, V., RIBEIRO, T., & LÓPEZ-CARRIL, S. (2025). Transformative blockchain technological approaches to sports events. ***Frontiers in Sports and Active Living***, 7, 1547137. https://doi.org/10.3389/fspor.2025.1547137

[14] 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. https://doi.org/10.3390/s23156666

[15] SARKER, I. H., JANICKE, H., MOHSIN, A., GILL, A., & MAGLARAS, L. (2024). Explainable AI for cybersecurity automation, intelligence and trustworthiness in digital twin: Methods, taxonomy, challenges and prospects. ***ICT Express***, 10(4), 935–958. https://doi.org/10.1016/j.icte.2024.05.007

[16] SETIAWAN, A., MUFTI, A., AIJAT MAU, F., PURKONI, A. (2025). Bridging Cybersecurity and Enterprise Risk Management in the Digital Era. TechComp Innovations: ***Journal of Computer Science and Technology***, 2(1), 28–38. https://doi.org/10.70063/techcompinnovations.v2i1.66

[17] WATCHERS, S., FOWLER, B., & SMITH, J. (2024). Beyond Gates and Metal Detectors: Understanding Security for Professional Sports Facilities. ***Sports Innovation Journal***, 5, 20–37. https://doi.org/10.18060/26908

[18] YAACOB, M. N., SYED IDRUS, S. Z., & IDRIS, M. (2023). Managing Cybersecurity Risks in Emerging Technologies. International ***Journal of Business and Technopreneurship (IJBT)***, 13(3), 253–270. https://doi.org/10.58915/ijbt.v13i3.297

Adam JACKO, Ing.
Michal VARMUS, assoc. prof., Ing., PhD.
Radoslav JANKAL, assoc. prof., Ing., PhD.
University of Žilina, Faculty of Management Science and Informatics, Department of Managerial Theories
Univerzitná 8215/1, 010 26 Žilina, Slovakia
e-mail: adam.jacko@fri.uniza.sk

THE PRACTICAL DEPLOYMENT OF UAVS: A MARKET ANALYSIS AND CASE STUDY APPROACH

SILVIA KRÚPOVÁ – GABRIEL KOMAN – ONDREJ STOPKA

Abstract: *The rapid advancement of unmanned aerial vehicle (UAV) technologies has significantly transformed a wide range of industries, enabling new operational capabilities and enhancing efficiency across multiple sectors. This study aims to examine the practical deployment of UAVs through a combined approach of market analysis and case study evaluation. The research investigates current market trends, key industry segments, and the regulatory environment shaping UAV adoption, while also providing in-depth insights into real-world applications. A mixed-methods approach is employed, integrating secondary data analysis of market reports with qualitative examination of selected case studies in sectors such as agriculture, logistics, and infrastructure inspection. The findings highlight the growing economic importance of UAVs, driven by technological innovation, decreasing costs, and expanding commercial use cases. At the same time, the study identifies critical challenges, including regulatory constraints, safety concerns, and limitations in operational scalability. The case study analysis demonstrates that UAV deployment can lead to substantial improvements in data collection, cost efficiency, and operational safety, although outcomes vary depending on industry context and implementation strategies. This paper contributes to the existing literature by linking macro-level market developments with micro-level practical applications, offering a comprehensive perspective on UAV integration in contemporary practice. The results provide valuable insights for policymakers, industry stakeholders, and researchers, and suggest directions for future research focused on regulatory harmonization and technological standardization.*

Keywords: *Unmanned Aerial Vehicles (UAVs); drone technology; market analysis; case study; UAV applications; precision agriculture; infrastructure inspection; drone logistics; regulatory frameworks; autonomous systems*

JEL Classification: *M15*

1. INTRODUCTION

Unmanned aerial vehicles (UAVs) have emerged as a transformative technology with rapidly expanding applications across both civilian and commercial domains. Initially developed for military purposes, UAVs have evolved significantly due to advances in sensor systems, navigation technologies, and data processing capabilities, enabling their deployment in increasingly complex operational environments (Clothier et al., 2015; Gupta et al., 2016).

The growing affordability and accessibility of UAV systems have accelerated their adoption across multiple industries, including agriculture, logistics, infrastructure inspection, and environmental monitoring. In these sectors, UAVs contribute to improved efficiency, enhanced data acquisition, and reduced operational risks (Zhang & Kovacs, 2012; Chung et al., 2020). For example, precision agriculture utilizes UAVs for crop monitoring and resource optimization, while infrastructure management benefits from safer and more cost-effective inspection processes.

Despite these advancements, the practical deployment of UAVs remains constrained by regulatory, technological, and societal factors. Aviation authorities impose strict operational limitations, particularly for beyond visual line-of-sight (BVLOS) missions, while concerns related to safety, privacy, and cybersecurity continue to influence public acceptance and policy development (Stöcker et al., 2017; Finn & Wright, 2016).

Although existing research has extensively examined UAV technologies and their applications, there is a relative lack of studies that integrate market-level developments with empirical evidence from real-world deployments. This gap limits a comprehensive understanding of how UAV adoption translates into practical outcomes across different industries.

This study addresses this gap by combining market analysis with case study evaluation to examine the practical deployment of UAVs. Specifically, it aims to (1) analyze current trends in the global UAV market, (2) explore the implementation of UAV technologies across selected sectors, and (3) assess the associated benefits and challenges.

The remainder of the paper is structured as follows: Section 2 reviews relevant literature, Section 3 outlines the methodology, Section 4 presents the market analysis, Section 5 discusses case studies, and Section 6 concludes the paper. To provide a theoretical foundation for the research and to contextualize the examined problem, the following section reviews relevant literature on UAV technologies, their applications, market developments, and associated regulatory challenges.

2. LITERATURE REVIEW

This section provides a critical overview of existing research on unmanned aerial vehicles (UAVs), focusing on their technological development, practical applications, market evolution, and associated regulatory challenges. The aim is to synthesize current knowledge and identify key gaps in the literature that justify the focus and contribution of this study.

Technological Development of UAVs

Unmanned aerial vehicles (UAVs) have undergone significant technological evolution over the past decades, largely driven by advances in miniaturization, sensor

integration, and autonomous navigation systems. These developments have enabled UAVs to transition from specialized military tools to versatile platforms applicable across a wide range of civilian and commercial domains. From a technical perspective, UAVs can be broadly categorized into fixed-wing, rotary-wing, and hybrid configurations, each characterized by distinct operational capabilities in terms of endurance, maneuverability, and payload capacity (Gupta et al., 2016).

Recent progress in artificial intelligence, machine learning, and real-time data processing has further enhanced the level of autonomy in UAV operations. As a result, modern UAV systems are increasingly capable of executing complex missions with minimal human intervention, including autonomous navigation, obstacle avoidance, and adaptive decision-making in dynamic environments (Chung et al., 2020). These technological advancements form the foundation for the expanding role of UAVs in contemporary industrial applications.

Applications of UAVs Across Sectors

The practical application of UAVs has expanded considerably, reflecting their adaptability and operational efficiency across diverse sectors. In agriculture, UAVs have become essential tools for precision farming, enabling detailed crop monitoring, yield estimation, and targeted resource application. These capabilities contribute to improved productivity and more sustainable resource management practices (Zhang & Kovacs, 2012).

In the construction and infrastructure sectors, UAVs are increasingly employed for surveying, inspection, and project monitoring. Their ability to access hard-to-reach or hazardous locations enhances safety while simultaneously reducing operational costs and improving data accuracy (Siebert & Teizer, 2014). Similarly, in logistics, UAVs are being explored as a viable solution for last-mile delivery, offering potential advantages in terms of speed, efficiency, and accessibility, particularly in remote or underserved areas (Dorling et al., 2017).

Beyond these sectors, UAVs play a critical role in environmental monitoring and emergency response. Their capacity for rapid data collection in inaccessible or high-risk environments makes them valuable tools for disaster management, environmental assessment, and search-and-rescue operations (Colomina & Molina, 2014). Collectively, these applications underscore the versatility of UAV technologies and their growing importance in modern industry.

Market Development and Industry Trends

The global UAV market has experienced substantial and sustained growth, driven by increasing commercial demand, rapid technological innovation, and declining system costs. The expansion of UAV applications across multiple industries has contributed to the emergence of new business models and service-oriented solutions. Market analyses suggest that the commercial UAV sector is expected to continue its upward trajectory, with particularly strong growth in agriculture, energy, and logistics (PwC, 2016).

At the same time, the market is characterized by increasing investment in research and development by both established technology companies and specialized UAV manufacturers. These investments are aimed at enhancing system capabilities, improving reliability, and expanding the range of possible applications. However, the pace and extent of market growth remain closely linked to regulatory developments. Aviation authorities, such as the Federal Aviation Administration (FAA) and the European Union Aviation Safety Agency (EASA), play a central role in defining operational constraints and enabling or restricting advanced UAV operations (Stöcker et al., 2017). The lack of regulatory harmonization across regions continues to represent a significant barrier to the global scalability of UAV services.

The integration of UAVs into civil airspace introduces a range of regulatory and ethical challenges that must be addressed to ensure safe and responsible operation. Safety concerns are particularly significant in densely populated areas, where UAV operations pose potential risks to people and infrastructure. Consequently, strict regulatory frameworks and technological safeguards are required to mitigate these risks.

In parallel, issues related to privacy and data protection have become increasingly prominent. UAVs are capable of capturing high-resolution imagery and sensitive data, raising concerns about surveillance and the misuse of personal information (Finn & Wright, 2016). Additionally, cybersecurity represents a critical area of concern, as UAV systems may be vulnerable to unauthorized access, data breaches, or malicious interference. Addressing these challenges requires coordinated efforts among policymakers, industry stakeholders, and researchers, as well as the development of comprehensive regulatory and technological solutions.

Despite the growing body of literature on UAV technologies and their applications, several gaps remain evident. Existing research tends to focus predominantly on technical aspects or specific application domains, often neglecting the broader relationship between market dynamics and practical implementation. Furthermore, there is a limited number of studies that provide comparative insights into how UAV deployment varies across industries and regulatory environments.

This study seeks to address these limitations by adopting an integrated approach that combines market analysis with case study evaluation. By linking macro-level market trends with micro-level operational evidence, the research aims to provide a more comprehensive understanding of UAV deployment in practice and contribute to the development of a more holistic perspective within the existing literature.he analysis of literature sources focused primarily on the characteristics of the terms smart city, sport management and their mutual comparison.

"The concept of Smart City originated in the early 1990s. The term encompasses the development of cities with new and improved developments in technology, innovation and globalization. Informational knowledge is used to address challenges such as urban transportation, service delivery, electricity and water distribution, and ensuring public safety," (Telang et al., 2021).

To fully understand this concept, it is useful to first briefly look at the word "smart" itself. In the context of technology, the term "smart" is used to refer to devices, systems, or places. It encompasses a multidimensional view including

information processing, internal regulation, operating in the world and knowledge acquisition, (Alter, 2020). According to Finocchi, Perri and Peverini (2020), in order for objects to be considered smart, they need to have certain characteristic properties. These include different degrees of substitutability, autonomy and authority.

Consequently, the Smart City concept represents the integration of these smart objects and information and communication technologies (ICTs) within cities in order to improve the services provided by the city and, ultimately, also to improve the quality of life of citizens. Smart cities largely focus on fostering technological innovation, developing no-new industries, strengthening the economy and maintaining a sustainable environment (Law, Lynch, 2019).

A common characteristic of the previous definitions is the improvement of the quality of life of citizens as the main goal of creating a Smart City. Janani et al. (2023) in their definition of the Smart City goal emphasize "addressing the challenges of resource scarcity, environmental pollution, population growth, and demographic change through technical, economic, and social innovations."

The concept of smart cities has gained substantial attention in recent years, characterized by the integration of information and communication technologies (ICT) to enhance the efficiency and sustainability of urban services. As urban populations continue to grow, the need for innovative solutions to manage resources, improve quality of life, and promote active lifestyles has become more pressing. This literature review explores the intersection of smart city initiatives and sport management, examining how these technologies can enhance sport participation (Bilohur et al., 2022).

Smart Cities and Technological Integration

The theoretical foundations of smart cities are built upon the integration of ICT, IoT, and data analytics to create interconnected urban environments. According to Hollands (2008), a smart city utilizes digital technology to enhance performance and well-being, reduce costs and resource consumption, and engage more effectively with its citizens. Similarly, Caragliu et al. (2011) emphasize the role of ICT in improving urban functionality and sustainability. These foundational perspectives underscore the potential of smart technologies to transform urban services, including sports facilities and programs.

