

Article

Methodology for Quantitative Risk Assessment in the Integration and Use of ERP Systems in Enterprises

Kiril Luchkov ^{1,*}  and Nadya Velinova-Sokolova ² ¹ Faculty of Management, Technical University of Sofia, 1000 Sofia, Bulgaria² Faculty of Economics and Business Administration, Sofia University “St. Kliment Ohridski”, 1113 Sofia, Bulgaria; nadya.sokolova@feb.uni-sofia.bg

* Correspondence: kiril.luchkov@tu-sofia.bg

Abstract

ERP systems significantly optimize many business processes and activities, but often their implementation and use in companies is a risky endeavor. They are the subject of various scientific studies and analyses in the fields of business, accounting and finance. The main focus in them falls on the process of implementing these systems, while the subsequent stages, risk analysis and long-term strategy are less affected. On this basis, this research paper proposes a methodology for quantitative assessment of identified ERP risks. It is based on a five-level matrix measuring three risk factors—influence, impact and vulnerability. The methodology has been empirically tested in three companies, different in size and operating in different economic sectors. The results show that the level of risk depends not only on the scale and complexity of the business, but also on the degree of integration of ERP solutions. Periodic application of the risk assessment methodology helps identify problem areas and facilitates management decision-making.

Keywords: ERP systems; risk assessment; business processes

1. Introduction

In recent years, ERP (Enterprise Resource Planning) solutions have established themselves as a systematic approach to optimizing processes and activities in a number of enterprises, providing them with strategic support in making management decisions. The widespread use of ERP systems in various industries and sectors has led to many challenges related to information security, functionality, operational sustainability, etc. However, these challenges also give rise to specific risks related to their integration, operation and maintenance. Studies in practice show that it is not always possible to fully synchronize ERP solutions with the IT architecture of the business. And this is actually a prerequisite for the emergence of organizational, operational, technical and other similar risks.

The accelerated digital transformation, the dependence on integrated technological solutions, and the increasing complexity of business emphasize the relevance of the researched issues. In the context of information security, ERP systems are becoming a universal mechanism for managing numerous activities, some of which are risky. In addition to management obstacles, many companies also experience technical problems arising from the mismatch between the software configuration and existing business processes and practices. Systemic errors in ERP platforms are often the result of a lack of commitment on the part of the staff, their insufficient qualifications and difficulties in mastering new



Academic Editors: Lawrence
Murphy Smith and Dimitrios
Koutmos

Received: 31 January 2026

Revised: 11 March 2026

Accepted: 13 March 2026

Published: 18 March 2026

Copyright: © 2026 by the authors.

Licensee MDPI, Basel, Switzerland.

This article is an open access article
distributed under the terms and
conditions of the [Creative Commons](https://creativecommons.org/licenses/by/4.0/)

[Attribution \(CC BY\)](https://creativecommons.org/licenses/by/4.0/) license.

functionalities. Therefore, the identification, assessment and management of risk factors is essential for the effective functioning and competitiveness of companies.

Business management systems are entering a new stage, as artificial intelligence (AI) began increasingly entering in 2026. ERP solutions will transform into Intelligent ERP—intelligent platforms powered by artificial intelligence that do not just serve the business but actively develop it. They will use machine learning (ML), neural networks (NN AI), deep learning (DL), natural language processing and robotics. Therefore, the development of the new technology is also driven by the growing need to reduce business operating costs by maintaining employee workflows, thus increasing the efficiency of the organization as a whole. The development of artificial intelligence is, in other words, a development that ERP developers, integrators and implementers must follow if they want to remain effective and competitive in the market. The implementation of modern ERP systems, on the other hand, is exposed to new levels of risk related to the integrity and security of the data used by machine learning algorithms, where some models can lead to erroneous automated decisions. At the same time, regulatory pressure for ESG reporting requires companies to ensure full transparency and traceability throughout the value chain, which creates a significant risk of sanctions in the absence of reliable integration. Last but not least, the rapid penetration of Generative AI into the corporate environment raises serious questions for management regarding the protection of intellectual property and cybersecurity of cloud ERP structures.

The risks inherent in the ERP environment are often underestimated by management, although this can significantly hinder the effectiveness of certain departments and structures. Underestimating these risks in the long term reflects not only on individual processes and activities in enterprises, but also on management decisions and the competitiveness of the business. Therefore, it is important that potential risks associated with ERP systems are promptly identified, assessed, prioritized and managed as far as possible.

In the analysis of the scientific literature on ERP systems, despite the abundance of research, there are still significant gaps, especially in terms of new technologies, risk assessment and real-world application after the system implementation process. The main focus in many publications falls on the implementation process, while the subsequent stages, risk analysis and long-term strategy are less affected. It is necessary to shift the focus from “how to implement ERP¹” to “how to manage, optimize, analyze risk and develop ERP based on modern information technologies”. In this regard, the purpose of this study is to propose a universal methodology for risk assessment in ERP systems, which can be applied by all enterprises, regardless of their sector or industry affiliation. The proposed methodology represents an integrated approach that combines good risk management practices and applicable regulatory requirements in the field of ERP. It meets not only the rapidly changing technological requirements, but also the real needs of modern companies.

2. Literature Review

Risk analysis and assessment are the most important and essential parts of any strategic management of a company. The focus of good risk management is on identifying, analyzing and assessing risk. These processes depend on various factors that can be both internal and external to a particular organization. The process of assessing and managing risk in an organization is mostly related to ensuring an adequate structure in order to meet the future needs of the business. It also covers management of decision-making processes, asset protection, ensuring better and more efficient allocation of capital and ways of its investment and reinvestment.

ERP systems are integrated information platforms that not only cover multiple business processes and activities, but also create conditions for collaboration between different units and departments in the company (Nawaz & Channakeshavalu, 2013). That is why

risk management in the implementation and use of these systems must be a comprehensive and continuous process. Due to the complexity of ERP solutions, even the smallest system problems and/or deviations can lead to the suspension or interruption of activities, limited planning, loss of information volumes, etc. Studies in practice show that insufficient planning, lack of professional skills and misunderstanding of the main business processes are among the most common reasons for the failure of ERP projects (Anaya & Qutaishat, 2022). Therefore, it is important to pay special attention to the risk aspects of the ERP environment in order to minimize the negative consequences for the business (including technological, organizational, financial, etc.).

