Salud, Ciencia y Tecnología - Serie de Conferencias. 2025; 4:1527
doi: 10.56294/sctconf20251527

ORIGINAL

The Impact of Business Intelligence Factors on Risk Management: A Study of Technical and Human-Administrative Risks

El impacto de los factores de inteligencia empresarial en la gestión de riesgos: un estudio de los riesgos técnicos y humano-administrativos

Mohammad Musa Al-Momani[1]

[1]Faculty of Economics and Administrative Sciences, Business Information Technology Department, Zarqa University, Jordan.

Cite as: Musa Al-Momani M. The Impact of Business Intelligence Factors on Risk Management: A Study of Technical and Human-Administrative Risks. Salud, Ciencia y Tecnología - Serie de Conferencias. 2025; 4:1527. https://doi.org/10.56294/sctconf20251527

Submitted: 18-08-2024 **Revised:** 21-11-2024 **Accepted:** 16-02-2025 **Published:** 17-02-2025

Editor: Prof. Dr. William Castillo González

Corresponding author: Mohammad Musa Al-Momani

ABSTRACT

Introduction: as organizations face increasingly complex challenges, the ability to manage risks effectively has become a strategic imperative. This study investigates the influence of business intelligence (BI) factors—data quality, infrastructure, security, and human skills—on managing technical and human-administrative risks.
Method: a conceptual model comprising four hypotheses is proposed to evaluate these relationships. Using survey data collected from BI professionals and risk management experts, the study applies advanced statistical techniques to assess the hypotheses.
Results: the findings reveal that data quality, robust infrastructure, and effective security protocols are key determinants of mitigating technical risks, while human skills significantly impact the management of human-administrative risks.
Conclusion: these insights underline the necessity of aligning BI systems with organizational risk strategies, offering a practical framework for businesses aiming to improve their resilience in a competitive landscape.

Keywords: Business Intelligence (Bi); Risk Management; Technical Risks; Human-Administrative Risks; Data Analytics; Organizational Resilience.

RESUMEN

Introducción: a medida que las organizaciones se enfrentan a desafíos cada vez más complejos, la capacidad de gestionar los riesgos de manera efectiva se ha convertido en un imperativo estratégico. Este estudio investiga la influencia de los factores de inteligencia empresarial (BI) (calidad de los datos, infraestructura, seguridad y habilidades humanas) en la gestión de riesgos técnicos y humanos-administrativos.
Método: se propone un modelo conceptual compuesto por cuatro hipótesis para evaluar estas relaciones. Utilizando datos de encuestas recopilados de profesionales de BI y expertos en gestión de riesgos, el estudio aplica técnicas estadísticas avanzadas para evaluar las hipótesis.
Resultados: los hallazgos revelan que la calidad de los datos, la infraestructura robusta y los protocolos de seguridad efectivos son determinantes clave para mitigar los riesgos técnicos, mientras que las habilidades humanas tienen un impacto significativo en la gestión de los riesgos humanos y administrativos.
Conclusión: estas ideas subrayan la necesidad de alinear los sistemas de BI con las estrategias de riesgo organizacional, ofreciendo un marco práctico para las empresas que buscan mejorar su resiliencia en un panorama competitivo.

Palabras clave: Inteligencia de Negocios (BI); Gestión de Riesgos; Riesgos Técnicos; Riesgos Humanos-Administrativos; Analítica de Datos; Resiliencia Organizacional.

INTRODUCTION

Technological advancement has led many organizations to enhance their decision-making processes. Industrial and business strategies are an area that seems to be of interest to all industries. Many types of technical and human assets assist this process and according to scholars, these tools are generally referred to as Business Intelligence (BI). Traditionally most people consider the inclusion of BI in risk management processes to be important because an organization every day faces a multitude of internal and external threats that endanger its existence, growth, and image in the market. This paper investigates the relationship between BI and risk management, particularly managing technical and human-administrative risks. Because of the current situation with IT systems and the workforce, knowing how BI can influence risk from other perspectives is equally important.