Building on the insights derived from the existing literature, the following section outlines the methodological approach adopted in this study to investigate the practical deployment of UAVs.

3. METHODOLOGY

The primary objective of this study was to examine the practical deployment of unmanned aerial vehicles (UAVs) by integrating market analysis with real-world case study evaluation. To achieve this objective, the research involved (1) a comprehensive review of academic literature, industry reports, and relevant online sources focusing on UAV applications, market developments, and regulatory frameworks, and (2) an analysis of selected case studies from sectors such as agriculture, logistics, and infrastructure inspection.

Content analysis was employed to process and interpret the collected data. The research utilized both deductive and inductive reasoning, alongside methods of comparative analysis, abstraction, and synthesis, in order to identify key trends, patterns, and relationships within the UAV market and its practical applications. The market analysis was based on secondary data obtained from publicly available reports and statistical databases, enabling the identification of major industry segments, growth dynamics, and influencing factors.

The case studies were selected based on their relevance, data availability, and representativeness of different application domains, allowing for a deeper understanding of operational benefits, limitations, and contextual differences in UAV deployment. The study adopts a global perspective, reflecting technological, economic, and regulatory aspects influencing UAV adoption. The main limitations of the research are associated with the reliance on secondary data and the selective nature of case studies, which may affect the generalizability of the findings. Based on the described research design and analytical methods, the following section presents the results of the market analysis and case study evaluation.

4. RESULTS

The analysis of secondary data confirms that the global UAV market has experienced sustained and dynamic growth, primarily driven by technological innovation, decreasing hardware costs, and expanding commercial applications. According to industry reports and academic studies, the commercial UAV market is projected to grow at a compound annual growth rate (CAGR) exceeding 15% in the coming years, with strong demand across agriculture, infrastructure, energy, and logistics sectors (PwC, 2016; Statista, 2023; Chung et al., 2020).

Agriculture represents one of the most mature segments, where UAVs are widely adopted for precision farming, remote sensing, and crop health monitoring (Zhang & Kovacs, 2012). Infrastructure inspection has also demonstrated strong growth, supported by the increasing need for efficient monitoring of aging assets (Siebert & Teizer, 2014). The logistics sector, although still emerging, shows rapid innovation and investment, particularly in last-mile delivery solutions (Dorling et al., 2017).

Regulatory frameworks remain a decisive factor influencing market development. Regions with more adaptive regulatory environments—such as the United States and parts of the European Union—demonstrate higher adoption rates, especially in commercial UAV operations (Stöcker et al., 2017; Clothier et al., 2015).

Case Study Results

The case study analysis provides empirical evidence of the practical benefits and limitations of UAV deployment across different sectors.

In agriculture, UAV applications have significantly improved the precision and efficiency of farming practices. Studies indicate that UAV-based monitoring can increase crop yield by up to 20% while reducing input costs through targeted resource application (Zhang & Kovacs, 2012; Hunt & Daughtry, 2018).

In infrastructure inspection, UAVs have enhanced both safety and operational efficiency. By replacing manual

inspections in hazardous environments, UAVs reduce risks to personnel while enabling faster and more accurate data collection (Siebert & Teizer, 2014; Ellenberg et al., 2016).

In logistics, UAVs demonstrate strong potential for optimizing delivery systems, particularly in remote or underserved regions. However, real-world implementation remains constrained by payload limitations, battery capacity, and regulatory restrictions (Dorling et al., 2017; Otto et al., 2018).

Cross-Case Analysis

A cross-case comparison reveals several consistent patterns across sectors. First, UAV deployment leads to significant improvements in data acquisition, operational efficiency, and safety. Second, the economic viability of UAV integration is highly dependent on scale, operational context, and regulatory conditions.

Furthermore, recurring challenges were identified across all case studies, including:

- regulatory constraints limiting operational flexibility,
- technological limitations such as battery life and payload capacity,
- integration challenges with existing workflows and systems.

These findings are consistent with previous research emphasizing the importance of regulatory harmonization and technological standardization for large-scale UAV adoption (Finn & Wright, 2016; Stöcker et al., 2017).

Key Findings

The findings of this study provide a comprehensive insight into the current state and practical implications of UAV deployment across multiple sectors. They can be synthesized into several key thematic areas:

First, the global UAV market demonstrates sustained and dynamic growth, driven by rapid technological innovation, decreasing acquisition and operational costs, and increasing demand for data-driven solutions. This growth is particularly evident in commercial sectors, where UAVs are transitioning from experimental tools to integral components of operational processes (PwC, 2016; Statista, 2023). The expansion of service-based UAV models further indicates a shift toward scalable and accessible deployment.

Second, UAV technologies significantly enhance operational efficiency and data acquisition capabilities. Across all examined sectors, UAVs enable faster, more accurate, and cost-effective data collection compared to traditional methods. This is particularly evident in applications such as precision agriculture and infrastructure inspection, where high-resolution imaging and real-time analytics contribute to improved decision-making and resource optimization (Zhang & Kovacs, 2012; Siebert & Teizer, 2014).

Third, the adoption of UAVs contributes to substantial improvements in occupational safety. By reducing the need for human presence in hazardous environments—such as high-altitude inspections or disaster zones, UAVs mitigate risks and enhance overall operational safety standards. This finding aligns with existing research emphasizing UAVs as tools for risk reduction in industrial contexts (Ellenberg et al., 2016; Campion et al., 2018).

Fourth, regulatory frameworks emerge as a critical determinant of UAV adoption and scalability. While technological capabilities continue to advance rapidly, regulatory restrictions, particularly those related to beyond visual line-of-sight (BVLOS) operations, airspace integration, and certification requirements—remain significant barriers to widespread implementation. Differences in regulatory approaches across regions further contribute to uneven market development (Stöcker et al., 2017; Clothier et al., 2015).

Fifth, the effectiveness and economic viability of UAV deployment are highly context-dependent. Factors such as industry type, scale of operation, infrastructure readiness, and level of technological integration play a crucial role in determining the overall impact of UAV adoption. While some sectors, such as agriculture, demonstrate immediate and measurable benefits, others—such as logistics—are still in transitional or pilot phases (Dorling et al., 2017; Zeng et al., 2019).

Finally, several persistent challenges continue to limit the full potential of UAV technologies. These include technological constraints (e.g., battery life, payload capacity), cybersecurity and privacy concerns, and difficulties related to system integration and interoperability. Addressing these challenges will require coordinated efforts in technological development, regulatory harmonization, and standardization processes (Finn & Wright, 2016).

Overall, the findings highlight that while UAVs offer substantial benefits and transformative potential, their large-scale deployment depends on the alignment of technological capabilities, regulatory frameworks, and industry-specific requirements. The results presented above are further interpreted and critically discussed in relation to existing literature and broader industry developments in the following section

5. DISCUSSION

The findings of this study confirm that the deployment of UAVs represents a significant technological and economic shift across multiple industries. Consistent with previous research, UAVs are increasingly transitioning from experimental tools to integral components of operational systems (Chung et al., 2020; Gupta et al., 2016; Hassanalian & Abdelkefi, 2017). The strong market growth identified aligns with broader industry analyses emphasizing the expanding role of UAVs in automation and digital transformation (PwC, 2016; Statista, 2023; Deloitte, 2020).

A key contribution of this study lies in linking market-level developments with empirical evidence from case studies. Existing literature often focuses on isolated applications; however, this study demonstrates that successful UAV integration depends on sector-specific conditions and operational requirements (Zhang & Kovacs, 2012; Siebert & Teizer, 2014; Lyu et al., 2020). This supports the argument that the effectiveness of UAV deployment is closely tied to the alignment between technological capabilities and application context.

The role of regulatory frameworks remains central to UAV adoption. Despite technological progress, regulatory constraints—particularly concerning beyond visual line-of-sight (BVLOS) operations—continue to limit scalability. This

finding is consistent with prior studies highlighting regulatory fragmentation as a major barrier to industry growth (Stöcker et al., 2017; Clothier et al., 2015; EASA, 2021). Furthermore, public perception and safety concerns continue to influence regulatory decision-making processes (Mozaffari et al., 2019; Boucher, 2015).

The variability of UAV impact across sectors also emerged as a key finding. While agriculture demonstrates immediate and measurable benefits, other sectors such as logistics remain in developmental stages due to technological and infrastructural limitations (Dorling et al., 2017; Otto et al., 2018; Goodchild & Toy, 2018). This suggests that UAV adoption follows an uneven trajectory across industries, influenced by both economic and technological readiness.

In addition, the study reinforces the importance of UAVs in improving safety and reducing operational risks. Their application in hazardous environments significantly reduces the need for human intervention, aligning with previous findings in infrastructure and disaster management research (Ellenberg et al., 2016; Erdelj et al., 2017; Motlagh et al. 2017). However, these benefits are accompanied by emerging concerns related to privacy, cybersecurity, and ethical implications, which remain insufficiently addressed in current regulatory frameworks (Finn & Wright, 2016; West & Bowman, 2016; LI et al., 2020).

Finally, the study highlights the need for further integration of UAV systems with broader digital ecosystems, including Internet of Things (IoT) platforms and smart infrastructure. Future developments in autonomous systems, artificial intelligence, and communication technologies are expected to further enhance UAV capabilities and expand their application potential (Khan et al., 2021; Shakhatreh et al., 2019).

6. CONCLUSION

This study examined the practical deployment of unmanned aerial vehicles (UAVs) through a combined approach of market analysis and case study evaluation. The findings confirm that UAV technologies are becoming increasingly integrated into a wide range of industrial applications, driven by technological advancements, cost reductions, and the growing demand for efficient and data-driven solutions.

The market analysis demonstrated strong and sustained growth in the global UAV sector, particularly within commercial applications such as agriculture, infrastructure inspection, and logistics. At the same time, the case study analysis provided empirical evidence of the operational benefits of UAV deployment, including improved data accuracy, enhanced efficiency, and increased safety. These findings highlight the transformative potential of UAVs as tools for innovation and optimization across multiple sectors.

However, the study also identified several key challenges that continue to limit the full-scale adoption of UAV technologies. Regulatory constraints, particularly those related to airspace integration and beyond visual line-of-sight operations, remain a major barrier to scalability. Additionally, technological limitations, such as battery life and payload capacity, as well as concerns related to privacy and cybersecurity, present ongoing challenges that must be addressed.

The results suggest that the successful integration of UAVs depends on the alignment of technological capabilities, regulatory frameworks, and industry-specific requirements. Sectors with clearly defined use cases and supportive regulatory environments are more likely to achieve effective and scalable implementation.

From a theoretical perspective, this study contributes to the existing literature by linking macro-level market trends with micro-level operational insights. From a practical standpoint, the findings provide valuable guidance for policymakers, industry stakeholders, and technology developers in shaping future UAV strategies and investments.

Future research should focus on the development of standardized regulatory frameworks, advancements in autonomous UAV systems, and the exploration of new application domains. In addition, further empirical studies are needed to assess the long-term economic and societal impacts of UAV deployment in real-world contexts.

Acknowledgement

This publication was realized with support of Operational Program Integrated Infrastructure 2014 - 2020 of the project: Intelligent operating and processing systems for UAVs, code ITMS 313011V422, co-financed by the European Regional Development Fund.

