

Article

Innovative Approach to Conceptual Design of Enterprise Risk Management Software

Petar Stanojević ^{1,*}, Mirjana Misita ², Goran Đurić ², Bogdan Kuzmanović ³, Mladen Milošević ¹ and Daniel Balos ⁴

¹ Faculty of Security Studies, University of Belgrade, Gospodara Vučića 50, 11118 Belgrade, Serbia; milosevic@fb.bg.ac.rs

² Faculty of Mechanical Engineering, University of Belgrade, Kraljice Marije 16, 11120 Belgrade, Serbia; mmisita@mas.bg.ac.rs (M.M.); gdjuric@mas.bg.ac.rs (G.Đ.)

³ Faculty of Technical Science, University of Novi Sad, Dositeja Obradovića 6, 21000 Novi Sad, Serbia; kbogdan@uns.ac.rs

⁴ MPA—Materials Testing Institute, University of Stuttgart, 70569 Stuttgart, Germany; daniel.balos@mpa.uni-stuttgart.de

* Correspondence: petar.stanojevic@fb.bg.ac.rs; Tel.: +381-65-752542

Abstract: The paper shows the integration of the theoretical and practical aspects of designing an ERM software tool. The basic idea of the designed ERM is conceived in the form of an algorithm using the integration of ISO 3100, the COSO framework, the risk matrix designed according to the risk appetite of the observed company, quantitative and qualitative models for risk assessment, and the generation of consequences and mitigating measures for each identified risk. Methodologies for risk assessment in the presented ERM include the following: For business risks, questionnaires were generated for different business areas (from knowledge bases) and the assessment was conducted according to risk matrices. Workplace risk is assessed according to the Kinney method, while technical risks are assessed according to the API 580, 581 standard. Software is created to outbalance problems of all types of risk that may arise regardless of the complexity of the business and the risk itself. The algorithm, model and software were developed and successfully tested in two Serbian companies.

Keywords: enterprise risk management; software solution; hazard; risk management



Citation: Stanojević, P.; Misita, M.; Đurić, G.; Kuzmanović, B.; Milošević, M.; Balos, D. Innovative Approach to Conceptual Design of Enterprise Risk Management Software. *Appl. Sci.* **2024**, *14*, 11255. <https://doi.org/10.3390/app142311255>

Academic Editor: Arkadiusz Gola

Received: 18 October 2024

Revised: 16 November 2024

Accepted: 18 November 2024

Published: 3 December 2024



Copyright: © 2024 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

1. Introduction

The problem of identifying company risks, as well as their classification, assessment, the prescription of risk mitigation measures, residual risk assessment, and risk prioritization, i.e., risk management, is an increasingly complex task, although many types of software for a holistic approach to risk management exist in the market. Namely, company risk management refers to the management of different types of risks: business, financial, workplace risks, HSE, safety, legal, technical (maintenance of equipment/installations), etc., but only a portion of them are calculated (assessed) based on different methodologies.

Enterprise Risk Management (ERM) software typically employs various methodologies for risk assessment, depending on the specific needs of the organization and the capabilities of the software. ERM has taken an important place in the scientific and professional literature and has significantly contributed to developing a new organizational climate [1–7]. Some common methodologies used in ERM software for risk assessment include the following: Quantitative Risk Analysis (QRA), Qualitative Risk Analysis, Scenario Analysis, Bow-tie Analysis, Fault Tree Analysis (FTA), Heat Maps or Risk Matrices, Monte Carlo Simulation, and others. ERM software often integrates multiple methodologies to provide a comprehensive risk assessment framework tailored to the organization's needs [8–11]. The choice of methodology depends on factors such as the nature of the risks, available data, organizational objectives, and regulatory requirements [12–15].

While common Enterprise Risk Management (ERM) software offers numerous benefits, such as improved risk visibility, enhanced decision-making, and a streamlined risk management process, there are also some potential disadvantages to consider, such as complexity, customization requirements, data quality, overreliance on technology, resistance to change, cost, regulatory compliance challenges, cybersecurity, etc. [16–24].