Risk factors play a significant role in the integration and use of ERP systems (Kwak & Stoddard, 2004). The main risk effects for individual companies are budget overruns, time overruns, project stoppages, poor business performance, insufficient system reliability and stability, low alignment of organizational processes, low user satisfaction, low degree of integration and flexibility, low alignment of strategic goals, and poor financial/economic performance (Aloini et al., 2007).

Several research studies have examined the risks associated with ERP and have attempted to classify them according to different criteria/attributes. The following six risk categories are presented by Sumner (2000):

- Organizational fit, i.e., inability to redesign business processes;
- Skill mix, i.e., insufficient training and retraining;
- Management structure and strategy, i.e., lack of support from senior management;
- Software system design, i.e., lack of integration;
- User involvement and training, i.e., ineffective communication;
- Technology planning/integration, i.e., inability to avoid technological barriers.

The above risk categories are also related to the following six main dimensions of risks in ERP implementation and use. They were identified by Poba-Nzaou and Raymond (2011), namely: organizational, business-related, technological, entrepreneurial, contractual and financial risks (Poba-Nzaou & Raymond, 2011).

To minimize the risk of an ERP project, Markus and Tanis (2000) recommend implementing a risk management plan at the different stages of the process—selection, implementation and use of the ERP system. A planned and systematically adopted risk management procedure throughout the ERP project reduces the possibility of risks occurring. Therefore, according to Bernroider and Leseure (2005), major mistakes are made in the early stages of an ERP project, even before the implementation process. However, Kliem (2000) emphasizes the effectiveness of risk management when it is introduced as early as possible in the life cycle of the system in question, when planning issues are most important and the criteria for system selection are defined.

Instead of using the aforementioned ready-made risk lists, a company may consider identifying its own company-specific list of risks for ERP integration. These risks can be supplemented by generic risk lists (Sumner, 2000). According to Boehm (1991), the risk assessment process involves risk identification, analysis, and prioritization of risk factors. Risk identification creates lists of risk elements specific to the ERP project that are likely to compromise its success (Boehm, 1991). Risk analysis estimates the loss in terms of probability and magnitude for each identified risk element. Risk prioritization results in a ranking of the risk elements that are identified and analyzed. To be effective, a risk assessment method must consider several potential aspects (technological, market, financial, operational, organizational, and business) and relate them to the project life cycle (Iskanius, 2009).

The scientific studies mentioned do not provide an exact answer to the development of a specific methodology for risk assessment and management using ERP systems. Their

effective application for business process management is related to the development of a risk matrix, which will allow for research and preparation of assessments based on considering factors such as influence, impact and vulnerability. The use of a risk matrix is a key tool for identifying, assessing and prioritizing potential threats in order to ensure optimization of business processes and risk control. The use of this methodology will allow the scope and objectives of the audit engagements to be considered when assessing ERP risk ([The World Intellectual Property Organization, 2025](#)). In this regard, they should focus on the assessment and include the following processes:

- Identification, assessment and management of risk by the organization's management;
- Compliance with legislation, internal acts and contracts;
- Reliability and comprehensiveness of financial and operational information;
- Effectiveness, efficiency and economy of activities;
- Protection of assets and information;
- Performance of tasks and achievement of objectives.

For the purposes of the analysis of ERP systems, the role of internal audit is to provide independent and objective assurance and reliability that risk management processes and internal controls are functioning effectively. This ensures that the organization can achieve its objectives in the short, medium and long term. Internal audits can help organizations in the integration and use of ERP systems, as well as improve their activities by:

- Assessing risk management, management and control processes;
- Ensuring the adequacy of internal control;
- Assessing quality, ethics, economy, efficiency and creating a control environment;
- Communicating information and opinions clearly and accurately.

From an internal audit perspective, ERP solutions have created both new opportunities and new challenges ([Bae & Ashcroft, 2004](#); [Debreceeny et al., 2005](#)). On the one hand, the use of an integrated system increases transparency in business processes. On the other hand, it eliminates the need for controls to ensure the consistency and accuracy of data when it is moved from one system to another. Given that ERP is a popular and pervasive platform used by many organizations, and due to increased attention to IT-related risks, security and internal controls related to information systems have increased significantly ([Chang et al., 2014](#)).

3. Materials and Methods

There is a significant amount of research in the scientific literature on ERP systems and their integration into the business context. In fact, the various studies do not offer an integrated framework or methodology for a combined assessment of potential risks. From a management perspective, this often makes their identification and prioritization difficult, as well as increases the likelihood of delaying the ERP systems integration process ([Rajapakse & Thushara, 2023](#)). In order to increase the effectiveness of ERP solutions and their integration into the business, it is necessary to initially identify potential risks ([Malik & Khan, 2020](#)). Then, they should be assessed using a selected methodology, which allows for adequate measures to be taken to limit, eliminate or manage them.

The study uses an integrated systems-analytical approach to develop and validate the five-step risk assessment matrix for ERP systems. This approach combines theoretical analysis and empirical observation of ERP processes, based on the concept of researchers who support the use of various methods to confirm the generated results ([Kozhukhivskyi & Kozhukhivska, 2020](#)). A conceptual framework for the quantitative measurement of risks identified in ERP systems is consistent with the logic and requirements of international risk management standards in order to ensure good compatibility and synchronization. A simi-

lar approach to systematization and assessment of risk factors is discussed and applied by Svensson and Thoss (2021), who classify risks according to certain criteria—technological, organizational and similar. The risk assessment matrix is empirically tested through questionnaires and structured interviews in three companies operating in different economic sectors. This ensures validation of the theoretical validity and practical applicability of the approach by comparing the results of the quantitative risk assessment with the expert assessment of department managers, IT specialists and internal auditors.

For the purposes of this study, a five-level risk assessment matrix is proposed that reflects the specific features of ERP platforms (see Table 1). It is based on three factors (including influence, impact, and vulnerability), each of which is rated on a scale from 1 to 5. The matrix is applicable only for the quantitative measurement of already identified risks. It takes into account their probability of occurrence, their potential impact on business processes and the degree of vulnerability to potential threats.

Table 1. Risk assessment matrix.

Scale	Influence	Impact	Vulnerability
1	minimal influence	minimal impact	minimal vulnerability
2	low influence	low impact	low vulnerability
3	medium influence	medium impact	medium vulnerability
4	great influence	great impact	great vulnerability
5	critical influence	critical impact	critical vulnerability

Source: Author's interpretation.