REFERENCES

[1] CLOTHIER, R. A. et al. (2015) Risk perception and the public acceptance of drones. In: ***Risk Analysis***, 35(6). DOI: https://doi.org/10.1111/risa.12330

[2] CHUNG, S. H. et al. (2020) Optimization for drone and drone-truck combined operations. In: ***Computers & Operations Research***, 123. DOI: https://doi.org/10.1016/j.cor.2020.105004

[3] COLOMINA, I. and MOLINA, P. (2014) Unmanned aerial systems for photogrammetry and remote sensing. In: ***ISPRS Journal***. DOI: https://doi.org/10.1016/j.isprsjprs.2014.02.013

[4] DORLING, K. et al. (2017) Vehicle routing problems for drone delivery. In: ***IEEE Transactions***. DOI: https://doi.org/10.1109/TSMC.2016.2582745

[5] ELLENBERG, A. et al. (2016) Bridge inspection using UAVs. In: ***Journal of Bridge Engineering***. DOI: https://doi.org/10.1061/(ASCE)BE.1943-5592.0000862

[6] FINN, R. L. and WRIGHT, D. (2016) Privacy and ethics for UAVs. In: ***Computer Law & Security Review***. DOI: https://doi.org/10.1016/j.clsr.2016.05.010

[7] GUPTA, L. et al. (2016) Survey of UAV systems. In: ***Journal of Intelligent & Robotic Systems***. DOI: https://doi.org/10.1007/s10846-016-0368-6

[8] HUNT, E. R. and DAUGHTRY, C. (2018) UAVs in agriculture. In: ***Remote Sensing***. DOI: https://doi.org/10.3390/rs10040570

[9] OTTO, A. et al. (2018) Optimization for UAV logistics. In: ***Transportation Science***. DOI: https://doi.org/10.1287/trsc.2017.0797
[10] PWC (2016) Clarity from above. Available at: https://www.pwc.com
[11] SIEBERT, S. and TEIZER, J. (2014) UAV construction monitoring. In: ***Automation in Construction***. DOI: https://doi.org/10.1016/j.autcon.2014.01.004
[12] STÖCKER, C. et al. (2017) UAV regulation review. In: ***Remote Sensing***. DOI: https://doi.org/10.3390/rs9050459
[13] ZHANG, C. and KOVACS, J. (2012) UAVs in agriculture. In: ***Precision Agriculture***. DOI: https://doi.org/10.1007/s11119-012-9274-5
[14] STATISTA (2023) Drone market forecast. Available at: https://www.statista.com
[15] HASSANALIAN, M. and ABDELKEFI, A. (2017) UAV classification and design. In: ***Progress in Aerospace Sciences***. DOI: https://doi.org/10.1016/j.paerosci.2017.04.003
[16] DELIOTTE (2020) Drone market insights. Available at: https://www2.deloitte.com
[17] LYU, X. et al. (2020) UAV applications in smart cities. In: ***IEEE Access***. DOI: https://doi.org/10.1109/ACCESS.2020.2974569
[18] GOODCHILD, A. and TOY, J. (2018) UAV delivery challenges. In: ***Transportation Research***. DOI: https://doi.org/10.1016/j.trc.2018.05.002
[19] ERDELJ, M. et al. (2017) UAVs in disaster management. In: ***Ad Hoc Networks***. DOI: https://doi.org/10.1016/j.adhoc.2016.10.002
[20] WEST, D. and BOWMAN, J. (2016) UAV ethics and regulation. In: ***Brookings Report***.
[21] BOUCHER, P. (2015) Domesticating drones. In: Science and Public Policy. DOI: https://doi.org/10.1093/scipol/scv047
[22] KHAN, M. et al. (2021) UAVs and IoT integration. In: ***Future Generation Computer Systems***. DOI: https://doi.org/10.1016/j.future.2020.10.021
[23] SHAKHATREH, H. et al. (2019) UAV communication networks. In: ***IEEE Access***. DOI: https://doi.org/10.1109/ACCESS.2019.2902843
[24] LI, J. et al. (2020) Deep learning for UAV-based object detection and tracking: A survey. In: ***IEEE Transactions on Neural Networks and Learning Systems***. DOI: https://doi.org/10.1109/TNNLS.2020.2972418
[25] MOTLAGH, N. H. et al. (2017) Low-altitude unmanned aerial vehicles-based Internet of Things services: Comprehensive survey and future perspectives. In: ***IEEE Internet of Things Journal***, 3(6). DOI: https://doi.org/10.1109/JIOT.2016.2612119
[26] CAMPION, M. et al. (2018) UAV swarm communication and control architectures: A review. In: ***Journal of Unmanned Vehicle Systems***, 6(1). DOI: https://doi.org/10.1139/juvs-2017-0019
[27] ZENG, Y. et al. (2019) Accessing from the sky: A tutorial on UAV communications for 5G and beyond. In: ***Proceedings of the IEEE***, 107(12). DOI: https://doi.org/10.1109/JPROC.2019.2952062
[28] MOZAFFARI, M. et al. (2019) A tutorial on UAVs for wireless networks: Applications, challenges, and open problems. In: ***IEEE Communications Surveys & Tutorials***, 21(3). DOI: https://doi.org/10.1109/COMST.2019.2902862

Gabriel KOMAN, doc. Ing., PhD.
Silvia KRÚPOVÁ, Ing.
Faculty of Management Sciences and Informatics, University of Žilina
Univerzitná 8215/1, 010 26 Žilina, Slovakia
e-mail: gabriel.koman@fri.uniza.sk, silvia.krupova@stud.uniza.sk

Ondrej STOPKA, doc. Ing., PhD.
Institute of Technology and Business in České Budějovice, Faculty of Technology
Okružní 10, České Budějovice, 370 01 – budova D, Czech Republic
e-mail: stopka@mail.vstecb.cz

STATUS OF PEOPLE WITH DISABILITIES IN THE LABOR MARKET

ALŽBETA KUCHARČÍKOVÁ – IVANA POMPUROVÁ

Abstract: *The aim of the article is to identify disadvantaged groups of people in the labor market, then focus on the characteristics and analysis of the position of people with disabilities in society and on the labor market. In the article, we also discussed the possibilities of improving their situation on the labor market and how digital technologies can contribute to this.*

Keywords: *disadvantaged people, people with disabilities, labor market, digital technologies*

JEL Classification: *J14, J 21, O 33*

1. INTRODUCTION

The labor market is a key market of the economy, where employers and job seekers meet. In the labor market, supply and demand meet. People on the labor market offer their labor and human capital, while businesses and the state demand and use them as an input that is an essential part of the production process. However, there are groups in this market whose work is not so much in demand due to their personal characteristics or work experience. These groups are referred to as disadvantaged job seekers in the Slovak Republic.

2. LITERATURE REVIEW

2.1 Identification and characterization of disadvantaged groups of people in the labor market

The identification of disadvantaged groups of citizens on the labor market in the Slovak Republic is enshrined in Act No. 5/2004 about Employment Services, as amended from 1 January 2025. The Act designates these groups as disadvantaged job seekers and identifies the following groups: *school graduates, citizens over 50 years of age, long-term unemployed citizens, long-term unemployed citizens, citizens with less than secondary vocational education, third-country nationals who have been granted asylum or subsidiary protection, single persons caring for a child or other dependent person, citizens with disabilities, and persons returning to the labor market after maternity or parental leave who did not have employment income while receiving the benefit.*

Several Slovak authors rely on this law in their publications when identifying disadvantaged groups of citizens on the labor market. Pawera et al. (2018) state in their article that the inclusion in the above groups is based on factors such as age, long-term unemployment, migration, education, disability or the inability to reconcile work and family life. They state that these factors limit the employment opportunities of disadvantaged people and worsen their position on the labor market compared to the majority population. Due to their life and social situation, they are perceived by employers as less or completely unattractive. Based on the analysis of the views of various authors on the definition of disadvantaged groups on the market, these authors adjusted the identification of these groups as follows: *women; persons belonging to the Roma ethnic group; persons younger than 26 years of age - graduates who have completed vocational education; seniors (over 50 years of age); persons with disabilities.* According to Ladňáková and Špániková (2020), an individual's chance of obtaining a quality job is influenced by factors such as gender, health status, education, age and ethnic origin. These factors represent the reasons why disadvantaged groups have worse employment opportunities in the labor market. The authors describe disadvantaged groups of people as risky because they are largely condemned to long-term unemployment or repeated job losses. In their article Zeman and Zubaľová (2020) criticize the insufficient legislative definition of disadvantaged groups in the legal order of the Slovak Republic. They point out in particular that the exhaustive list lacks several groups that face significant barriers in practice on the labor market. These groups included parents returning from parental or maternity leave without prior employment, young people leaving children's homes, marginalized Roma communities, and also persons after completing a prison sentence.

In *foreign literature,* disadvantaged groups are often *referred to* as *discriminated against*. Calderón-Milán et al . (2020) use this term to refer to people whose *work and social characteristics* lead to them being negatively discriminated against in the regular labor market. They also included *women, young people, people with disabilities, and people with lower levels of education or insufficient qualifications in the group of discriminated against people in the labor market.* Deselnicu et al. (2024) identified older and younger employees, women, people at risk of poverty, Roma, and adults with disabilities as discriminated against groups of workers. The authors point out that these groups face various forms of unequal treatment, social stereotypes, and limited opportunities in the labor market.

Based on the analysis of the views of individual authors, it can be stated that women*, citizens belonging to the Roma ethnic group, citizens at risk of poverty, citizens who were not employed before the start of maternity or parental leave, young people leaving children's homes and citizens returning from prison* can also be added to the legally defined disadvantaged groups of job seekers (school graduates, citizens over 50 years of age, long-term unemployed citizens, citizens with less than secondary vocational education, long-term unemployed citizens, asylum seekers or persons with supplementary protection, single persons caring for a child or

other dependent person, citizens with disabilities, citizens after maternity or parental leave without employment income).

2.2 People with disabilities

Citizens with health disabilities are also a disadvantaged group on the labor market. Disadvantage can manifest itself at various levels of physical, mental, or social functioning.

Kuklek et al. (2021) identified disability as one of the most significant barriers to the labor market. It can take various forms, such as visual impairment, physical mobility limitations, communication problems, or reduced quality of life, etc. People with disabilities constitute a very diverse group with different needs and problems. The authors also stated that there is a high correlation between adult disability and high psychological stress.

Michna et al. (2017) reported in their research that despite the continuous efforts of individual countries to increase the employment of people with disabilities, their employment rate remains significantly lower compared to people without disabilities. The results of their research indicate that the main obstacles faced by employers in the selection process for these people include, in particular, insufficient education or qualifications.

A 2025 study found that people with disabilities prefer the option of working from home. If the number of job opportunities that allow remote work increases, the labor market could be much more inclusive for people with disabilities. The positive effect of this phenomenon has already begun to be felt to some extent as a result of the lockdown during the COVID-19 pandemic (Derbyshire et al., 2025).

Thanks to the analysis of the above sources, it can be noted that the group of disabled people is very diverse, and therefore there may be several different reasons for difficult entry into the labor market. However, in general, this disadvantaged group has a higher unemployment rate than people without disabilities. One option to reduce inequality in the labor market is to allow these people to work from home.

3. METHODOLOGY

The aim of the article is to identify disadvantaged groups of people in the labor market and then focus on the characteristics and analysis of the position of people with disabilities in society and on the labor market. In the article, we used a content analysis of literary sources that relate to the identification and characteristics of people with disabilities. We identified forms of support for these people in the labor market and the possibilities of using digital technologies to facilitate the employment of this group of people who are disadvantaged in the labor market.

4. FINDINGS

4.1 Disability categorization

The term disabled person is understood not only as an officially medically diagnosed person, but also as an individual who feels limited due to treatment or serious illness. Based on this assumption, it can be stated that the group of disabled people is truly diverse and includes various forms of disadvantage that may not even be officially classified. However, for the purposes of this work, this chapter presents the most common types and categories of disability reported in professional literature.

Jenei et al. (2024) confirm in their research that disability can vary in severity from partial to complete and can be temporary or permanent. It can affect *a person's sensory, motor and mental functions, including walking, vision, speech and communication.* In Slovakia, a distinction is made between people with severe disabilities, who are entitled to special social support, and people with less severe disabilities, who can also benefit from social care. A disability level of 41% or more means reduced working capacity, while a rating above 50% is considered severe disability and often significantly limits the ability to perform work.

Zakiei et al. (2020) reported that the main types of disability include *physical-motor, visual, hearing and intellectual disabilities.* They also pointed out that their share represented approximately 3.4% of the world's population. The World Health Organization (WHO) estimated in 2023 that there were approximately 1.3 billion people living with a significant form of disability in the world, which was approximately 16% of the population (Tóthová et al.,2025). Konečný et al. (2025) confirmed that people with disabilities represent the largest minority group in the world, yet they still face significant obstacles in all areas of their lives.

Tarasoff et al. (2020) identified very similar categories of disabilities in their research: physical, sensory, intellectual, and developmental. *Physical disabilities* include conditions such as spinal cord injury or cerebral palsy and are associated with limitations in mobility, flexibility, or fine motor skills. *Sensory disabilities* refer to vision or hearing impairments, which can affect the ability to receive and process information from the external environment. *Intellectual and developmental disabilities* include, for example, Down syndrome or autism spectrum disorder. These types of disabilities are characterized by limitations in cognitive abilities, learning, communication, and adaptation to everyday situations.