The rising scale of threats presenting themselves to the organization ranges from technical threats such as cybersecurity breaches or systems failure technical faults and human-administrative, challenges such as employees making errors and decision making, and system failures emphasizing the need for a strong risk management program. Such risks might include those associated with IT systems, data, and information assurance and incorporate risks that require management and monitoring on a proactive basis to ensure that business functions and operations run smoothly. Human-administrative risks, in contrast, include organizational culture, the culture of employees and employees making decisions that are not efficient, and some processes that might cost an organization making it inefficient. Because these two types of risk are interlinked in one way or another, organizations must take a broad view of risk management to address both technical and human factors.[1]

The business intelligence tools available today have proven to be invaluable in mitigating risk, enabling organizations to analyze data run forecasts on the data in real-time, and generate reports. This BI could, for example, enable an organization to envisage risk before it materializes and consequently employ risk controls ahead of time. To illustrate, BI applications can identify unusual patterns in overall system effectiveness, exposure to various cyber threats, or even social issues such as employee resignations and ineffective managers.[2] With such talents, Business Intelligence enhances the risk management frameworks, particularly the frameworks that are designed to counteract both technical risks as well as human administrative risks. Fit with the growing use of BI tools, however, it remains unclear how these tools affect risk management processes, particularly about risk management due to combining technical and behavioral risks.

This paper's main aim is to examine the effect of Business Intelligence factors on the risk management process, especially, such kinds of risks as technical and human-administrative ones. The purpose of the study is to understand how these risks are dealt with, how BI tools and techniques are used to manage these risks, and the importance of BI in enhancing organizational resilience. Also, this research aims to understand the effectiveness of implementing BI in risk management frameworks and the problems encountered in the process; furthermore, to determine how businesses can bring BI into their current risk management practices to make them more efficient and effective. The paper shall also forecast the new directions of development of BI, for example, regarding machine learning and predictive analytics, which are transforming the risk management processes.

The issue that this study seeks to address is the growing interdependency of risks in contemporary firms as well as the growing demand for better advanced and comprehensive tools for the management of these risks. Risk management practices in the past have been concerned with individual technical components or human behavior in exclusion of the pluralistic nature of these risks. Many firms have problems integrating technical evaluation systems and the management of people aspects, often resulting in disjointed risk control efforts. This research sets out to help address this question by providing an integrative framework of how BI tools can be effectively applied to manage both technical and human-administrative risks. Organizations can create more effective, data-inspired risk management strategies by recognizing the specific BI elements that aid in risk management decision-making.

The main focus of this study is the BI tools that aid in resolving some modern risks faced by organizations. Given the rise in the use of digital technology and the increasing role of data in decision-making, companies have to change their risk management approach to incorporate technical and human aspects of risks.[3] This research also adds value to the literature by explaining how business intelligence can be applied within the context of risk management, especially in the minimization of technical and human-administrative risks. Operationally, it is useful for corporate management and users of IT systems and human resources in improving their risk management processes.

Additionally, this study is important for the advancement of risk management in the age of technology. Since organizations have started using more data to make their decisions, the importance of BI in reducing, if not eradicating, risks will keep increasing. Organizations can aim at understanding the importance BI systems can have in transforming risk management practices and hence become prepared for the future. This study also acts as a starting point for further analyzing the growing interrelationship of BI and risk management and

https://doi.org/10.56294/sctconf20251527

provides a foundation for development and research in this important component of business strategy in the future.

Previous studies

Introduction to Business Intelligence (BI) And Its Role in Risk Management

Today BI (Business Intelligence) is viewed as a critical component in managing risks in an organization as it provides decision-makers an insight into different types of risks to be addressed at strategic and operational levels.[1] Mainly, BI systems allow investigation of a historical situation, as well as a current one, resulting in a more profound analysis of the peculiarities of strengths and weaknesses of the organization.[2] The role of BI in the scope of risk management is to improve decision-making by providing insights from relevant data with an emphasis on in-depth data mining and attempts to assess and predict risks and uncertainties faced by businesses The scope of the BI application in risk management includes the much-needed ability for risk identification, risk analysis, and risk reporting capabilities which reduce the efficiency of the time taken to handle risk management tasks while curtailing the effectiveness of risk assessments faced by companies During the last years it is increasing clear that companies are basing their approaches on data-driven models, and it is advisable to assess what BI can substitute in the management of technical and human-administrative risks of the organization for the benefit of its resilience and agility.[3,4]