Unlike traditional two-factor risk matrices, which are based primarily on the factor's "probability" and "impact", the proposed methodology includes a third independent factor—"vulnerability". In the ERP environment, vulnerability is not limited to exposure to external threats. It reflects the degree of organizational maturity, the level of integration between modules, as well as the training of personnel to work with them. The contribution of the study is expressed in the identification of vulnerability as an independent measure of architectural sensitivity in ERP systems. In this way, the proposed matrix adapts the general principles of risk management to the specifics of the ERP environment, considering the relationship between IT architecture and business processes.

The determination of the levels of individual risk factors is based on pre-selected criteria. In fact, these criteria show what the scale of a potential risk event can be and what its consequences are. The values in the scale, which are assessed as minimal, reflect those situations in which the risk has a limited impact on individual ERP modules and does not lead to serious disruptions to business processes. There are risk events that can affect one or several functional areas or create temporary difficulties in the operation of the ERP system. For them, according to the scale, average values are used. Alternatively, the highest values are an indication of the presence of a risk of significant disruptions to the ERP architecture. These disruptions can lead to interruption or cessation of key business processes—activities. Thus, by using the five-point scale, the qualitative characteristics of the risk are transformed into a quantitative assessment. A real opportunity is created for subsequent analysis and comparability of the results.

It can be argued that the proposed risk assessment matrix is adapted to the specifics of the studied environment. The reason is that on the one hand it takes into account the complexity of ERP systems, and on the other hand it allows for multidimensional and quantitative measurement of the three risk factors. In fact, this approach provides a high degree of analytical precision by transforming qualitative assessments into a quantitative scale. This scale is compatible with the requirements and guidelines of international

risk management standards, including ISO 31000:2018—Risk management: Guidelines (International Organization for Standardization, 2018), ISO/IEC 27005:2022—Information security, cybersecurity and privacy protection: Guidance on managing information security risks (International Organization for Standardization & International Electrotechnical Commission, 2022), and others.

The level of overall risk measured using the risk assessment matrix can vary in the range from 1 to 125. It is determined by the following formula:

$$\text{Overall risk} = \text{Influence} \times \text{Impact} \times \text{Vulnerability}$$

The relationship between the scale for assessing individual risk factors (Table 1) and the classification of the overall risk (Table 2) is established through the range of possible values of the product of the three factors (including influence, impact and vulnerability). Since each factor is assessed on a scale from 1 to 5, the minimum value of the overall risk is 1, and the maximum—125. The resulting interval is divided into five categories corresponding to the different risk levels—low, medium, high, very high and catastrophic risk. For the purposes of the study, Table 2 serves as an interpretation scale for the quantitative results obtained during the testing of the proposed risk assessment methodology. The risk categories track the degree of impact of a given risk event on work processes and establish the need for a management response. The quantitative values of the influence, impact and vulnerability factors are combined into an integrated indicator of the overall risk. On this basis, the identified risks are classified and, if necessary, relevant management measures are subsequently proposed.

Individual risk factors do not act in isolation but mutually reinforce their impact. With a high degree of vulnerability, even a moderate impact can lead to a significant increase in the overall risk. The factors are considered to be equal weight, as the goal is to ensure the universality of the methodology and its applicability in different sectors and industries. This allows us to maintain the logical consistency of the methodology when assessing complex risk situations.

The conceptual logic of the proposed methodology for quantitative risk assessment is based on a multifactor model, in which the overall risk level is determined as a product of three key factors—influence, impact and vulnerability. The choice of this model aims to detail the probability of risk occurrence by including the ERP environment-specific factor “vulnerability”. Unlike general risk frameworks, this approach takes into account the direct relationship between the software architecture and the company’s readiness for integration of ERP solutions. The developed risk assessment methodology is consistent with good practices in the field of information security and risk management.

For the purposes of the study, each component of the formula has a specific scope. For example, impact measures the intensity of external or internal factors provoking a given risk event. Impact identifies the risk consequences (including direct and indirect) on business processes. And vulnerability takes into account the degree of maturity and the ability of the company to neutralize threats to an acceptable level through the control mechanisms integrated into ERP systems. In the context of ERP systems, these factors take into account not only technological, but also organizational and process aspects of risk.

For interpretation of the results of the risk assessment, it is recommended to use a rating scale (see Table 2). This scale allows classifying the identified risks into a certain category, as well as assisting the responsible persons in choosing appropriate measures to reduce the already assessed risks. Each of the defined categories is directly related to a specific strategy for responding to the risk by management.

Table 2. Rating scale for classifying overall risk levels (based on the product of the three risk factors).

Range	Overall Risk Level	Possible Reactions to the Risk	Recommended Management Measures to Overcome
From 1 to 25	Low risk	Accepting the risk or ignoring it	• Overview of the main business processes in the individual ERP modules; • Documenting problem areas in ERP systems; • Periodic random data check in.;
From 26 to 50	Medium risk	Monitoring and risk analysis	• Regular monitoring of key ERP modules for early identification of potential failures; • Engaging experts/users to monitor key modules; • Identification and analysis of possible consequences on business processes and preparation of an action plan in the event of exponential risk growth.
From 51 to 75	High risk	Risk management	• Specialized training of staff for working with ERP functionalities; • Implementing corrective actions for deviations, module testing and quality control; • Optimization of business processes in the ERP platform according to the manufacturer's system requirements.
From 76 to 100	Very high risk	Intensive risk management	• Improved monitoring through integration of an early warning system; • Formation of a specialized team of experts to respond to critical problems; • Involving all stakeholders in the risk management process and providing communication channels.
From 101 to 125	Catastrophic risk	Risk termination or avoidance	• Temporarily suspending the operation of problematic ERP modules until the malfunctions are corrected; • Generating backup copies of information flows and adopting data security plans to prevent possible damage; • Offering alternative options for continuing work.

Source: Author's interpretation.

The ranges in the rating scale are consistent with the maximum value of the product of the three factors. Each risk category corresponds to a specific interval of possible outcomes. In fact, this ensures logical consistency between the assessment matrix and the classification of the overall risk.

When determining the risk levels, predefined criteria were used. These criteria reflect not only the scope of the affected business processes, but also the possibility of interruption of activity and the presence of internal control mechanisms. The minimum values in the rating scale indicate whether there are isolated (incidental) deviations with a limited impact on individual ERP modules. The average values cover violations that affect several functional areas. Critical values for the relevant risk factor are associated with a systematic violation of the ERP architecture and interruption of key business processes.