Tomek et al. (2014) in their article are based on the UN definition, according to which persons with disabilities are people with long-term *physical, mental, intellectual or sensory limitations.* These limitations can take the form of visual, hearing, physical or mental disorders, which often require a specific approach from the surrounding environment. The authors also point out that disability can affect anyone during their life, either temporarily or permanently.

Birau et al. (2019) found that the type of disability significantly affects the position of people in the labor market. Visually impaired people have the highest employment rate and the shortest average time to regain employment. On the contrary, people with mental or psychological disabilities are in a significantly more disadvantageous position than other groups, according to them. Alzahrani (2025) assessed that people with intellectual and developmental disabilities have a more complicated entry into the labor market and one of the main prerequisites for their employment is quality education.

The above sources show that people with disabilities represent a diverse group and constitute a significant part of the total population. The main types of disability most often included in the professional literature are physical, sensory,

mental and developmental forms of limitations. A disability can be permanent or temporary and affects various areas of life, which subsequently affects the individual's employment opportunities. Research confirms that the type and severity of the disability significantly shape their position on the labor market. People with visual impairment, which is among the sensory limitations, show relatively favorable results. On the contrary, people with mental or developmental disabilities remain in a significantly disadvantaged position. These findings point to the need to perceive disability as a complex phenomenon with a diverse impact on a person's life and at the same time create the basis for the next chapter, which will address the position of these people in society and on the labor market.

4.2 The status of people with disabilities in society and on the labor market

The issue of the position of people with disabilities in the labor market, but also in society as a whole, is addressed by many authors, who draw attention to the persistent inequalities and obstacles preventing their full inclusion.

Fouquet (2025) stated that in developed OECD countries, people with disabilities made up approximately 15% of the working-age population in 2022. Despite the fact that the overall employment rate is growing year-on-year, the employment rate of this disadvantaged group remains approximately 25% lower than that of people without disabilities. The reason may be both the individual limitation in access to work itself, which results from physical or mental limitations, but also the personal preferences of these people. The author highlighted that the reason for the lower employment rate of this group may also be their lower motivation to remain in the labor market due to public transfers and social benefits. This may also be due to discrimination by employers, which is often associated with the assumed lower productivity of these workers.

According to Urbancová et al. (2020), the employment and inclusion of people with disabilities in work collectives are closely linked to diversity in the workplace. Employment represents one of the essential elements of shared recognition and contributes to a sense of inclusion and citizenship. Despite this, people with disabilities remain underrepresented in the labor market.

The UN addresses this issue in the Convention on the Rights of Persons with Disabilities, which obliges states to ensure equal access to employment for people with disabilities. Article 29 of the Convention emphasizes the need for equal employment opportunities in both the public and private sectors and the support of their self-employment, entrepreneurship or establishment of their own businesses by the Ministry of Labor and Social Affairs (Watson et al., 2022).

Urbancová et al. (2020) state that potential job opportunities for this group include, for example, positions in call centers or employment in protected and integrated enterprises, where people with disabilities must make up 20-50% of the workforce. These enterprises operate on a market principle and allow people with disabilities to work under standard conditions, with obtaining a specific position depending on their abilities and skills. Integration projects are most often implemented in sectors such as gastronomy, gardening, crafts or animal care.

Jetha et al. (2020) highlight that people with disabilities face greater difficulties in the labour market, especially in obtaining, maintaining and advancing in employment. Limited labour market participation can make it more difficult to access basic resources such as income, food security and safe housing, which in turn leads to a deterioration in their health and socio-economic status. At the same time, this group of people often needs comprehensive health and support care, and inadequate working conditions can further intensify these needs. Older workers with disabilities are a particularly vulnerable group in the labour market, as health limitations significantly exacerbate their disadvantaged position.

Shaw et al. (2022) in their research strongly emphasize the need to perceive the employment of people with disabilities in a broader social context. They point out that the main challenge of the problem of disadvantage of people with disabilities is that they are still not perceived in society as full citizens with a self-evident right to be part of work and social systems. Persistent stereotypes or prejudices cause their exclusion and prevent them from actively participating in work. To remove these barriers, long-term structural change is needed, based on thorough analysis, with disabled people themselves involved in the process of finding solutions.

The issue of the impact of social exclusion on the integration of people with disabilities into the labor market was also addressed by the authors Birau et al. (2019). In their research, the authors focused on analyzing the situation in *Romania*, describing the integration of this disadvantaged group into the labor market as a sustainable response to the deepening labor shortage. The research results show that the main obstacle for this group is not disability itself, but insufficient infrastructure, complicated access to transport, and persistent social stigma or discrimination. These factors contribute to the fact that many of them stop actively looking for work or have difficulty maintaining employment. Some employers avoid employing people with disabilities due to the need to adjust the working environment and conditions. Finally, the authors criticized the Romanian government's previous measures, which they described as insufficient to address social exclusion and support the labor integration of people with disabilities.

The state of public care for people with disabilities is very inadequate in many less developed countries. A 2025 study by Griffiths et al. provides a compelling example of this claim. The authors focused on how employment rights are implemented in *Uganda,* where approximately 12% of the population is made up of people with disabilities. They point out that despite well-known evidence of discrimination in the labour market, there is little information about the actual implementation of legal norms. They also found that interviews with political leaders influenced their attitudes and intentions, suggesting that even minimal intervention can initiate a change in approach to the issue (Griffiths et al., 2025).

The insufficient implementation of legal norms to support persons with disabilities in African countries was also analyzed by Shumba and Moodley (2018). The authors focused on the state of this issue specifically in *Namibia*, identifying a lack of accountability as the primary cause. They point out that the government there has not created

sufficient mechanisms that would oblige it to be accountable to people with disabilities in the areas of healthcare, education, or social support. According to them, it is the absence of clearly defined accountability that causes a significant gap between the creation and actual implementation of policies.

In contrast to African countries, where legal support for people with disabilities is insufficient, research from other parts of the world shows significant differences in approaches to this issue. For example, Lin et al. (2018) report that in *China* , people with disabilities often deny discrimination, which hinders their social inclusion. At the other end of the spectrum, *Sweden is* one of the most progressive countries in terms of equality and employment for people with disabilities. As many as 78.1% of people with visual impairments and 89.2% of people with hearing impairments work there (Boman, 2015). International data shows that countries with high female employment rates achieve significant GDP growth. Estimates suggest that if women with disabilities were to fully participate in the labor market, economic performance could increase by approximately 3 to 7% (Jenei et al., 2024).

Shabunova et al. (2016) in their study examined what barriers exist for this disadvantaged group in labor market in *Russia* . One of the significant obstacles to promoting the employment of people with disabilities is insufficient vocational training and limited retraining opportunities. They found that only about 38% of people with disabilities work in the field for which they are qualified. Based on the research results, they also identified the main ways that can significantly improve the competitiveness of this group. These were, in particular, increasing financial support for employers of this group, creating a central register of unemployed people with disabilities, and expanding vocational training opportunities that will respond to current needs on the labor market.

According to Ahmed et al. (2025), people with disabilities still perform significantly worse at work than their able-bodied counterparts, despite existing international standards. Al-Hendawi et al. (2024) point out that their hourly wage is around 12% lower on average globally, with the gap even greater in economically weaker countries, exceeding 25%. Although several studies confirm that an inclusive workplace brings economic benefits, such as higher morale and lower turnover, discrimination in the recruitment process persists. This situation is also exacerbated by systemic barriers, in particular employer bias, inadequate infrastructure and poor implementation of existing policies.

By positioning people with disabilities in *Slovak* The labour market was examined by Masárová et al. (2019), who assessed it as unfavourable, although some improvement can be observed in recent years. They state that the share of working people with disabilities is lower than the average in the Slovak Republic and a significant part of this group remains economically inactive. The long-term problem of unemployment of disadvantaged groups in Slovakia is also pointed out by Poláčková (2020), who also criticizes the low level of involvement of non-governmental organisations in supporting the employment of these people.

4.3 Forms of support for the labor and social integration of people with disabilities

Reducing social disparities requires the effective integration of people with disabilities. For them to fully participate in everyday life and the working environment, it is necessary to create suitable conditions for them and provide adequate support.

According to Rahman (2025), it is widely accepted that *vocational rehabilitation* is a key tool for promoting independence and social inclusion of people with disabilities. Vocational rehabilitation is a process that includes various support services, such as job placement, career guidance, job adaptation and skills development. It aims to enable people with disabilities to achieve economic independence and enhance their active participation in social life. Studies from Scandinavian countries, Europe and the United States confirm that individually tailored support leads to higher employment rates. Conversely, in low- and middle-income countries, community-based programmes contribute to empowerment (Chun et al., 2024 , Lee et al., 2020 , Dispenza, 2021).

The issue of supporting the integration of people with disabilities was also addressed by Masan et al. (2022), in the form of *social rehabilitation* . By this term, the authors understand a set of activities that support the independence of a person with a disability and the development of their abilities necessary for everyday life. According to them, social rehabilitation is highly individual, depends on the needs, possibilities and motivation of the individual and requires a special approach from the social worker. It supports self-sufficiency, a sense of self-worth, psychological stability, social relationships and helps overcome psychological barriers that prevent full integration. The authors conducted research in Slovakia that focused on the extent to which social rehabilitation contributes to the integration of people with disabilities into society. The results showed that rehabilitation programs significantly support the independence, self-confidence and social functioning of these people. At the same time, it turned out that high-quality cooperation between clients and workers is an important prerequisite for a successful rehabilitation process. The research also highlighted the need to strengthen professional training and raise awareness of modern trends in social rehabilitation so that these services can be further developed and respond more effectively to the needs of the target group.

Among the forms of support that can significantly contribute to the integration of disabled people, especially in the area of employment, is the possibility of working from home. A 2025 study shows that many disabled people prefer this form of work. Remote work allows them a greater degree of self-sufficiency and reduces the barriers associated with commuting or physical access to the workplace. This form of employment is also beneficial for employers, as adjusting the work environment or working conditions to create an inclusive workplace can be organizationally and financially demanding for many (Derbyshire et al., 2025).

4.4 People with disabilities and digital technologies

With the growing importance of remote work, it is natural to pay attention to the digital technologies that are closely related to it. This chapter therefore focuses on the role that

digital technologies play in the lives of people with disabilities.

Jetha et al. (2023) highlighted the importance of supporting the employment inclusion of people with disabilities in an increasingly digitalised work environment, identifying it as a key priority for social policy and public health. Digital technologies have made significant contributions to the employment integration of people with disabilities by offering digital tools that facilitate their engagement in work (e.g. smartphones or computers), improving assistive devices (e.g. speech-to-text applications) and improving workplace accessibility, for example through robotic systems performing physically demanding tasks.

However, historical data also show that people with disabilities have long faced barriers to accessing and using digital technologies compared to people without disabilities. This inequality is often referred to as the digital divide and is mainly reflected in limited access to the internet (Düplaga, 2017 ; Dijk, 2017). For example, in Canada, in 2017, 19.5% of adults with disabilities did not use the internet (Choi, 2021), compared to approximately 9% of people without disabilities. This gap is driven by a combination of factors, such as low technological literacy, low financial costs or lack of opportunities for technological training. As the work environment increasingly moves online, these limitations directly reduce their employment opportunities (Jetha et al., 2023 ; De et al., 2020).

Fajadro-Castro et al. (2025) report that people with disabilities face significant barriers to accessing integrated employment. They identified people with intellectual disabilities as a group with a higher need for support. Digitalisation may exacerbate their situation, as they are often employed in simple manual positions that can be easily replaced by technology.

This issue was also addressed in the past by the Slovak author Ondrejková (2016), who highlighted the importance of the effective use of modern information and communication technologies by persons with disabilities. The author draws attention to the need to implement new e-government services and create single points of contact in Slovakia, while ensuring web accessibility must also be part of these changes. These changes will enable the full functioning of the given group in the digital society. Research has shown that in the field of electronic communication, people with disabilities achieved a relatively good level of digital skills, which significantly contributes to their everyday life and integration.