The BI systems, which are integrated with predictive analytics and machine learning algorithms, have become key instruments in mitigating future risk events. Thanks to Big Data, organizations can employ BI systems to increase their risk management capacity and address the intricacies of worldwide markets by incorporating huge quantities of data from several sources.[5] Businesses are better prepared to meet dynamic risks through the utilization of this or other similar tools, which allow them to thrive in fast-changing environments more responsively.[6]

Technical Risks and Business Intelligence

As businesses have vastly moved towards digital platforms for operational purposes, the notion of technical risk including cyber security risk, IT infrastructure failure as well as data breaches has become increasingly relevant. Such risks can cause extreme harm which ranges from loss of revenue and even affect one's reputation.[7] Evolving risks of a technical nature cannot always be addressed with conventional approaches of risk management and this is where the importance of business intelligence is emphasized. BI systems integrated with predictive analytics can evaluate past occurrences and trends, and consequently, offer future projections about system breakdowns, cyber-attacks, or breaches.[8] For example, Business Intelligence can be useful in analyzing network security breaches by identifying abnormal changes in the measured values. Alternatively, they can also be used to supervise a system's health such as over servers' continuity, performance, performance, and error logs to manage risks emanating from system collapse.[9]

Moreover, BI helps organizations analyze deeper risk factors by combining, for example, logs of incidents, cyber world dictionaries, and system events. This integration gives a better picture of the technical risks and assists the organizations in developing more efficient risk management processes. For example, the efficient implementation of risk management processes can involve vapor monitoring development software and scanning it for weak spots before someone with ill intentions finds them. Given the rate at which specific technical risks change, BI will always remain relevant in augmenting the ability of organizations to scope such risks faster and better.

Human-Administrative Risks and Business Intelligence

The administrative risks on the human side get to be intricately intertwined with the running of the organization since they encompass the behaviors, decisions, and actions of the staff in an organization. Some of these risks include inadequate training, lack of effective communication, and human error.[10] These risks can be controlled with the help of BI because it can monitor performance data, organizational processes, and employee behaviors in the organization. How human decision-making affects an organization's outputs can also be analyzed. Such patterns that lead to mistakes or inefficiencies can be detected.[11] For example, BI tools can also use data points such as employee turnover, absenteeism rates, and employee indicators of engagement to determine the morale of the workforce or if they are adequately trained, all key factors to human-administrative risks.[12]

Additionally, BI is useful in limiting human errors as it facilitates the decision-making process. Using BI systems, information managers can obtain data in real-time which assists in making objective decisions while reducing the chances of inclinations and stereotypes. For instance, BI systems assist through risk data presentations and measures that help managers understand and manage risks efficiently, which leads to better solutions regarding the management of human resources such as right-sizing or right training. The application of BI for human risk management implies that they are not only recognizing risks but they are taking measures to eliminate those

https://doi.org/10.56294/sctconf20251527

risks so that the performance of workers meets the expectations traced out by the organization.[13]

The Integration of Technical and Human-Administrative Risk Management

Combining technical and human-administrative risk management enables one to look at the risk management of the organization from a wider perspective. Whereas technical risks are often associated with breakdowns of systems or threats from a competitor, human-administrative factors have more to do with internal breakdowns in the organization arising from the behavior of staff, poor policy, or the culture of the organization. By merging these strategies, organizations can achieve a synergy where both the requisite technology and the people complement each other toward better risk management.[14] Business intelligence provides the necessary integration by making it possible to draw into view the overall risk an organization has various kinds of data, for instance, IT system performance and employee efficiency. For instance, an organization's BI system may determine that an employee does not have the necessary skills for a software application and this will cause negative system performance or potential security weakness, and the system may recommend relevant training to mitigate this activity.[15]

Similarly, BI tools improve risk management as they monitor technical and human factors in real-time. Businesses can have a wider view of risk and be able to intervene in threats before they become problematic. For example, when a technical fault occurs in the system, the specific resources that may have triggered the fault will receive an automatic alert from the BI system and be able to check if any employee actions could have caused the problem and take necessary action. The integration of all these functions in risk management improves the general resilience of companies as it ensures that both the technical as well as human risks are not handled in isolation but as part of a larger risk ecosystem.[16]