The above-proposed risk assessment methodology reflects the author's concept of quantitative measurement of risks associated with ERP solutions. By examining the factors of influence, impact and vulnerability, an objective picture of the potential threats that may arise in the process of implementation and integration of ERP systems in the business is achieved (Efe, 2024; Rahman et al., 2024). The rating scale allows for the categorization and prioritization of risks, which facilitates making relevant management decisions and planning preventive measures.

Before the introduction of the proposed methodology in the studied companies, the assessment of risks related to ERP systems was not carried out through a structured quantitative model. For the risk assessment, they used internal control procedures, periodic

inspections and expert discussions between management personnel and IT specialists. For example, in company “AB” it was found that risk management is carried out at two levels: through ongoing control of information arrays and verification of the correctness of the management reports generated. In company “CD” the risk analysis is carried out through a periodic review of deviations in the logistics and commercial processes. The ERP system SAP supports the processing and coordination of these processes. In company “EF” for the risk assessment, internal technical reviews were introduced. Their role is to guarantee the stability of the Microsoft Dynamics ERP system and its integration with production processes. The risk management practices introduced in the three companies do not provide a single quantitative framework for comparing the various risk factors. They only allow the problem areas in the operation of the ERP systems to be identified.

4. Results

The developed risk assessment methodology has been implemented in the activities of three companies operating in different economic sectors. The study was conducted during the period of one (1) year September 2024–September 2025. The information base was provided by conducting individual semi-structured interviews and completing self-assessment cards. Department managers, IT specialists and internal auditors participated in the process of identifying and assessing risk factors. In each of the companies studied, between three and five experts were involved in the risk assessment process. The assessments were formed individually by each participant using predefined criteria. For each risk factor, an average value was calculated, rounded to the nearest integer. In the presence of significant differences, additional discussion was held until consensus was reached.

In fact, the purpose of the study is to examine the applicability of the matrix for assessing the identified risks, as well as to compare the generated results. This allows for the construction of an individual risk profile for each of the analyzed companies, taking into account its scale and the specifics of the activity, the characteristics of the industry, etc. The analysis also makes it possible to identify the risk areas requiring management measures to minimize the level of risk.

Below are the profiles of the three companies included in the study:

- “AB” is a small-sized company operating in the service sector. Its main activity is related to the provision of consulting services, including professional training in financial, accounting, tax and other issues, as well as the development of specialized software solutions for business. It uses ERP systems, based on CRM (Customer Relationship Management) and BI (Business Intelligence) platforms, to manage its processes, for its financial reporting, as well as for making various management decisions.
- “CD” is a large company that is fully engaged in commercial activities. It has retail outlets located in various regions and areas around the world. It is constantly growing through acquisitions and mergers. This is the reason why it owns and uses different IT systems for many unrelated business processes. To solve this problem, “CD” has undertaken a strategy to implement ERP system. SAP ERP was chosen as such a system, as it supports modules for human resources management, financial reporting, supply chain management and sales.
- The scope of the sample also includes the company “EF”, which is categorized as medium. Its main activity is focused on the production of machinery and equipment for steel processing, paper production, chemical industry and shipbuilding. It is interesting to note that according to its organizational structure, the finance department consists of only three employees and all duties regarding reporting, internal control and internal audit are performed by them. One year ago, it invested in a new software product—Microsoft Dynamics ERP—in order to improve the processes of effective

management of costs and financial resources, improve and optimize reporting, as well as for synchronization and cooperation between the main production activities.

The use of customized ERP solutions in each of the three companies creates specific challenges both in identifying potential risks and in managing them. It was found that in company “CD”, in which SAP ERP is implemented, the prevailing risks are related to the integration of multiple functional modules and the coordination between different sales structures. One of the main challenges for company “EF” is the dependence of production processes on the stability and reliability of the Microsoft Dynamics ERP information system. The reason is that in case of possible system deviations, the production schedule may be disrupted, which subsequently leads to delays in deliveries. In company “AB”, ERP solutions are implemented through a combination of CRM and BI platforms. Such a configuration complicates data integration and increases the risk of inconsistencies in management reports. The differences and challenges characteristic of the three companies show that the risk profile of ERP systems depends not only on the technical characteristics of the software used. It is also influenced by the organizational environment and the degree of integration of business processes.

The validation of the risk assessment methodology was implemented only in three companies included in the sample. The purpose of this step is not statistical verification. The idea is to verify the applicability, functionality and conceptual logic of the proposed methodology by testing it in real business conditions. By comparing the expert opinions of managers, IT specialists, etc., with the obtained quantitative assessments, it was established to what extent it reflects the real risk characteristics of the studied business organizations. The results also provide an opportunity to perform a comparative analysis between companies depending on the scale, complexity of the processes and the degree of implementation of ERP systems.

By applying the five-step risk assessment matrix, the risks associated with the implementation and use of ERP systems in the three companies were identified and measured. The analysis tracks the probability of occurrence of risk events, their potential impact on business processes and the degree of vulnerability (Mistry, 2025). The summarized results regarding the individual risk profile of the companies are presented in Table 3.

Table 3. Identifying risk factors in companies “AB”, “CD” and “EF”.

Company	Risk Characteristics		
	Influence	Impact	Vulnerability
“AB”	Medium influence	Low impact	Minimal vulnerability
“CD”	Minimal influence	Great impact	Medium vulnerability
“EF”	Great influence	Medium impact	Critical vulnerability

Source: Author’s interpretation.

The three companies studied show different risk profiles. These differences stem from the scale of the business, the complexity of the processes and the degree of integration of the ERP systems. In “EF”, the high vulnerability is associated with limited administrative capacity and a strong dependence of production operations on the implemented ERP system. In “CD”, a higher impact is reported, due to the geographical fragmentation of the commercial activity and the use of multiple interconnected ERP modules. In “AB”, the lower values are explained by the smaller scale of the business and the more limited scope of the implemented ERP functionalities.

The analysis of the main risk factors related to the integration of ERP systems in the individual economic sectors reveals some differences between the three companies. In the risk profile “EF” a high impact and critical vulnerability are observed. This necessitates the need for active control over all ERP modules and, respectively, adequate preventive mea-

asures by management. In company “CD” a minimal impact is observed, accompanied by a significant impact on business processes. To minimize the risk, systematic optimization and monitoring of key ERP functionalities, as well as periodic staff training, are recommended. Company “AB” shows relative stability in terms of risk, therefore no additional actions are required to optimize the ERP platform used. It has a moderate influence, low impact, and minimal vulnerability.