4. CONCLUSION

Available sources show that people with disabilities have long been in a disadvantaged position, both on the labor market and in society as a whole. Research agrees that the causes of this condition are extremely complex, as they include not only health restrictions and inadequately adapted working conditions, but also persistent prejudices from the environment. Analyses also show that there are significant differences between the current state of this issue in individual countries. In less developed countries, the problem persists mainly in the weak implementation of legal measures and insufficient support and interest from the state. On the contrary, in more developed countries, social attitudes and low expectations towards this group play a greater role. However, the example of a progressive country shows that with appropriately created conditions and equal treatment, the employment rate of people with disabilities can be significantly higher. Research also shows that, despite the existence of international standards and legislative frameworks, the work outcomes of people with disabilities remain significantly worse in global comparison, and disparities persist, especially in remuneration and recruitment processes. Overall, it can be noted that improving the status of this group requires long-term efforts, as it depends significantly on a gradual change in social attitudes. Therefore, it is necessary to pay attention to forms of support that can truly strengthen their work and social integration, which is discussed in more detail in the following subsection.

In supporting the integration of disabled people into society and the labour market, based on an analysis of available resources, social and vocational rehabilitation is particularly key. These processes include various activities that help develop skills, increase the self-sufficiency of the individual and support their readiness to participate in everyday life and the working environment. Rehabilitation programmes also remove or mitigate barriers that prevent people with disabilities from realising their potential, thereby significantly contributing to their successful integration. In the working environment, the possibility of working from home has proven to be an important form of supporting the integration of this disadvantaged group. This is a form of work that will guarantee their better access to job opportunities and reduce the obstacles that disabled people often encounter.

Based on the analysis of available sources, it follows that digital technologies can significantly support the work integration of people with disabilities, but their benefits are still limited by differences in digital skills and access to modern tools. Although technologies open up new possibilities, not all people with disabilities have ideal conditions for using them. It is also important to take into account that some groups, such as people with intellectual disabilities, need more significant support in the application of digital technologies. At the same time, these people are mainly employed in manual positions requiring low qualifications, which are most at risk of technological replacement. Overall, it appears that more attention will need to be paid to the development of digital skills and abilities and other support measures to strengthen their social and work inclusion.

Acknowledgement

The article was written as part of the solution of the grant task: VEGA 1/0112/25, APVV-25-0117, APVV-25-0085.

REFERENCES

[1] AHMED, I. et al. 2025. Economic inclusion and quality of life: Assessing the impact of integrating people with disabilities into Saudi Arabia's labor market. ***Research in Developmental Disabilities***. 167, 2025.
[2] AL-HENDAWI, M. et al. 2024. Career Choices Among Individuals with Disabilities in the Gulf Region: Cultural, Religious, Policy, and Socio-Economic Influences: A Literature Review. ***Societies***. 14, 2024, 11.
[3] ALZAHRANI, H. 2025. Indicators of competitive employment for individuals with intellectual and developmental disabilities (IDDs) in Saudi Arabia: A qualitative study. ***Acta Psychologica***. 257, 2025.
[4] BIRAU, FR. et al. 2019. Social Exclusion and Labor Market Integration of People with Disabilities. A Case Study for Romania. ***Sustainability***. 11(18), 5014.
[5] BOMAN, T. et al. 2015. Employment opportunities for persons with different types of disability. ***Alter***. 9, 2015, 2, pp. 116-129.
[6] CALDERÓN-MILÁN, MJ et al. 2020. Labour Inclusion of People with Disabilities: What Role Do the Social and Solidarity Economy Entities Play? ***Sustainability***. 2020, 1079.
[7] DE, R. et al. 2020. Impact of digital surge during Covid-19 pandemic: A viewpoint on research and practice. ***International Journal of Information Management***. 55, 2020.
[8] DERBYSHIRE, DW. et al. 2025. Widening inclusion: A discrete choice experiment of job preferences of disabled people. ***Economic and Labour Relations Review***. 36, 2025, 1, pp. 234-256.
[9] DESELNICU, DC et al. 2024. Discrimination Against Vulnerable Personnel in the Workplace. ***Proceedings of the International Conference on Business Excellence***. 18(1), 2024, pp. 1007-1017.
[10] DIJK, V. et al. 2017. Digital Divide: Impact of Access. *The International Encyclopedia of Media Effects.* 2017, pp. 1-11.
[11] DISPENZA, F. 2021. Empowering the Career Development of Persons With Disabilities (PWD). ***Journal of Career Development***. 48, 2021, 5, pp. 670-685.
[12] DUPLAGA, M. 2017. Digital divide among people with disabilities: Analysis of data from a nationwide study for determinants of Internet use and activities performed online. ***PLoS ONE***. 12, 2017, 6.
[13] FAJARDO-CASTRO, L. et al. 2025. Digitalization and integrated employment for persons with intellectual disabilities. ***Research in Developmental Disabilities***. 164, 2025.
[14] FOUQUET, F. 2025. How Does Disability Affect School-to-Work Transitions? Evidence From a French Labour Market Integration Survey. ***Kyklos***. 78, 2025, 4, pp. 1358-1374.
[15] GRIFFITHS, A. et al. 2025. The role of qualitative methods in shaping policy on employment rights for people with disabilities in Uganda. ***Societal Impacts***. 6, 2025.
[16] CHOI, R. 2021. Accessibility Findings from the Canadian Survey on Disability, 2017. ***Canadian Survey on Disability Reports***. 2021.
[17] CHUN, J. et al. 2024. Promoting quality career pathways for individuals with disabilities through the public vocational rehabilitation program. ***Journal of Vocational Rehabilitation***. 60, 2024, 3, pp. 299-310.
[18] JENEI, S. 2024. The workforce challenges of disabled people in Hungary and Slovakia during the COVID-19 pandemic. ***Alter-European Journal of Disability Research***. 18, 2024, 3.
[19] JETHA, A. et al. 2023. Divided in a digital economy: Understanding disability employment inequities stemming from the application of advanced workplace technologies. ***SSM - Qualitative Research in Health***. 3, 2023.
[20] JETHA, A. et al. 2020. The working disadvantaged: the role of age, job tenure and disability in precarious work. ***BMC Public health***. 20(1), 2020, 1900.
[21] KONEČNÝ, V. et al. 2025. Persons with reduced mobility and consequences related to their demand for public passenger transport in the conditions of Slovak Republic. ***Transportation Research Interdisciplinary Perspectives***. 32, 2025.
[22] KUKLEK, NM. et al. 2021. Raising employment and quality of life among people with disadvantages - results of a Hungarian project. ***BMC Public Health***. 21(1), 2021, 1729.
[23] LADŇÁKOVÁ, V., ŠPÁNIKOVÁ, M. 2020. Long-Term Unemployment of the Risk Groups in the Slovak Labour Market. ***Proceedings of CBU in Social Sciences***. 1, pp. 128-133, 2020.
[24] LEE, E. et al. 2020. State Vocational Rehabilitation Services and Employment Outcomes for Asian Americans with Psychiatric Disabilities. ***Community Mental Health Journal***. 56, 2020, 5,pp. 854-866.
[25] LIN, ZX. et al. 2018. Denial of disability discrimination by disabled people in China. ***Disability & Society***. 33, 2018, 5, pp. 804-809.
[26] MASAN, J. et al. 2022. New Trends in the Field of Social Rehabilitation of People with Disabilities. ***Clinical Social Work and Health Intervention***. 13, 2022, 3, pp. 41-46.
[27] MASÁROVÁ, J. et al. 2019. Postavenie osôb so zdravotným postihnutím na trhu práce v slovenskej republike. ***Zdravotnícke listy***. 7, 2019, 4.
[28] MICHNA, A. et al. 2017. Job Preferences and Expectations of Disabled People and Small and Medium-Sized Enterprises in Poland: Implications for Disabled People's Professional Development. ***Human Resource Development Quarterly***. 28, 2017, 3, pp. 299-336.
[29] ONDREJKOVÁ, A. 2016. ADAPTATION TO THE INFORMATION SOCIETY OF PEOPLE WITH DISABILITIES IN SLOVAKIA. *CBU* ***International Conference Proceedings 2016: Innovations in Science and Education***. 4, 2016, pp. 262-275.
[30] PAWERA, R. et al. 2018. An issue of age in the labour market in Slovakia. ***Economic Annals****-XXI.* 168, 2018, 12-12, pp. 93-99.
[31] POLÁČKOVÁ, Z. 2020. The role of organizations of the non-profit sector in the employment of people disadvantaged in the labour market in Slovakia. ***Problemy Polityki Spolecznej***. 50, 2020, pp. 27-41.
[32] RAHMAN, MH. 2025. Gender disparities in vocational rehabilitation: A scoping review on employment and empowerment among persons with disabilities. ***Journal of Medicine, Surgery, and Public Health***. 7, 2025.
[33] SHABUNOVA, AA. et al. 2016. Pressing Issues of Disability Employment. ***Economic and Social Changes-Facts Trends Forecast***. 48, 2016, 6, pp. 126-142.

[34] SHAW, J. et al. 2022. Achieving disability inclusive employment – Are the current approaches deep enough? ***Journal of International Development.*** 34, 2022, 5, pp. 942-963.
[35] SHUMBA, T. et al. 2018. Implementation of disability policy framework in Namibia: A qualitative study. ***South African Journal of Physiotherapy***. 74(1), 2018.
[36] TARASOFF, L. et al. 2020. Maternal disability and risk for pregnancy, delivery, and postpartum complications: a systematic review and meta-analysis. ***American Journal of Obstetrics and Gynecology***. 222, 2020, 1, pp. 27-32.
[37] TOMEK, M. et al. 2014. Transport safety at evacuation for people with disabilities. ***Kontakt***. 16, 2014, 3, pp.195-202.
[38] TÓTHOVÁ, L. et al. 2025. Differences in the subjective quality of life among individuals with physical disabilities based on sports activity-in the Slovak contextT. ***Kontakt-Journal of Nursing and Social Sciences Related to Health and Illness***. 27, 2025, pp. 288-294.
[39] URBANCOVÁ, H. et al. 2020. Diversity Management as a Tool of Sustainability of Competitive Advantage. ***Sustainability***. 12(12), 2020, 5020.
[40] WATSON, J. et al. 2022. The impact of the United Nations Convention on the Rights of Persons with Disabilities (CRPD) on Victorian guardianship practice. ***Disability and Rehabilation***. 44, 2022, 22, pp. 2806-2814.
[41] ZAKIEI, A. et al. 2020. Classification of various types of disability and determining their predictive causes in western Iran. ***Clinical Epidemiology and Global Health***. 8, 2020, 1, pp. 1-7
[42] Zákon o službách zamestnanosti. 2025. Zákon č. 5/2004 Z. z. ***Slov-lex***. [Online] 2025. https://www.slov-lex.sk/ezbierky/pravne-predpisy/SK/ZZ/2004/5/.
[43] ZEMAN, J., ZUBAĽOVÁ, A. 2020. The Employment Support of Disadvantaged Population in the Open Labor Market with an Emphasis on Disabled People in Slovakia. ***Scientific Papers of the University of Pardubice-Series D-Faculty of Economics and Administration***. 2020, 28, 1.

Alžbeta KUCHARČÍKOVÁ, prof., Ing., PhD.
Ivana POMPUROVÁ, Bc.
University of Zilina, Faculty of Management Science and Informatics, Department of Macro and Microeconomics
Univerzitná 8215, 010 26 Zilina, Slovakia
e-mail: alzbeta.kucharcikova@uniza.sk

EMPLOYMENT OF PEOPLE WITH DISABILITIES IN THE LABOR MARKET – ANALYSIS OF RESEARCH STUDIES

ALŽBETA KUCHARČÍKOVÁ – IVANA POMPUROVÁ

Abstract: *The aim of this article is to find out what is the position of people with disabilities in the labor market, what are the barriers to employment and what conditions need to be changed to facilitate the employment of these people. In the article, we identified, analyzed and compared the results of various 10 research studies which were conducted in Europe, Asia and Canada. To achieve the goal, scientific methods of description, content analysis, comparison and synthesis were used.*

Keywords: *people with disabilities, labor market, employment, barriers, education*

JEL Classification: *J14, J 20*

1. INTRODUCTION

The labor market is a space where demand and supply for labor and human capital meet. Both of these factors are owned, offered on the labor market, and subsequently rented by economic entities called households. Labor and human capital represent essential production inputs for enterprises, for which they pay wages to households. Payments for the rental of labor and human capital represent production costs for enterprises. On the supply side of the labor market, there are also groups of people who have problems with employment due to the existence of various disabilities. This includes, for example, people with health disabilities. Despite legislative measures and the growing emphasis on inclusion, these people often encounter barriers in obtaining and maintaining employment. The most significant obstacles include employer prejudices, an inadequately adapted work environment, or limited access to education and retraining. Health disabilities can thus lead to lower employment rates and a higher risk of social exclusion. However, the employment of people with disabilities brings benefits not only to individuals, but also to society as a whole. Employment promotes diversity, social cohesion, and more efficient use of the production factor labor and human capital. The article synthesizes the results of international research surveys that have addressed the position of people with disabilities in national labor markets.