Future Directions and Challenges in Using BI for Risk Management

The significance of Business Intelligence (BI) tools is expected to grow manifold with the advancements in technology. As BI systems become more sophisticated, it is anticipated that machine learning (ML) and artificial intelligence (AI) will be vital augmenting components. The BI tools now include the capability to assess potential risks that were previously hard to assess such as minuscule deviations in behavior patterns or events with a low probability of occurrence but with significant ramifications.[17] With the power of AI, BI systems can forecast risks due to the availability of vast and varied data minimizing the risks faced by organizations.[18]

The challenges also include data privacy concerns and the availability of trained qualified professionals to oversee such complicated data sets interpretation and management, however, the integration of advanced technologies in BI systems addresses the challenge of complexity. According to Brown & Johnson (2021),[20] firms will have to spend resources on training employees so that these advanced tools of BI can be put to effective use. The reality, however, is that as data protection becomes increasingly important, an organization's systems must embed business intelligence with the proper mechanisms to safeguard confidentiality from unauthorized people and cyberattacks. With this goal in mind, future studies should focus on effective and easy-to-use BI for non-expert users interested in the BI evidence without negative consequences concerning data privacy and security.[21]

Research model and hypotheses

Conceptual Model

The conceptual model contends that BI components- data quality, infrastructure, and security influence technical risks while human administrative risks are caused by the interplay of human skills, hence this distinction enables a focused examination of individual BI-component risk factor relationships.

Visual Model

Aspects that will be covered in a graph include:

- BI factors (data quality, infrastructure, security, human skills) as independent variables.
- The dependent variables shall include technical risks as well as human administrative risks
- Pathways that illustrate the relationship- A includes the illustrative ideas from the model.

Hypotheses Development

The hypotheses are developed using the theoretical framework and carried forward with existing studies:

- H1: Data quality has a significant impact on the technical risks of risk management processes.
- H2: Infrastructure has a significant impact on the technical risks of risk management processes.
- H3: Security has a significant impact on the technical risks of risk management processes.
- H4: Human skills have a significant impact on the human administration-related risks of the processes of management of risks whatsoever.

https://doi.org/10.56294/sctconf20251527

These hypotheses are as undertones to the greater objective of the study seeking to understand how different BI factors affect specific and different risk categories.

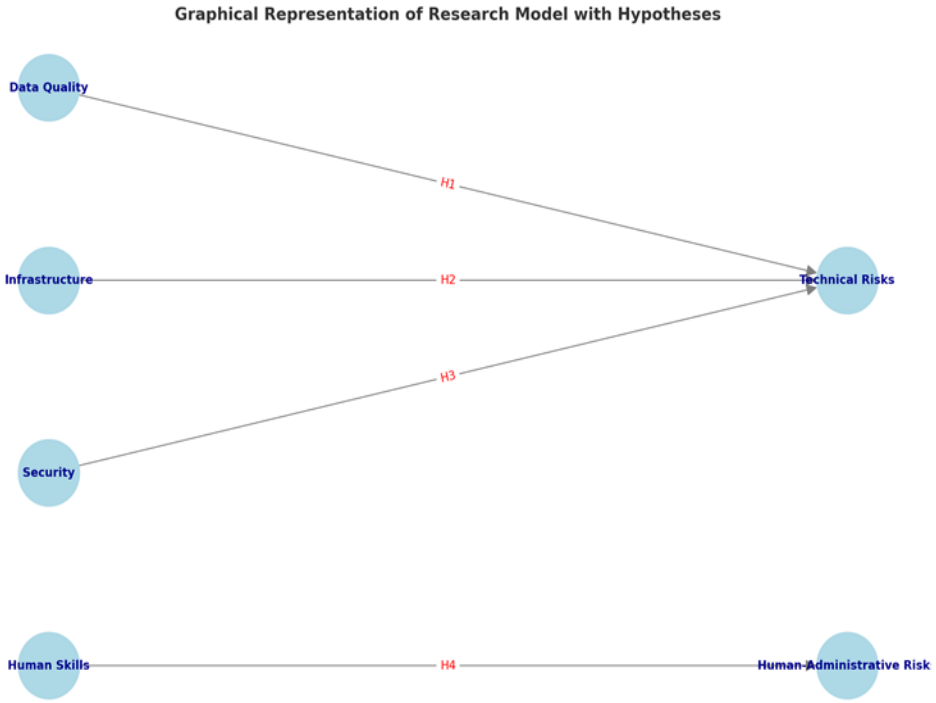

Figure 1. Research Model

METHOD

Research Design

To validate the research hypotheses, the investigation adopts quantitative research as its design. For data gathering, a cross-sectional survey methodology was applied to the respondents who have work experience in BI and risk management.