The comparative analysis reveals that the risk associated with ERP solutions increases with the scale, complexity and degree of integration of business processes between departments in companies. Management measures and mechanisms for reducing potential threats should focus not only on technical support and updating of modules in ERP systems, but also on the development of personnel competencies and strengthening coordination between departments.

The values of the individual risk factors are formulated through expert assessment based on predefined criteria. Each participant in the study assesses the factors influence, impact and vulnerability on the five-point scale presented in Table 1. When determining the values, several criteria are taken into account: (1) the company’s dependence on the ERP system; (2) the presence of internal control mechanisms; (3) the scope of the affected ERP modules and (4) the degree of influence on the main business processes. When there are factors that can affect a significant part of the company’s business activities, higher values of influence are assigned. For example, higher values in terms of impact are determined in the case of potential consequences on more than one business process or structural and organizational unit. Higher values of vulnerability reveal the degree of readiness to identify and limit risk events. After performing the individual assessments by the participants in the study, an average value is established for each risk factor, which is rounded to the nearest integer. And the resulting values are used to calculate the overall risk level.

The results of the quantitative risk assessment are summarized in Table 4.

Table 4. Risk assessment in the implementation and use of ERP systems in the companies “AB”, “CD” and “EF”.

Criteria	Company “AB”	Company “CD”	Company “EF”
Influence	3	1	4
Impact	2	4	3
Vulnerability	1	3	5
Overall Risk	6	12	60
Risk Category	Low Risk	Medium Risk	High Risk

Source: Author’s interpretation.

The study identified several risk situations related to the functioning of the ERP systems in the three companies. In company “AB”, the risk should not be underestimated, despite its categorization as low. Inconsistencies between the data processed in the different CRM and BI modules are possible, which can be a prerequisite for inaccuracies and errors in management reports. The main risk in company “CD” is related to the integration of multiple ERP modules and the exchange of data between different sales structures. This increases the likelihood of delays in the exchange of information or the occurrence of inconsistencies between the individual information flows. The situation in “EF” is more complicated and cannot be assessed unambiguously, given its risk profile. In this case, the risk is considered significant, since systematic deviations in the ERP architecture can directly reflect on the production schedule. In the long term, this can lead not only to delays in deliveries, but also to disruption of the production rhythm and difficulties in resource planning. The identified risk situations in “AB”, “CD” and “EF” show that the quantitative

assessment of risk is not based solely on abstract rating values. It has a direct connection to real organizational and technological difficulties in the use of ERP systems.

The results obtained reveal significant variations in the risk levels between the three companies. They are due, on the one hand, to the specificity of their activities and the complexity of the business processes, and on the other—to the duration of the implementation and use of ERP systems with different functionalities. It is necessary to implement differentiated management measures for risk management in each of the studied companies, as well as to establish a policy for periodic monitoring of the ERP systems.

Company “AB” is characterized by the lowest level of risk, due to the fact that it has simpler financial reporting and good synchronization of the main business activities. In company “CD”, the risk is identified as medium, since its commercial processes are significantly complicated. As a result, it also uses multiple ERP modules that support the servicing of commercial operations. Company “EF” is exposed to high risk. It has a high degree of dependence on the integrated ERP system, which is used to coordinate and optimize the main production operations. The results obtained in the risk assessment confirm that its increase is directly related to the complexity of business processes and the degree of integration of ERP solutions.

In response to the assessed risks, it is recommended that the three companies surveyed adopt a set of measures to improve the risk management process. Some of the main recommendations are summarized in Table 5.

Table 5. Recommendations for ERP risk management in companies “AB”, “CD” and “EF”.

Company	Risk Profile	Main Recommendations
“AB”	Overall risk = 6 (low)	• Periodic monitoring of frequently used ERP modules (every quarter); • Documenting problem areas as needed; • Conducting regular training on working with ERP functionalities; • Ensuring good communication between departments.
“CD”	Overall risk = 12 (medium)	• Ongoing optimization of key ERP modules; • Conducting regular monitoring by ERP experts (every quarter); • Approval of a policy for action in critical situations; • Additional specialized training for working with new ERP functionalities.
“EF”	Overall risk = 60 (high)	• Regular audits of the ERP system (2 times a year); • Formation of a specialized team of risk management experts; • Business process optimization and ERP module testing; • Developing strategies for protecting information assets; • Establishing a coordination mechanism between departments.

Source: Author’s interpretation.

The recommendations proposed in Table 5 are tailored to the organizational specifics and scale of the companies studied. For example, periodic monitoring of the main ERP modules on a quarterly basis in company “AB” is considered sufficient for early identification of potential deviations. The main argument is that “AB” is a small organization that uses a limited number of ERP functionalities given the relatively simplified business processes. In company “CD” a more complex organizational structure is observed, as well as a wider regional scope of activity. For these reasons, in “CD” more intensive control over the integration between ERP modules and good coordination of information flows is required. In company “EF”, where production processes are highly dependent on the functioning of the ERP system, it is recommended to conduct regular internal audits at least twice a year. Therefore, effective ERP risk management requires adapting the control mechanisms to the specifics of the organizational environment and the degree of dependence of business processes on IT systems.

Given the dynamic nature of processes in an ERP environment, it is relevant to apply the proposed risk assessment methodology regularly, i.e., at a certain interval of time. This allows the teams responsible for risk to promptly identify potential deviations, as well as to adopt measures to minimize their impact (Musaji, 2002).

The analysis demonstrates that overall risk values exhibit significant variance across the three studied organizations. This divergence confirms the sensitivity of the risk assessment methodology to diverse organizational and technological environments. Furthermore, the study identifies a positive correlation between elevated risk levels and increased complexity in business process architecture, a high degree of dependence on ERP solutions, and lower levels of organizational maturity.

In the subsequent SWOT analysis, the quantitative data find their qualitative confirmation, where high risk levels correspond to certain weaknesses in the ERP environment. This confirms that the proposed methodology serves not only for quantitative measurement of the identified risks, but also for its subsequent interpretation from a management point of view. In this way, conditions are created for making informed decisions regarding the priority areas in risk management and planning of preventive measures.