2. LITERATURE REVIEW - PEOPLE WITH DISABILITIES

To understand the position of people with disabilities in society and on the labor market, it is first necessary to define who belongs to this group and what characteristics distinguish them from the rest of the population. According to Orieshchikova (2014), people with disabilities are among the marginalized groups who often need special help from professionals. However, their basic needs are the same as those of the majority population, because they also need love, acceptance, space for development and self-realization. However, disability brings limitations that affect all areas of their lives. People with mental, physical or sensory disabilities often have to face various barriers. These can be communication, spatial or appearance barriers, but they also have to resist invisible barriers in the form of prejudice and lack of acceptance from others.

People with disabilities are considered not only those whose disability has been officially confirmed by a medical report, but also people who subjectively feel that they are health-impaired due to a chronic illness or treatment. Such limitations affect their quality of life and interfere with their daily functioning, as well as their opportunities to apply themselves in the labor market. Although the number of people with disabilities in the working age group is increasing and policy measures are responding to this group more and more actively, there are few studies that focus on labor market policies supporting their work integration from the perspective of the actors involved themselves (Holubová et al., 2024 ; Sollár et al., 2022)

According to Marceková et al. (2021) , people with disabilities are a minority in society and often remain on the margins of social events. They encounter barriers every day that complicate their daily activities and make it difficult to fully integrate among people without disabilities. Bendíková et al. (2018) argue that people with disabilities have more limited access to healthcare, income programs, social support, education, leisure activities, and even employment opportunities that would positively affect their psychological well-being.

Šubová (2023) stated in her research that EU countries use various social policy instruments to prevent financial vulnerability of households and mitigate the consequences of illness or job loss. Based on the analysis of social expenditure, she concluded that people with disabilities have long been among the most supported groups within the EU, which is also confirmed by the findings of Halásková (2018). This fact indicates that people with disabilities are considered a group with a high level of vulnerability within social policy and therefore require systematic and long-term support.

Based on the analysis of the sources, it can be concluded that a person with a disability can be considered an individual whose health limitations affect their daily functioning and access to opportunities. This group includes not only people with an officially confirmed disability, but also people who feel limited as a result of illness or treatment. Research shows that these people often face various barriers and social disadvantages, which limit their full participation in social life. The findings also confirm that within the EU they are

considered one of the most vulnerable groups and therefore require long-term support from social policy.

3. METHODOLOGY

The aim of this article is to find out what the position of people with disabilities is in the labour market, what are the barriers to employment and what conditions need to be changed to facilitate the employment of these people. In the article, we identified, analysed and compared the results of various research studies that have been published since 2017, with some surveys being conducted earlier. To achieve the goal, scientific methods of description, content analysis, comparison and synthesis were used. 10 research studies were selected for comparison, which were conducted in Europe, Asia and Canada.

4. FINDINGS

4.1 Research studies

RESEARCH STUDY 1 - SURVEY OF THE FUNCTIONALITY OF PORTUGAL LEGAL MECHANISMS IN THE FIELD OF WORK INTEGRATION OF PEOPLE WITH DISABILITIES (PORTUGAL)

The first foreign research study that will be presented in more detail in this subsection is a survey from 2024, which *examined whether Portuguese legal mechanisms supporting the working conditions of people with disabilities actually work in practice*. In Portugal, the position of workers with disabilities or chronic and oncological diseases is protected not only by national legislation, but also by international and European legislation that is part of the local legal system. The authors Neto et al. (2024) focused on whether the legal regulations in this system are sufficient, whether these rights are known and used by people with disabilities, and whether employers actually recognize and respect them.

This survey was conducted in 2022, and the authors used a mixed data collection method. The authors first collected data through a questionnaire among people with disabilities and then conducted interviews, which allowed for a more detailed examination of their subjective experiences. Such a combination allowed for a more comprehensive view of the research issue.

For the purpose of the quantitative questionnaire survey, distributed using the Google Forms platform, a sample of 195 respondents aged 21 to 78 who identified themselves as people with a disability or chronic illness was approached. The majority were women, many had a university degree, and all reported having previous work experience. The authors used IBM SPSS statistical software to process and therefore analyze the obtained data. The authors mainly used descriptive analysis and, where necessary, the chi - square test to verify the relationships between variables.

The second, qualitative part of the research was conducted in the form of semi-structured interviews with 8 people with disabilities, who were selected from among the participants of the previous questionnaire survey. The aim was to gain a deeper insight into their experiences and attitudes towards reasonable accommodation. The interviews also took place in 2022, mostly in person, except for one that took place online. They lasted approximately an hour and, with the consent of the respondents, were recorded and subsequently transcribed. All participants had either congenital or acquired disabilities. The sample consisted of four men and four women aged between 33 and 72, with the majority having a university degree.

The research results show that people with disabilities perceive legal reasonable accommodation as an important tool that can positively influence their inclusion in the working environment. Although respondents also identified measures related to the organization of work as useful, such as adjusting working hours or more time off, these are less often implemented in practice. Employers prefer adjustments that are directly related to the performance of work, such as providing special equipment. The research also revealed several barriers that prevent the real exercise of the right to reasonable accommodation, in particular employees' concerns about negative reactions from colleagues or superiors if they request these adjustments.

RESEARCH STUDY 2 - EMPLOYMENT OF PEOPLE WITH DISABILITIES IN SMEs (POLAND)

The work of Michna et al. (2017) *focuses on the employment of people with disabilities in small and medium-sized enterprises in Poland* . The authors guided their analysis with a general research question: How can the chances of people with disabilities obtaining a job in small and medium-sized enterprises (SMEs) be improved, taking into account their work preferences and expectations, as well as the expectations of the employers themselves. The aim of the study was to identify the needs, ideas and requirements of both groups in relation to employment and, on this basis, to propose solutions that could support higher work integration of this disadvantaged group in SMEs.

To achieve this goal, the authors conducted a multi-stage research study that combined quantitative and qualitative approaches. The quantitative part was conducted on a large sample of 1,041 unemployed people with severe or severe disabilities and on a set of 150 small and medium-sized enterprises from various sectors. In both cases, structured questionnaires were used, which were completed in cooperation with trained interviewers. These workers helped the respondents with the completion and, if necessary, explained the questions in more detail. This qualitative survey was conducted in 2007, focusing on identifying barriers, experiences and needs of this group in the work process.

The qualitative phase then included case studies in three SMEs that have been actively employing disabled workers for a long time. This phase used structured interviews with questionnaires, with the respondents being top managers of the selected SMEs. This survey was carried out in 2012, and during this period a new structured questionnaire was also developed for employees of these enterprises that actively support and implement the employment of disabled people.

To process the data obtained, the authors applied a sequential explanatory strategy, in which they first analyzed quantitative data and then used qualitative findings to explain and supplement them in more detail. The combination of both approaches provided them with a more comprehensive and accurate view of the research issue (Michna et al., 2017).

Results

This multi-stage research study shows the following results: SMEs still lack more precise information about the possibilities of employing people with disabilities, which

makes it difficult for them to take the necessary measures in practice. Nevertheless, case studies have shown that many managers perceive disabled employees positively and appreciate their work commitment and loyalty. Unemployed people with disabilities themselves confirmed that they prefer administrative and office jobs and expect support from employers, mainly in the form of an adapted workplace, subsidized transport and further education opportunities. IT courses were identified as the most desirable, which is also in line with the needs of SMEs. The results show that a significant proportion of disabled people would prefer part-time work, which is already provided by many companies. Overall, this study shows that with better information, targeted support, and adaptation of working conditions, the expectations of both parties can be significantly aligned, which increases the chances of successful employment integration of this group.

RESEARCH STUDY 3 - SUPPORTING YOUNG PEOPLE WITH DISABILITIES DURING THE TRANSITION FROM SCHOOL TO EMPLOYMENT (CANADA)

Another research analyzed focused on *the role of job accommodations and benefits in supporting young Canadian adults with disabilities during their transition from school to work*. The authors Jetha et al. (2019) aimed to achieve the following objectives with this study: To describe what specific job accommodations and benefits young people with disabilities need most and whether they prefer physical (referred to in the study as "hard") workplace accommodations, organizational ("soft") accommodations, or health benefits. To identify barriers that prevent these young people from accessing these accommodations or benefits, and to examine the relationship between the type of disability and the need for accommodations.

Data collection was carried out in the form of an online survey, the target group of which was young people with disabilities aged 18 to 35. These were respondents who were still studying, employed or actively looking for work. The questionnaire was completed by 155 respondents, whose average age was 25.8 years. The majority were women and a large part of the participants were still students at the time of the survey. More than half were also employed, mainly part-time. The most frequently reported types of disability included physical, mental and learning disabilities, with most respondents having more than one limitation.

Chi-square tests were used to process the data obtained. The analysis was carried out in the statistical software SAS 9.3. However, there is no clear indication of the year in which the responses were collected in this study.

Results

Research has shown that young adults with disabilities most often need extended health insurance and so-called soft work arrangements (e.g. flexible working hours or ongoing support in the workplace). However, providing these adjustments can be more challenging in some job sectors. The findings also showed that people with mental disabilities need these forms of support even more often. Respondents also reported several barriers to assessing adjustments and benefits. These included concerns about disclosing their disability, which clearly makes it more difficult for them to access the benefits they need. The authors therefore point to the need for better communication and a more proactive approach from employers (Jetha et al., 2019).

RESEARCH STUDY 4 - SURVEY OF PERCEPTIONS OF FUTURE LABOUR MARKET APPLICATION AMONG YOUNG ADULTS WITH DISABILITIES (CANADA)

The fourth research study naturally follows on from previous research, as the authors Jetha et al. (2020) decided to examine how *young adults with disabilities perceive their participation in the future labor market* . They proceeded from the fact that the world of work is changing rapidly, which may mean not only new opportunities but also significant barriers for this group. The authors therefore focused on how young people with disabilities assess their possibilities to participate in working life in rapidly changing conditions.

This study included young Canadian adults with disabilities, aged 18 to 36, who were approached after giving consent based on their participation in previous research by the same author team. The characteristics of the respondents were intentionally diverse to ensure the broadest possible view of the research topic. A total of 22 individual interviews were conducted. Data collection took place in the form of semi-structured telephone interviews, which allowed participants to freely describe their work experiences and perceptions of the future of work. The interviews took place from February 2020, were recorded, anonymized, and then transcribed verbatim.

Thematic analysis was used to process the data, in which researchers looked for recurring motifs and meanings in the participants' responses. Interview transcripts were coded by multiple team members to ensure greater accuracy and reliability of the analysis. NVivo software was used to organize and process the data.

Results

The study showed that young people with disabilities perceive their future employment mainly through their own health limitations, rather than through broader changes in the labor market. Digital technologies were identified as an aspect that plays a significant role in the future of the labor market. However, respondents to this research perceive them differently, with people with stable jobs seeing them as an opportunity, while those in precarious conditions are more likely to fear them. The authors point out that many of them have limited opportunities to develop their technical skills, which may further disadvantage them in the future. This again suggests the need for better support and education that takes into account not only the needs of this disadvantaged group, but also the rapid changes in the labor market (Jetha et al., 2020).

RESEARCH STUDY 5 - DIGITAL TRANSFORMATION AND ITS IMPACT ON THE EMPLOYMENT OF PEOPLE WITH DISABILITIES (CANADA)

The topic of the fifth research study is also closely related to previous findings, as it is again researched by the same team of authors. This time, Jetha et al. (2023) focused on how *the rapid development of digital technologies in the workplace is changing the employment conditions of people with disabilities* . The study seeks to clarify how digital transformation brings new challenges, but also opportunities for their long-term application in the labor market.

This time, however, the survey respondents were not people with disabilities themselves, but experts on the future of work, policymakers and employment service providers for this group. Data collection took place in the form of individual semi-structured interviews, in which participants were asked for their views on the impact of the rapid development of digital technologies on the working conditions and employment of people with disabilities. At the same time, they were asked to identify strategies that could support inclusive employment in a digitalized work environment.

Forty respondents from across Canada were interviewed, with 60-minute interviews conducted over the phone. Responses were collected from January to April 2021. A grounded theory approach was used to process the data, allowing the authors to develop concepts based on interviews with experts. The interviews were then coded and analyzed using NVivo software.