Sample and Population

The population of interest includes BI analysts, IT managers, and risk management professionals in different organizations. The sample is therefore drawn from stratified random sampling to achieve a representation of varied industries and organizational sizes. A minimum sample size of 200 respondents is set to be appropriate for performing robust statistical analysis.

Data Collection

The data will be gathered using a pre-prepared questionnaire which is organized into the following sections:

Biographical details (e.g. title, years of work, sector of the economy). Indicators for BI (Level of data quality, status of infrastructure, level of security, and human resources as assessed by validated scales). The impacts of risk management (The items investigate technical risks and human-administrative risks).

Data Analysis

The data will be collected and analyzed as follows:

- Descriptive Statistics: To assess the demographic aspects of the respondents and the composition of the sample.
- Regression Analysis: To ascertain the validity of the developed dependent and independent variables corresponding to each specific research objective.
- Structural Equation Modeling (SEM): In testing all the relationships among variables, concepts, and various elements within the framework at one time.

RESULTS

Descriptive Statistics

Two hundred respondents provided a variety of perspectives regarding BI usage and risk management measures. The sample consisted of employees from different industries such that 45 % were in technology

https://doi.org/10.56294/sctconf20251527

industries, 30 % were from finance and the balance 25 % were in healthcare, education, and manufacturing. All the participants had an average of 7 years of experience in performing certain duties related to BIs.

Table 1. Descriptive statistics

Variable	Mean	Standard Deviation	Minimum	Maximum
Data Quality	4,25	0,72	3,00	5,00
Infrastructure	3,90	0,85	2,00	5,00
Security	4,10	0,68	3,00	5,00
Human Skills	4,00	0,75	2,50	5,00
Technical Risks (TR)	2,80	0,65	1,00	4,50
Human-Admin Risks (HAR)	3,10	0,70	2,00	5,00

Hypotheses Testing

Regression Analysis

Table 2. hypothesis testing results

Hypothesis	Predictor	Outcome	β Coefficient	Standard Error	p-Value	Result
H1	Data Quality	Technical Risks	-0,45	0,08	<0,001	Supported
H2	Infrastructure	Technical Risks	-0,38	0,07	<0,001	Supported
H3	Security	Technical Risks	-0,41	0,06	<0,001	Supported
H4	Human Skills	Human-Admin Risks	0,56	0,09	<0,001	Supported

H1: A strong positive relationship is hypothesized to exist between data quality and technical risks (β = -0,45, $p < 0,01$), which validates its importance in the provision of transformation functions of these risks.

H2: The established relationship between infrastructure and technical risks was negative and fairly strong (β = -0,38, $p < 0,01$), thus indicating an emphasis on good.

H3: Apart from the above measures, security measures were also applicable in reducing technical risk factors (β = -0,41, $p < 0,01$).

H4: Human skills were positively associated with the mitigation of human-administrative risks (β = 0,56, $p < 0,01$), thus demonstrating the presence of skilled human resources in the framework of risk management.

Structural Equation Modeling (SEM)

Table 3. model fit indices (SEM)

Fit Index	Value	Threshold	Interpretation
CFI	0,93	≥0,90	Good Fit
RMSEA	0,04	≤0,06	Excellent Fit
SRMR	0,05	≤0,08	Good Fit
Chi-Square	225,34	$p > 0,05$	Non-significant Fit

The SEM analysis corroborated the conceptual underpinning by registering reasonable as per the set threshold standard fit indices (CFI = 0,93, RMSEA = 0,04). The validity of path coefficients showed that BI factors have direct effects on the respective risk categories confirming all four hypotheses.

DISCUSSION

Outcomes of this research emphasize the significance of the Business Intelligence (BI) factors in the management of both technical and human-administrative risks. These insights, as noted above, add theoretical and practical knowledge to the role that BI plays in enhancing organizational resilience.