5. Discussion

The present study, which is based on a five-step risk assessment matrix, reflects the specific features of ERP platforms. It is based on the three analyzed factors—influence, impact and vulnerability and is applicable only for quantitative measurement of already identified risks. Through the analysis, the probability of occurrence of risk events, their potential impact on business processes and the degree of vulnerability are tracked. The results obtained from the practical application in the three analyzed companies confirm the conceptual logic of the proposed three-factor risk model.

In the three companies studied, the role of stakeholders in the risk management process is different. On the one hand, it depends on the organizational structure, and on the other it depends on the nature and specificity of business processes. It was found that in company “AB” the main participants in risk management are the financial manager, IT specialists and employees. Their responsibility is reduced to the processing and analysis of data in the CRM and BI modules of the ERP system. In company “CD” a wider range of participants is involved in risk management, such as ERP administrators, representatives of senior management, managers of sales units and financial controllers. Their efforts are aimed at coordinating the work of individual ERP modules and functionalities. In company “EF” the production managers, the financial department and system administrators take part in the risk management process. They monitor how the Microsoft Dynamics ERP platform functions, as well as what its impact is on production processes. The active participation of these stakeholders allows for more effective identification, analysis and control of risks associated with the operation of ERP systems.

The results of the study highlight the need for effective integration of ERP solutions into the business, addressing technical challenges, increasing project efficiency and training for the effective use of IT systems. Based on the study of the ERP environment and the results obtained from the three companies analyzed, a SWOT analysis was prepared. The goal is to summarize the trends observed from the research conducted, as well as to outline opportunities for the implementation of the systems in various businesses. It is presented in Table 6.

Table 6. SWOT analysis of ERP systems.

Strengths: • Effective management of costs and financial resources; • Synchronization and cooperation between the main activities; • Better communication channels; • Improved reporting (operational and financial); • Easier generation of reports necessary for making management decisions; • Work “in real time” for a large part of business processes; • Generation of reports and reports according to professional needs; • New strategies for improving the activity; • Building a modern ERP infrastructure.	Weaknesses: • Implementation costs exceed the average level, which is 50–100% of the sales value of the ERP system; • The high sales value; • The high costs of implementation and maintenance of the systems; • Too slow ERP integration process; • Poor management of data and information channels; • High indirect costs (new computers, IT staff, staff training, etc.); • The need for frequent maintenance of the implemented ERP systems.
Opportunities: • The development of new functionalities and modules; • The expansion of integration capabilities; • Central control over workflow data; • The creation of a department for consulting on the use of ERP systems; • The increase in ERP applicability in more industries, sectors and enterprises; • The introduction of a new technological application; • Easier response to the personal needs and requirements of customers.	Threats: • Different levels of protection of IT systems; • Lack of well-trained personnel for the use of ERP systems; • Lack of trained consultants in the field of ERP systems; • Insufficient knowledge of the business regarding the capabilities and/or return on investment of ERP systems; • Aggressive advertising and sales policies of competitors; • Lower price offered by competing ERP systems; • Changing economic environment conditions; • Changing customer profile.

Source: Author’s interpretation.

The results of the SWOT analysis reflect the main factors that influence risk management when using ERP systems in the companies studied by. In company “AB”, some of the advantages are related to improved analytical data processing and generation of management reports through CRM and BI functionalities. In company “CD”, the SAP ERP system provides both coordination between multiple sales units and centralized management of information flows. The Microsoft Dynamics ERP software product, integrated in company “EF”, supports synchronization between production processes and financial management. At the same time, the identified weaknesses and threats manifest themselves differently in the activities of the three companies. In company “AB” they are mainly related to the limited scope of ERP functionalities, while in “CD” they arise as a result of the more complex integration between the individual modules. In company “EF” the main risks arise from the higher dependence of production activities on the stability of the ERP platform. Strengths and weaknesses, and opportunities and threats manifest themselves differently in “AB”, “CD” and “EF”. The reason is that their manifestation depends not only on the organizational context, but also on the degree of integration of business processes.

Internal auditing of IT systems and related organizational procedures is critical to the ERP risk assessment process. This audit should be executed through pre-defined planning and control frameworks. From a procedural standpoint, it encompasses several key stages: identification and classification, analysis, model selection, monitoring, mitigation, and risk minimization.

Going through the specified stages in the ERP risk assessment and management process is characterized by planning, implementation of measures and subsequent evaluation of the results obtained. Effective risk management must involve various stakeholders, tailored to each specific organization, each with defined roles and authority levels. These stakeholders contribute uniquely to risk identification, analysis and control. These risks are also given one of four levels—external engagement, program management, workflow level and work package level, in accordance with the current reporting structure.

Effective risk management, specifically regarding the implementation and utilization of ERP systems, requires systematic reporting, continuous review, and standardized regulation of the assessment and analysis processes. In this context, various international standards and frameworks define the essential elements required for robust monitoring and control. In general, they are reduced to:

- Measuring the results obtained;
- Analyzing and evaluating the procedures and information that were used during the risk management process;
- Using the acquired knowledge and evaluating the errors, with the aim of their future reporting and obtaining optimal assessments.

Based on the results obtained from the applied risk assessment methodology, the use of ERP systems facilitates the identification and management of risks in the company. Integrated ERP solutions improve the planning and execution of audit engagements (Musaji, 2002). At the same time, for their successful integration, it is important to analyze the existing activities and processes in the company in order to create appropriate organizational change (Magnusson & Olsson, 2005). Each organization has its own need, not only for operational changes, but also for systemic changes and adaptations, in order to function in an efficient and effective manner (Sullivan, 2009). For example, different ERP users have personal needs and requirements for integrated business process management.

The implementation and use of ERP systems should not be viewed simply as a project to acquire a new software platform, but as an opportunity to effectively manage all business processes of the company, as well as for risk analysis and assessment. In this regard, steps should be taken in two directions:

- Modifying business processes to fit the software specification of the particular system. On the one hand, fewer modifications to the software application should reduce errors and help to use newer versions and releases. On the other hand, this choice may mean changes in long-established ways of assessing risk and making various management decisions (which often provide a competitive advantage).
- Modifying IT systems to fit the processes (McAdam & Galloway, 2005).