Results

The interviews showed that the digital transformation of the economy is perceived as a rapid process in which digital technologies become a common part of the working environment. Experts agreed that these changes also significantly affect the working conditions of people with disabilities, both positively and negatively. They pointed out that this is a group that already faces the so-called digital divide, i.e. inequalities in access to digital technologies, resources and necessary skills. Since people with disabilities often work in less qualified positions, they may be most at risk from technological advances. However, experts emphasized that properly set up digital solutions can contribute to greater job availability, flexibility and overall facilitation of work performance (Jetha et al., 2023).

RESEARCH STUDY 6 - WORK EXPERIENCES OF EMPLOYEES WITH DISABILITIES IN POST-SOVIET SOCIETY (RUSSIA)

The sixth research study focuses on *the current work experiences of people with disabilities in the post-Soviet environment,* which has so far been little explored in professional literature. The authors Lolat-Pazarauskiene et al. (2025) point out that most of the research to date comes from Western countries, while the cultural and social conditions of the former Soviet states remain out of focus. The author team also included a person who had direct contact with the researched environment and issues, as she comes from Lithuania and herself lives with a visible physical disability. Her personal experience with this environment provided the study with a deeper and more authentic perspective on the reality of everyday working life of people with disabilities in this region.

Data was collected through individual interviews conducted, recorded and subsequently analyzed by a researcher with personal experience in the subject. The interviews were conducted in 2022 and 2023, with respondents being people with visible physical disabilities working full-time in Lithuania. The survey involved 45 respondents, with each interview lasting approximately 40 to 100 minutes. A grounded theory approach was used to process the data, with the analysis supported by MAXQDA 2022 software.

Results

The results of this research study showed that, despite the existing legislation, precarious and unsatisfactory working conditions persist for people with disabilities in Lithuania. Several respondents described general feelings of helplessness due to their limited mobility. Some even stated that their disability was used to the advantage of employers, for example by hiring more disabled employees, but at lower wages, which indicated their bad intentions. It also turned out that these negative experiences are interconnected. Lack of accessibility, prejudice and unstable working conditions reinforce each other. The research thus suggests that the existing system in this society still fails to ensure fair conditions and inclusion in practice (Lolat-Pazarauskiene et al., 2025).

RESEARCH STUDY 7 - PARTICIPATION OF EMPLOYEES WITH DISABILITIES IN THE LABOUR MARKET: AN INTER-ORGANISATIONAL EVALUATION (INDIA)

The research study examines *the status of inclusion of employees with disabilities in workplaces in India.* The authors Ghosh et al. (2024) analyze how individual organizations ensure inclusion and adaptation of the work environment for these employees through the use of personnel practices. With the study, the authors try to bring a new perspective on the employment of people with disabilities in a developing country, since most of the research to date has focused mainly on organizations in Western countries.

The research involved HR professionals or heads of inclusion and diversity from organizations in India who were involved in implementing policies for people with disabilities. 16 organizations participated in the study, each represented by one respondent. These organizations included Indian startups, foreign multinationals operating in India, and Indian multinationals, which allowed for comparisons. In addition, 8 employees with disabilities working in these organizations also participated in the research. Data was collected through semi-structured online interviews via Skype over a four-month period in early 2018.

The interviews were recorded with the consent of the respondents and subsequently transcribed. The authors analyzed these transcripts, identified main themes, and compared the responses of the respondents across organizations. Based on this analysis, the data obtained were divided into thematic categories, which allowed for a better interpretation of the research results.

Results

The research results show that there are several common elements in the area of human resource management in supporting the inclusion of employees with disabilities among the organizations studied. These organizations emphasized their strong commitment to inclusion and emphasized that when hiring and advancing employees, their abilities, knowledge and experience are the main determinants, not their disability. At the same time, it turned out that the successful implementation of inclusive measures is conditional in the involvement of employees at different levels of the organization. Several tools were used in individual organizations to support inclusion, such as adapting job positions to employees' abilities, cooperating with non-profit organizations in recruiting candidates with disabilities, conducting workshops aimed at raising awareness about the inclusion of this group, or creating support employee groups.

However, the research also revealed certain differences between individual types of organizations. In larger multinational companies, the initiative in the field of inclusion of people with disabilities is more often formalized and is part of broader organizational policies. In the case of startups, this issue is more informal in nature and results from an open organizational culture. Differences therefore understandably also appeared in the methods of recruiting employees with disabilities, adaptation processes or supporting their professional development (Ghosh et al., 2024).

RESEARCH STUDY 8 - SURVEY ON INCOME EARNING OPPORTUNITIES OF PEOPLE WITH DISABILITIES BASED ON SKILLS FROM VOCATIONAL EDUCATION (CHINA)

The eighth research study examined *the impact of vocational training programs for people with disabilities on their earnings in mainland China*. Li et al. (2024) point out that skills development and vocational training for people with disabilities are key tools for improving their labor market outcomes. However, they also point out that there are currently only a limited number of studies that examine the effects of these training programs for people with disabilities in China. The authors attempt to address this research gap by evaluating China's government-subsidized vocational training program. The study addresses two main research questions: to what extent do vocational training programs contribute to income generation for people with disabilities and what factors influence the ability to generate income after completing these programs.

The data were collected through an online survey involving 11,296 respondents from 31 provincial administrative regions in China. Data collection took place between June and October 2018. Methods such as logistic regression analysis, principal component analysis, and chi - square test were used to process the data.

Results

The results of the study show that the most significant factor influencing the ability of people with disabilities to earn an income after completing vocational training is the correspondence between the content of the completed training and their current employment. Other factors also increase the effectiveness of the programs, such as the provision of practice and accommodation, longer course duration, barrier-free environment, and participant satisfaction with the training content. The motivation of participants and their active involvement in the educational process also play an important role. The findings also suggest that some socio-economic characteristics, such as older age, higher education, or male gender, may have a positive impact on the income of training participants, while the type or degree of disability was not shown to be a significant factor. The study also highlights the importance of cooperation between educational institutions, employers, and the public sector in linking vocational training with practical work experience (Li et al., 2024).

RESEARCH STUDY 9 - PERSONS WITH DISABILITIES IN THE LABOR MARKET OF THE CITY OF SPLIT (CROATIA)

The study focuses on the employment of people with disabilities in the Croatian city of Split. The research deals with *the implementation of the Law on Vocational Rehabilitation and Employment* of People with Disabilities and also examines the opinions and attitudes of these people towards the problems they encounter in employment, as well as the shortcomings of the aforementioned law (Relja et al., 2018).

Data collection was carried out through a questionnaire survey in 2015. The sample of 49 respondents consisted of people in the age group from 20 to 61. The authors used mainly descriptive statistical analysis when processing the data, evaluating the respondents' answers using percentages and formulating conclusions based on the results obtained.

Results

The research results show that people with disabilities (PWSs) continue to face several obstacles in the labor market. The most significant include insufficient awareness of employers about their problems, persistent stereotypes about their work performance, lack of qualifications, architectural barriers, and limited job opportunities. The research also showed that many respondents were not familiar with the new Act on Vocational Rehabilitation and Employment of PWDs and, according to them, its adoption did not significantly contribute to improving their employability. Respondents also pointed out the need for greater involvement of PWDs in public decision-making processes and proposed several measures to improve their situation, such as supporting social activities, improving communication with employers, providing professional support, or increasing financial assistance. The research results also emphasize the importance of supporting the employment of people with disabilities, which can contribute to changing society's attitudes and improving their quality of life, as this depends not only on healthcare, but also on the possibility of fully participating in working and social life (Relja et al., 2018).

RESEARCH STUDY 10 - WORKFORCE CHALLENGES FOR PEOPLE WITH DISABILITIES IN HUNGARY AND SLOVAKIA DURING THE COVID-19 PANDEMIC (HUNGARY, SLOVAKIA)

The latest study examines *the development of the situation of people with disabilities in Hungary and Slovakia.* It aims to assess whether the state social network and existing support mechanisms provide sufficient conditions to ensure the livelihood and adequate standard of living of people with reduced working capacity. It also points out that during the COVID-19 pandemic, many people with disabilities were pushed out of the open labour market and moved into sheltered employment, which was often reflected in a lower standard of living (Jenei et al., 2024).

The data in this survey were collected in a mixed method, with the authors using both quantitative and qualitative methods. In-depth interviews were conducted with 5 disabled employees in Slovakia and 9 disabled people in Hungary, as well as leaders of advocacy organizations. The interviews took place between 2021 and 2022. Data collection was also carried out through an empirical questionnaire survey, in which 380 respondents participated, of which 164 were from Slovakia and 216 from Hungary. The questionnaire responses were collected between July and October 2022. When processing the data, the authors used a qualitative analysis of in-depth interviews, which they supplemented with the use of word clouds to identify the most frequent themes and key concepts. The questionnaire

survey was subsequently also worked with a quantitative evaluation of the responses.

Results

The results of the interviews show that people with disabilities who lost their jobs in the open-labor market often had the opportunity to apply for jobs in the sheltered labour market. At the same time, it was shown that state support and legislation can have a positive impact on the employment of these people, but the open labour market still represents a challenging environment for them. Therefore, the importance of sheltered employment increased during the pandemic, as employers in this sector generally did not lay off their workers.

In Slovakia, the results indicate a greater emphasis on the sheltered employment system. Respondents consider this type of work environment to be safer and more stable, especially in times of crisis. They also emphasized the importance of community support and social services that help people with disabilities solve both work and everyday life problems.

In Hungary, research has found that there is a greater emphasis on the inclusion of people with disabilities in the open labour market. Organisations and various initiatives are trying to support their employment in mainstream work environments and enable them to work alongside the majority population. This approach may contribute to greater social acceptance, but it also creates several barriers to finding employment.

Research also highlights the importance of special education, family support and community organizations, which play an important role in integrating people with disabilities into working life. Respondents emphasized the need for real support in finding work and creating work opportunities that would allow them to lead independent lives (Jenei, et al., 2024).

5. COMPARISON AND SYNTHESIS OF THE OBTAINED KNOWLEDGE

This subsection will compare and synthesize the findings from the research studies analyzed above that addressed the issue of employment of people with disabilities (PWDs). Since individual studies come from different countries, they also reflect different social, economic, and legislative conditions.

The topic of legislative conditions was addressed not only by the Portuguese and Croatian studies, but also by the Lithuanian study and research focused on the challenges in the workforce for people with disabilities in Hungary and Slovakia. The need for state legislative support is perceived in most of these studies as an important factor in improving the employment of people with disabilities. First of all, it is therefore important that individual states set legislation and policies towards people with disabilities in a way that supports their integration into the labor market. At the same time, however, it is essential that these measures are actually applied in practice. Although laws and regulations exist in several countries, their implementation is often insufficient, and employers do not always follow them in practice. Legislation is therefore an important prerequisite for supporting the employment of people with disabilities, but its consistent application in practice remains a problem.

Several studies analyzed points to the importance of education, especially specialized or vocational education, which can help people with disabilities better prepare for specific job positions. Such education also increases their chances of finding employment in the labor market and can also contribute to their career growth or improved financial evaluation.

The most frequently highlighted factor in most of the studies analysed was the need for support from employers. This support should not only consist of adjusting the working environment, but also in the overall approach of employers and their active efforts to create an inclusive working environment. Employers can significantly contribute to reducing prejudice and stereotypes in the workplace. Several respondents in individual studies also stated that they felt apprehensive about openly admitting their disability or asking for the support and adjustments to which they are entitled by law. This fact shows that support from employers alone is not enough for the successful integration of people with disabilities into society. As the last study analysed also shows, support from family, community and civic organisations also plays a significant role, which can help individuals overcome barriers in the labour market, solve everyday problems and strengthen their social integration,

A more detailed overview of the results of the individual studies analyzed is provided in the following table, which summarizes basic information about the individual studies, such as authors, year of publication and implementation of the research, country of implementation of the survey, number of respondents, methods of data collection and processing used, as well as main findings. The data presented in the table is based on information that has been described in more detail in previous chapters.

6. CONCLUSION

The article dealt with the identification and characteristics of people with disabilities. After their more detailed characteristics, their categorization was defined through professional literature. We identified and analyzed foreign research studies on the selected group, and the findings confirmed that the integration of persons with disabilities requires a combination of appropriately set legal regulations, a more active approach of employers, better information about the issue, accessible education for these disadvantaged persons, but especially a change in social attitudes towards the elimination of prejudices on the part of the majority population.