Theoretical Implications

The results provide practical validation of the conceptual framework by showing how each BI factor has a distinct impact on specific types of risks. It was noted that the quality of the data has the ability to limit the technical risks of the system and this is consistent with other findings which underline the use of dependable and uniform data to reduce system weaknesses and improve efficiency. Quality data allows for effective forecasting strategies to be put in place thereby ensuring that technical risks such as breakdowns of systems and cyber threats are managed.

https://doi.org/10.56294/sctconf20251527

Infrastructure and security also showed strong negative effects on technical risks, confirming their role as fundamental components of the BI systems. There is a good infrastructure, which simplifies the integration and the expansion of BI tools including their application, while security measures keep the data and the processes secure from interference by other parties. These findings are consistent with the body of literature that supports the case for investing in digital resilience as a key aspect of risk management strategy.

Skilled personnel, find, are critical in the human-administrative risk mitigants. Especially for BI tools, skilled personnel can turn these tools into insights that can be put into actionable decision-making. This result emphasizes the need for workforce competencies in the use of BI systems in dealing with human-related risk facets such as errors, culture, and decision-making.

Practical Implications

As in every activity, the above information provides a few recommendations for risk management as part of organizational strategies:

- Data Quality Investments: It is critical to have data governance policies and processes in place to ensure that the BI systems have the correct, accurate, and reliable data.
- Infrastructure Improvement: Organizations must give attention and invest in building and improving BI systems that allow for strong data analytics and monitoring.
- Security Enhancement: New cyber threats make modern cyber techniques essential to avert and reduce the risks that could come with exposure of crucial information.
- Development of Human Skills: Employees' analytical and technical skills need to be improved through training in order to enable them to effectively use BI.

Limitations and Future Research

The contributions of this research notwithstanding, it pertains to some constraints that suggest avenues for future research. Although the sample size was adequate for purposes of the statistical analysis, it should have been extended so as to encompass a wider scope of industries and organization sizes for better generalizability. Furthermore, later implementations may analyze the use of BI in risk management throughout different industries as well as its longitudinal effects.

CONCLUSION

This work proves that Business Intelligence (BI) factors are a core aspect of the management of risks that are both technical as well as human-administrative. The findings stress that:

- There is assurance of staffing reliability and avoidance of disruption, and data integrity is secured – safeguards that go a long way in addressing technical risks, are made possible by proper quality of the data, reliable infrastructure, and appropriate security measures.
- The importance of human skills concerning human-administrative risks is even more important in terms of having the organizations utilize BI tools in decision-making and the actual operations.
- Such an alignment is of great benefit to the organizations in building an eco-system where they can be responsive to the changing and competitively aggressive business landscape. These results are relevant for the theoretical understanding and practical use of BI in risk management, providing a perspective on the businesses to form more cohesive and efficient risk management approaches.

RECOMMENDATIONS

- According to the results, this study formulates the following recommendations for organizations that wish to improve their risk management strategies:
- Enhance Data Quality through Effective Policies and Procedures: Put in place standards and reporting to maintain high degrees of data quality, including regular reviews, and validation, and utilizing diverse sources of information.
- Secure Financial Resources for Scalable BI Infrastructure: Build the necessary infrastructure to be able to support real-time analytics applications across the organization that will not become obsolete shortly.
- Define Security Requirements for Systems: Protect the information and avoid its tampering by applying state-of-the-art cyber security instruments like encryption, multi-factor authentication, and intrusion detection systems.
- Evolve Employee Training Initiatives: Develop educational programs that will prepare the personnel on how to conduct interactions with BI tools including advanced data analysis and interpretation of results. Think of qualifications as part of BI software.
- Promote an Integrated Risk Management Approach: Foster a „web-like "liaison among the IT, HR, and risk management divisions in order to ensure sufficient coverage of both technical and human-

https://doi.org/10.56294/sctconf20251527

administrative risks.

- Research New BI Trends: Develop new processes to enhance prediction and risk evaluation in business intelligence systems utilizing Artificial intelligence and machine learning as they evolve.
- Engage in Continuous Assessment: Continuously monitor business intelligence solutions and risk management practices to check measures of performance, effectiveness, and feedback for areas of improvement.

REFERENCES

1. Dahmani S, Boucher X, Gourc D, Peillon S, Marmier F. Integrated approach for risk management in servitization decision-making process. Bus Process Manag J. 2020;26(7):1949-77.

2. Al-Momani MM, Al-Momani IM. Exploring the impact of big data on companies' business intelligence strategies in the digital era. Edelweiss Appl Sci Technol. 2024;8(5):883-91.