The relationship between the use of ERP systems and risk assessment is based on the correct determination of the impact of specific risk factors (Zhang et al., 2025). The process of analyzing potential risks can be divided into the following categories: (1) ERP provider, (2) ERP system and (3) the company using the system. The most significant potential risk associated with the ERP provider is the selection of an unsuitable partner who does not understand the specific wishes and needs of the company or is not interested enough to commit to the project of the respective company. A high potential risk is the fact that the ERP provider may discontinue the development and/or support of the ERP system. Most potential risks associated with the ERP system depend on its technical and functional characteristics. This refers to how well the system can be implemented, configured and integrated. In fact, most potential risks regarding the company itself are related to its personnel and management, as well as their skills, knowledge and experience (Costa et al., 2024).

The appropriate choice of ERP system can significantly reduce subsequent implementation risks, such as the impact of operational risks. Although there are some frameworks that help manage implementation risk, they are usually too theoretical and their use is limited mainly due to a lack of knowledge on the part of users. Therefore, it is necessary to prepare an analysis of the company's needs to help manage the risk of ERP implementation effectively. The new ERP system should facilitate operational processes for the company, as the system will process information throughout the enterprise. In this regard, training is an important part of the implementation process, as the lack of training often leads to negative attitudes and unsuccessful implementation (Garly, 2011). However, successful implementation does not only depend on the quality and quantity of training, but also on the willingness of employees. A successful ERP deployment aims for operational efficiency, which facilitates robust risk mitigation and supports strategic decision-making.

Managerial Implications

Making the right management decisions is essential for the development of business processes and risk management in companies. This is where ERP systems help and it is necessary to outline the management consequences. The following can be mentioned as such: (1) they allow management to act preventively, which leads to cost reduction; (2) they enable automated controls in the system (e.g., access and approval levels) and thus limit the possibilities for internal fraud and abuse; (3) they create the possibility of more flexible planning of activities and effective decision-making; and (4) optimization of compliance with legal rules and requirements, as well as internal audit mechanisms.

6. Conclusions

The risk assessment methodology developed in the article takes into account the importance of both IT systems and internal audit mechanisms and principles. In risk management, the stage of identifying risk factors may be more important than the stages of risk analysis and developing a mechanism for its reporting. This is because if risks are not identified correctly, subsequent complex analysis techniques or management decisions made on this basis are unlikely to lead to the desired results. On the other hand, appropriate risk identification can facilitate both appropriate subsequent analysis and management actions. The proposed risk assessment methodology will not only help stakeholders (client, consultant or ERP provider) to correctly identify risks, but will also facilitate objective analysis and allow for appropriate management of these risks. The risk assessment is based on taking into account the influence of three factors. This allows for effective management of business processes and making complex and justified decisions to optimize activities. The proposed methodology is new, because so far only two-factor ones have been applied. In a proactive approach to this process, all stakeholders participate in identifying and analyzing the risk for each stage of the ERP implementation project before making decisions about the specifics of the project (e.g., resource allocation, choice of implementation approach, selection of contractors and suppliers, etc.). The success of ERP implementation is partly related to the fact that stakeholders understand and appreciate the importance of the systems in optimizing the activities of companies (Salih et al., 2022).

The goal of ERP system integration is to make companies' business processes more effective and efficient in order to achieve competitive success in the market. However, some risk factors are widespread and must be taken into account in risk management. It is important to analyze the existing processes and the effectiveness of the activities in the company in order to create mechanisms that could be implemented in a new ERP system for a specific company.

The results of the study clearly show that the applied methodology for risk assessment in ERP systems is an effective tool that serves to identify problem areas in business process management. The analysis carried out in the three companies confirmed that the increase in risk is due to the scale and complexity of the business. It should be borne in mind that the proposed methodology for quantitative risk assessment can be used in the following areas: (1) for optimization and synchronization of business processes; (2) for improving internal control and audit procedures; and (3) for making relevant management decisions. In subsequent scientific research, it is possible to adapt the methodology for next-generation ERP solutions, including the integration of cloud technologies and systems in various industrial sectors, the development of intelligent ERP systems, AI-based and Internet of Things-based systems, etc. In this way, its scope of application will be expanded in the context of the sustainability and competitiveness of enterprises.

Author Contributions: Conceptualization, K.L. and N.V.-S.; methodology, K.L. and N.V.-S.; validation, K.L. and N.V.-S.; formal analysis, K.L. and N.V.-S.; investigation, K.L. and N.V.-S.; resources, K.L. and N.V.-S.; data curation, K.L. and N.V.-S.; writing—original draft preparation, K.L. and N.V.-S.; writing—review and editing, K.L. and N.V.-S.; visualization, K.L. and N.V.-S.; supervision, K.L. and N.V.-S.; project administration, K.L.; funding acquisition, K.L. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by the European Union—NextGenerationEU, through the National Recovery and Resilience Plan of the Republic of Bulgaria, grant number BG-RRP-2.004-0005. The APC was funded by the European Union—NextGenerationEU, through the National Recovery and Resilience Plan of the Republic of Bulgaria, grant number BG-RRP-2.004-0005.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: The names of the companies are not disclosed in order to protect company confidentiality and in accordance with the principles for the protection of sensitive information according to the ethical guidelines of COPE (Committee on Publication Ethics). For the purposes of this study, they are conventionally identified as “AB”, “CD” and “EF”.

Acknowledgments: This work has been accomplished with financial support by the European Regional Development Fund within the Operational Programme “Bulgarian national recovery and resilience plan”, procedure for direct provision of grants “Establishment of a network of research higher education institutions in Bulgaria”, and under Project BG-RRP-2.004-0005 “Improving the research capacity and quality to achieve international recognition and resilience of TU-Sofia (IDEAS)”.

Conflicts of Interest: The authors declare no conflicts of interest. The funders had no role in the study design, data collection, analysis, or interpretation; in the writing of the manuscript; or in the decision to publish the results.

Note

- ¹ For the purposes of this study, it is necessary to note that “ERP system implementation” will refer to the technical and organizational process of installing and configuring the software. “Integration” describes the connection of the ERP system with other existing applications that the company already implements, the term “usage” focuses on the actual operation and practical use of the systems.