Table 1 Overview of the results of the analysis of the research studies mentioned

Authors	Country and year of survey	Number of respondents	Collection methods used	Data processing methods used	Results obtained
Neto, J. Pino, PC Neca, P. Bento, S. (2024)	Portugal 2022	195	Questionnaire	IBM SPSS statistical software, descriptive analysis, chi -square test	Legally reasonable adjustments are assessed by PWDs as important for work integration. Measures ensuring the overall well-being of these people, such as adjustment of working hours and more leave, are not often implemented in practice. Employers prefer technical adjustments to the workplace (e.g. special equipment). Psychological barriers have also been identified in this issue in the form of fears of negative reactions from colleagues and superiors if they request reasonable adjustments.
		8	Semi-structured interviews		
Michna, A. Kmieciak, R. Burzynska--Ptaszek, K. (2017)	Poland 2007	1,041 Disabled	Structured questionnaires	Sequential explanatory strategy	PWDs prefer office jobs. They expect support from employers in the form of adapted workplaces, subsidized transportation, and opportunities for further education. IT courses are most in demand, both by employees and employers. PWDs prefer part-time work, which many companies already actively support. A combination of better information, targeted support, and adaptation of working conditions is needed for the successful work integration of PWDs.
		150 SMEs			
	Poland 2012	3 SMEs	Structured interviews with questionnaires		
Jetha, A. Bowring, J. Furrie, A. Smith, F. Breslin, CC. (2019)	Canada Year not listed	155	Online questionnaire	Descriptive statistics, analysis of variance, chi - square tests, statistical software SAS 9.3	Young adults with disabilities most often report the need for expanded health insurance and soft adjustments to working conditions (e.g. flexible working hours) in relation to this issue. People with mental disabilities need these adjustments even more often. Respondents reported that they are concerned about disclosing their disability. Better communication and a more active approach on the part of employers are needed to improve the current situation.
Jetha, A., Shamaee, Ali, Tompa, E., Smith, P. Bültmann, U. Bonaccio, S. Tucker, L., Norman, C. Banks, C., Gignac, M. (2023)	Canada 2020	22	Semi-structured interviews	Thematic analysis, NVivo software	Young people with disabilities perceive their future in terms of their own health limitations as well as changes in the labour market. Although digital technologies were identified as a key aspect of the future of work, respondents perceived them differently. For some, they represent an opportunity, for others a concern. The research again highlights the need for better support and education.
Jetha, A., Bonaccio, S. Shamaee, A. Banks, C. Bültmann, U. Smith, P., Tompa. E. Tucker, L., Norman, C. Gignac, M. (2023)	Canada 2021	40	Semi-structured interviews	Grounded theory approach, NVivo software	The digital transformation is significantly affecting the working conditions of people with disabilities, both positively and negatively. Based on interviews with experts, it was found that this group faces a digital divide, i.e. inequalities in access to digital technologies, necessary skills and resources. Since people with disabilities often work in positions that require low qualifications, they are most at risk.
Lolat-Pazarauskiene, A., Ward, A. (2025)	Lithuania 2022 -2023	45	Individual interviews	Grounded Theory Approach, MAXQDA 2022	The existing legislative system in post-socialist countries is insufficient, as it cannot really guarantee better conditions for PWDs in practice. In Lithuania, precarious and unsatisfactory working conditions persist. The employment of PWDs is often abused by employers for financial gain.
Ghosh, K. Liu, Y. Mishra, M. (2024)	India 2018	16	Semi-structured interviews	Qualitative content analysis of the obtained data, categorization of the obtained data into thematic groups	In Indian multinational companies, disability inclusion is more often formalized, often as part of broader organizational policies. In contrast, in the case of startups, disability inclusion activities tend to be more informal. The companies surveyed expressed a strong commitment to inclusion and stated that the successful implementation of inclusive measures is conditional on the involvement of employees at different levels of the organization.
		8 PWD			
Li, W. Ni, TR. Zhang, Y. Wang, D. Parrado, S. (2024)	China 2018	11,296	Online questionnaire	Logistic regression analysis, principal component analysis and chi -square test.	The most important factor influencing the ability of PWDs to earn an income after completing vocational training is the alignment between the content of the training and their current employment. The motivation of PWDs and their active involvement in the learning process have also been shown to be key aspects of the success of vocational training. Cooperation between stakeholders is essential when linking vocational training with practical work experience.

Relja, R. Popovic, T. Rakic, T. (2018)	Croatia 2015	49	Online questionnaire	Descriptive statistical analysis	In Split, Croatia, PWDs face several obstacles in the labor market. The most significant ones include insufficient awareness of employers about their problems, persistent stereotypes about their work performance, lack of qualifications, architectural barriers, and limited job opportunities. PWDs do not consider the Act on Vocational Rehabilitation and Employment to be significantly beneficial. PWDs emphasize the need for their involvement in public decision-making processes.
Jenei, S. Szalai, S.M. Leicht, F. Molnar, S. Varga, E. Poor, J. (2024)	Slovakia 2021-2022 Hungary	5	In-depth interviews	Qualitative analysis, word cloud method, quantitative evaluation of findings	State support and legislation can have a positive impact on the employment of PWDs. In Slovakia, the results indicate a greater emphasis on the sheltered employment system. Respondents consider this type of work environment to be safer and more stable, especially in times of crisis. In Hungary, on the other hand, there is a greater emphasis on the integration of PWDs into the open labour market. The survey results highlight that special education, family support and community organisations play an important role in the integration of PWDs into working life.
		164	Empirical questionnaire		
		9	In-depth interviews		
		216	Empirical questionnaire		

Source: own processing

Acknowledgement

The article was written as part of the solution of the grant task: VEGA 1/0112/25, APVV-25-0117, APVV-25-0085.

REFERENCES

[1] ORIEŠČIKOVÁ, H. 2014. ***Analýza zamestnanosti osôb s mentálnym postihnutím.*** Ružomberok : VERBUM-vydavateľstvo KU, 2014. ISBN 978-80-561-0141-4.

[2] SOLLÁR, T. et al. 2022. Depression and anxiety as predictors of quality of life after a stroke. ***Kontakt-Journal of Nursing and Social Sciences Related to Health and Illness***. 24, 2022, pp. 79-84.

[3] ŠUBOVÁ, N. 2023. Comparison of EU Countries Based on Social Policy Instruments to Mitigate Financial Vulnerability of Households. ***Politická ekonómie***. 71, 2023, pp. 23-45.

[4] HOLUBOVÁ, B. et al. 2024. Institutional constraints to social dialogue in work integration of persons with disabilities: Slovakia and Norway compared. *Employee* ***Relations: The International Journal***. 46, 2024, 3, pp. 532-549.

[5] HALÁSKOVÁ, R. 2018. Structure of General Government Expenditure on Social Protection in the EU Member States. ***Montenegrin Journal of Economics***. 14, 2018, 4, pp. 7-21.

[6] BENDÍKOVÁ, A. et al. 2018. Satisfaction with Life Scale analyses among healthy people, people with noncommunicable diseases and people with disabilities. ***Family medicine and primary care review***. 20, 2018, 3, pp. 210-213.

[7] MARCEKOVÁ, R. et al. 2021. Accessible Tourism - Current State In Slovakia. ***Entrepreneurship And Sustainability Issues***. 9, 2021, pp. 66-86.

[8] NETO, J. et al. 2024. Silenced Voices. Reasonable Accommodation at the Workplace for Disability and Illness: First Person Accounts. ***Revista Critica De Ciencias Sociais***. 134, 2024, pp. 3-28.

[9] MICHNA, A. et al. 2017. Job Preferences and Expectations of Disabled People and Small and Medium-Sized Enterprises in Poland: Implications for Disabled People's Professional Development. ***Human Resource Development Quarterly***. 28, 2017, 3, pp. 299-336.

[10] JETHA, A. et al. 2019. Supporting the Transition into Employment: A Study of Canadian Young Adults Living with Disabilities. ***Journal of Occupational Rehabilitation***. 29, 2019, pp. 140-149.

[11] JETHA, A. et al. 2020. The working disadvantaged: the role of age, job tenure and disability in precarious work. ***BMC Public Health***. 20(1), 2020, 1900.

[12] JETHA, A. et al. 2023. Divided in a digital economy: Understanding disability employment inequities stemming from the application of advanced workplace technologies. ***SSM - Qualitative Research in Health***. 3, 2023.

[13] LOLAT-PAZARAUSKIENE, A. et al. 2025. Workplace experiences of employees with chronic physical disability in post-soviet society: A new model of escape from precarious work. ***European Management Journal***. 2025.

[14] GHOSH, K. et al. 2024. Labor market participation for employees with disabilities: a cross-organizational review in India. ***Disability & Society***. 39(4), 2024, pp. 892-913.

[15] LI, W. et al. 2024. Can people with disabilities obtain income by using skills learned from vocational trainings? Evidence from mainland China. ***Higher Education Skills and Work-Based Learning***. 14, 2024, 2, pp. 386-408.

[16] RELJA, R. et al. 2018. Persons With Disabilities In The Labour Market Of The City Of Split: Reality And Perspectives. ***Economic and Social Development***. 2018, pp. 393-406.

[17] JENEI, S. et al. 2024. The workforce challenges of disabled people in Hungary and Slovakia during the COVID-19 pandemic. ***Alter-European Journal of Disability Research***. 18, 2024, 3.

Alžbeta KUCHARČÍKOVÁ, prof., Ing., PhD.
Ivana POMPUROVÁ, Bc.
University of Zilina, Faculty of Management Science and Informatics, Department of Macro and Microeconomics
Univerzitná 8215, 010 26 Zilina, Slovakia
e-mail: alzbeta.kucharcikova@uniza.sk

INSTRUCTIONS

Submissions should be written in English. The author is responsible for scientific accuracy, originality, and the formal appropriateness of the article. It is not allowed to submit article that was published in another journal. The editorial board has the right to refuse publication of the article.

The articles should be submitted electronically using MS Word and in doc (docx) format. The editorial board may, if necessary, formal edit received articles.

Article headline should be written in font size 14 bold capital letters and aligned to the left margin.

The author´s name should be written without titles or degrees and in font size 12 with a single space, size 11, between it and the text of article.

The text of the article should be divided into chapters. Titles of chapters must be numbered, written in bold type, and arranged from the left margin. It is necessary to follow the format described below:

- Arrangement into blocks
- Font style: Calibri
- Font size: 11
- Indent each new paragraph 5 spaces
- Spacing: single
- Do not include page numbers.

Charts and graphs must be numbered and the references must be in the text. The name of a table (Table 1) or a graph (Figure 1) should be written in font size 11 bold, aligned from the left margin. Pictures and graphs must be visible and clear even in a black and white version. The source from which the author obtained the material should be written under every chart and graph.

Formulas must be numbered. The number should be written in font size 11 in parentheses, aligned to the right margin and next to the formula.

Length of article: maximum length should be 6 pages of A4 format.

References to literature should be presented according to ISO 690. The list must contain only sources used in the text. References should be presented in the text in its respective place with an indication number in square parentheses. Footnotes are not allowed. The indicated number should be written in the end of the article in the references. Other information for the preparation of articles are given on the website of the journal (http://www.infoma.fri.uniza.sk/mse.php).

Author´s address: The author should present his/her contact information and co-authors´ as well below the list of references. It must consist of first name and surname (including titles and degrees), name of university, name of faculty, name of department (institute) and e-mail address.

Review. A double-blind peer review is arranged by the editorial board.

The title and abstract should be in English. Below the abstract there will be given key words in English and JEL Classification codes (see http://www.aeaweb.org/journal/jel_class_system.php).

Address of the Editorial Office

University of Žilina
Faculty of Management Science and Informatics
Department of Management Theories
Management: Science and Education ~ m:se
Univerzitná 8215/1, 010 26 Žilina, Slovakia
e-mail: mse.journal@fri.uniza.sk, michal.varmus@fri.uniza.sk, viliam.lendel@fri.uniza.sk

Subscription

Subscription orders must be sent to the editorial office. It is possible to order older issues only until present supplies are exhausted.

Information for Authors

Contributions in the journal have been reviewed but not edited. Journal is issued 2 times a year.

Circulation: 100 prints, **ISSN 1338-9777**, IČO 37 808 702

The Slovak Republic Ministry of Culture has approved publication of the Slovak Scientific Journal Management: Science and Education ~ m:se Reg. No.: EV 4822/13

Volume 15, Number 1, April 2026