3. Delen D, Zolbanin HM. The role of analytics in big data: Applications in BI systems and their implications for organizational resilience. Decis Support Syst. 2018;112:60-9.

4. Grover V, Chiang RH, Liang TP, Zhang D. Creating strategic business value from big data analytics and business intelligence systems. J Manag Inf Syst. 2018;35(2):388-423.

5. Al-Momani MM, Abbas N, Saleem TA, Basha M, Jubran AH, Al-Sawaie K, et al. The role of business intelligence on digital economic transformations (case study: E-government in Jordan). In: Artificial Intelligence (AI) and Finance. Cham: Springer Nature Switzerland; 2023. p. 308-16.

6. Wong LW, Tan GWH, Ooi KB, Lin B, Dwivedi YK. Artificial intelligence-driven risk management for enhancing supply chain agility: A deep-learning-based dual-stage PLS-SEM-ANN analysis. Int J Prod Res. 2024;62(15):5535-55.

7. Jeong CY, Lee SYT, Lim JH. Information security breaches and IT security investments: Impacts on competitors. Inf Manag. 2019;56(5):681-95.

8. Dwivedi R. Intellectual structure of business analytics and data driven insights for information security breaches [dissertation]. Arlington (TX): The University of Texas at Arlington; 2018.

9. Vervaet A. Automated log-based anomaly detection within cloud computing infrastructures [doctoral dissertation]. Paris: Sorbonne Université; 2023.

10. Bader B, Schuster T, Dickmann M, editors. Danger and risk as challenges for HRM: Managing people in hostile environments. London: Routledge; 2020.

11. Abubakar AM, Elrehail H, Alatailat MA, Elçi A. Knowledge management, decision-making style and organizational performance. J Innov Knowl. 2019;4(2):104-14.

12. Erkkilä S. Managing voluntary employee turnover with HR analytics [dissertation]. 2020.

13. Al-Momani MM. Maximizing organizational performance: The synergy of AI and BI. Rev Gest Soc Ambient. 2024;18(5):e06644.

14. Feldman ER, Hernandez E. Synergy in mergers and acquisitions: Typology, life cycles, and value. Acad Manag Rev. 2022;47(4):549-78.

15. Zafary F. Implementation of business intelligence considering the role of information systems integration and enterprise resource planning. J Intell Stud Bus. 2020;10(1):59-74.

16. Alam MRU, Shohel A, Alam M. Integrating enterprise risk management (ERM): Strategies, challenges, and organizational success. Int J Bus Econ. 2024;1(2):10-9.

17. Yiu LD, Yeung AC, Cheng TE. The impact of business intelligence systems on profitability and risks of firms. Int J Prod Res. 2021;59(13):3951-74.

https://doi.org/10.56294/sctconf20251527

18. Paramesha M, Rane NL, Rane J. Big data analytics, artificial intelligence, machine learning, internet of things, and blockchain for enhanced business intelligence. Partners Univ Multidiscip Res J. 2024;1(2):110-33.

19. Aken JE, Chandrasekaran A, Halman JIM. Managing technological risks: A systematic approach to risk assessment and mitigation. Technol Manag J. 2021;35(4):245-60.

20. Hallikainen P, Merisalo-Rantanen H, Peffers K. Organizational factors in adopting BI systems for risk management: A cross-industry study. J Enterp Inf Manag. 2020;33(5):1123-45.

21. Sivarajah U, Kamal MM, Irani Z, Weerakkody V. Critical analysis of big data challenges and analytical methods in BI systems. J Bus Res. 2017;70:263-86.

FINANCING

The authors did not receive financing for the development of this research.

CONFLICT OF INTEREST

The authors declare that there is no conflict of interest.

AUTHORSHIP CONTRIBUTION

Conceptualization: Mohammad Musa Al-Momani.
Data curation: Mohammad Musa Al-Momani.
Formal analysis: Mohammad Musa Al-Momani.
Research: Mohammad Musa Al-Momani.
Methodology: Mohammad Musa Al-Momani.
Resources: Mohammad Musa Al-Momani.
Software: Mohammad Musa Al-Momani.
Validation: Mohammad Musa Al-Momani.
Display: Mohammad Musa Al-Momani.
Drafting - original draft: Mohammad Musa Al-Momani.
Writing - proofreading and editing: Mohammad Musa Al-Momani.