References

- Aloini, D., Dulmin, R., & Mininno, V. (2007). Risk management in ERP project introduction: Review of the literature. *Information & Management*, 44(6), 547–567. [[CrossRef](#)]
- Anaya, L., & Qutaishat, F. (2022). ERP systems drive businesses towards growth and sustainability. *Procedia Computer Science*, 204, 854–861. [[CrossRef](#)]

- Bae, B. B., & Ashcroft, P. A. (2004). *Implementation of ERP systems: Accounting and auditing implications*. Available online: <https://www.csulb.edu/~bbae/publication/ERP%20implementation%20&%20implications.june%2004%20ISCJ.pdf> (accessed on 15 December 2025).
- Bernroider, E., & Leseure, M. J. (2005). *Enterprise resource planning (ERP) diffusion and characteristics according to the system's lifecycle: A comparative view of small-to-medium sized and large enterprises*. Working Papers on Information Systems, Information Business and Operations, No. 01/2005. Institut für Informationsverarbeitung und Informationswirtschaft, WU Vienna University of Economics and Business. [CrossRef]
- Boehm, B. W. (1991). Software risk management: Principles and practices. *IEEE Software*, 8, 32–41. [CrossRef]
- Chang, S.-I., Yen, D. C., Chang, I.-C., & Jan, D. (2014). Internal control framework for a compliant ERP system. *Information & Management*, 51(2), 187–205. [CrossRef]
- Costa, F., Silva, P., & Mendes, R. (2024). Retaining talent in IT: Key factors for employee engagement and satisfaction. *arXiv*, arXiv:2402.01573.
- Debreceny, R., Lee, S.-L., Neo, W., & Toh, J. S. (2005). Employing generalized audit software in the financial services sector. *Managerial Auditing Journal*, 20(6), 605–618. [CrossRef]
- Efe, A. (2024). Risk modelling of cyber threats against MIS and ERP applications. *Journal of Information Security and Management*, 12(1), 45–62. [CrossRef]
- Ganly, D. (2011). *Address six key factors for successful ERP implementations*. Gartner Research. Available online: <https://www.gartner.com/en/documents/1603415/address-six-key-factors-for-successful-erp-implementation> (accessed on 20 December 2025).
- International Organization for Standardization. (2018). *Risk management: Guidelines (2nd ed.)* (ISO 31000:2018). ISO. Available online: <https://www.iso.org/standard/65694.html> (accessed on 7 January 2026).
- International Organization for Standardization & International Electrotechnical Commission. (2022). *Information security, cybersecurity and privacy protection: Guidance on managing information security risks (4th ed.)* (ISO/IEC 27005:2022). ISO. Available online: <https://www.iso.org/standard/80585.html> (accessed on 12 January 2026).
- Iskanian, I. (2009). Risk management in ERP project in the context of SMEs. *Engineering Letters*, 17(4), EL_17_4_08.
- Kliem, R. L. (2000). Risk management for business process reengineering projects. *Information Systems Management*, 17(4), 66–68. [CrossRef]
- Kozhukhivskiy, A. D., & Kozhukhivska, O. A. (2020). ERP-system risk assessment methods and models. *Radio Electronics, Computer Science, Control*, (4), 151–162. [CrossRef]
- Kwak, Y. H., & Stoddard, J. (2004). Project risk management: Lessons learned from software development environment. *Technovation*, 24(11), 915–920. [CrossRef]
- Magnusson, J., & Olsson, B. (2005). *Affärssystem* (1st ed.). Studentlitteratur AB.
- Malik, M. O., & Khan, N. (2020). Analysis of ERP implementation to develop a strategy for its success in developing countries. *Production Planning & Control*, 32(12), 1020–1035. [CrossRef]
- Markus, M. L., & Tanis, C. (2000). The enterprise system experience—From adoption to success. In R. W. Zmud (Ed.), *Framing the domains of IT management: Projecting the future through the past* (pp. 173–207). Pinnaflex Educational Resources Inc.
- McAdam, R., & Galloway, A. (2005). Enterprise resource planning and organisational innovation: A management perspective. *Industrial Management & Data Systems*, 105(3), 280–290. [CrossRef]
- Mistry, D. (2025). Risk-aware migration strategies for enterprise ERP systems in regulated industries. *Journal of International Crisis and Risk Communication Research*, 8(S11), 135–146. [CrossRef]
- Musaji, Y. F. (2002). *Integrated auditing of ERP systems* (1st ed.). Wiley.
- Nawaz, M. N., & Channakeshavalu, K. (2013). The impact of enterprise resource planning (ERP) systems implementation on business performance. *SSRN Electronic Journal*, 2(4), 30–47. [CrossRef]
- Poba-Nzaou, P., & Raymond, L. (2011). Managing ERP system risk in SMEs: A multiple case study. *Journal of Information Technology*, 26(3), 170–192. [CrossRef]
- Rahman, M. M., Kshetri, N., Sayeed, S. A., & Rana, M. M. (2024). AssessITS: Integrating procedural guidelines and practical evaluation metrics for organizational IT and cybersecurity risk assessment. *Journal of Information Security*, 15, 564–588. [CrossRef]
- Rajakapase, D. P. P. K., & Thushara, S. C. (2023). Critical failure factors in ERP implementation: A systematic literature review. *Journal of Business and Technology*, 7(1), 65–90. [CrossRef]
- Salih, S., Abdelsalam, S., Hamdan, M., Ibrahim, A. O., Abulfaraj, A. W., Binzagr, F., Husain, O., & Abdallah, A. E. (2022). The CSFs from the perspective of users in achieving ERP system implementation and post-implementation success: A case of Saudi Arabian food industry. *Sustainability*, 14(23), 15942. [CrossRef]
- Sullivan, L. (2009). *Post-implementation success factors for enterprise resource planning (ERP) student administration systems in higher education institutions* [Doctoral dissertation, University of Central Florida]. Electronic Theses and Dissertations, 3884. Available online: <https://stars.library.ucf.edu/etd/3884> (accessed on 17 January 2026).
- Sumner, M. (2000). Risk factors in enterprise-wide/ERP projects. *Journal of Information Technology*, 15(4), 317–327. [CrossRef]

- Svensson, A., & Thoss, A. (2021). Risk factors when implementing ERP systems in small companies. *Information*, 12(11), 478. [CrossRef]
- The World Intellectual Property Organization. (2025). *Internal audit manual*. Available online: https://www.wipo.int/about-wipo/en/docs/oversight/iaod/audit/internal_audit_manual.pdf (accessed on 22 January 2026).
- Zhang, J., Zhou, S., & Ma, F. (2025). Does ERP implementation lower corporate financing costs? A dual perspective from risk management and value creation. *Risks*, 13(9), 164. [CrossRef]

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.