In their research, Valashani and Abukari [12] discuss the architecture of ERM solutions in the modern environment, and on the basis of their research they conclude that ERP systems architecture has evolved from a simple two-tier architecture based on the client–server model into more modern models with three tiers or more using complicated infrastructures and platforms. The authors also state that web-based and cloud-based architectures are very common and can be seen in many ERP design frameworks, and that more and more companies are shifting their ERP deployment strategy into cloud-based ERP implementation. On the other hand, Mohamed et al. [15] state that with cloud-based ERP it is necessary to introduce standards, rules, and regulation because the main challenge with this technology is security challenges. Also, these authors state that, beside security risks, key identified challenges include customization and integration limitations, performance risks, functionality limitations, etc.

Some of these disadvantages, like customization to requirements, resistance to change, and regulatory compliance are affecting the universality and sustainability of ERM solutions, i.e., the obsolescence or non-use of the acquired software solution after a few years. Therefore, we formulated the task of creating a new approach to ERM solution design by enabling the following functionalities:

- For certain risks, the user can independently choose between a quantitative or qualitative method of risk assessment, depending on the available data. Considering that there are different types of risks (some of which can be quantified more successfully and others less successfully), and considering that in different companies there are different levels of maturity for the application of quantitative methods, an appropriate balance must be found. In cases of technical risk assessment, quantitative methods must be used more, while, for example, in the assessment of legal risks, this is generally inadequate;
- The ERM user can, in accordance with his needs, independently adjust the method of risk assessment through adjustable risk matrices (matrix size, x and y axes, calculation, ALARP zone, specific Heat map);
- The ERM user can independently choose the risk assessment methodology for a specific risk: risk matrix, Kinney method, API 580, 581 (American Petroleum Institute, Washington, Standard [25], 580—Risk Based Inspection, 581—Risk Based Inspection Technology [26]) heuristic model, etc.;
- The user of ERM can supplement the knowledge base in accordance with his needs or in accordance with compliance with prescribed regulations.

2. Methodology

In this paper, a methodology for the design of ERM software was generated such that the software solution relies on the following principles:

- Connecting ISO 31000 [27] and COSO frameworks [28];
- Application of expert knowledge in hazard identification;
- Connecting hazard and risk;
- Determination of risk appetite and adjustment of the risk matrix accordingly (5×5 matrices, 3×3 matrix, etc.) for as many risk types as needed (asset, safety, environment, reputation, etc.);
- Different risk assessment methodologies (quantitative, qualitative, semi-qualitative, Kinney, API 581, FMEA, etc.).

The proposed methodology for the design of ERM software is presented in the form of algorithms in Figure 1. The algorithm contains the following steps:

1. External experts input knowledge into a database: This step involves external experts providing their insights and knowledge into a centralized database;
2. Internal experts go through questionnaires: Internal experts review and respond to questionnaires created by external experts or surveys designed to assess various hazards. This step is important in order to allow internal experts to see their risks from a different angle, that is, from external expertise and the generated heuristic knowledge base;
3. Hazard database is generated according to the internal experts' answers: Based on the responses provided by internal experts, a hazard database is compiled or updated;
4. From this point, the joint teamwork of internal and external experts is needed to make a suitable decision: Is a hazard a risk? At this juncture, there is a decision point where the experts evaluate whether a hazard identified in the database poses a risk or not.
 - 4.1. If Yes, then the flowchart branches out further:
Additional steps might include risk assessment, risk mitigation strategies, etc.;
 - 4.2. If No, then the flowchart may lead to actions such as:
Further assessment to understand why it's not considered a risk.
5. Updating the hazard database accordingly.
6. Closing the assessment loop.
7. Regardless of the process of generating risks arising from hazards, the risk base is supplemented with the entry of acknowledged risks (existing risks in the observed company) which gives additional flexibility to the approach.
8. Risk Management process, updating classification, updating mitigation measures, updating risk assessments, etc.
9. Finally, based on the implemented processes of connecting risks with elements of organizational structures & units (COSO framework), it is possible to generate different risk cards, perform Risk Score analysis and Ie-factor (Investment effectiveness) analysis. Failure to achieve the goals of a part of the organizational structure can be considered a risk, so it is necessary to link risks with the organizational structure, which is a core of COSO framework approach.

This flowchart captures the process from external knowledge input to internal evaluation, database generation, and the decision-making process regarding whether identified hazards constitute risks.

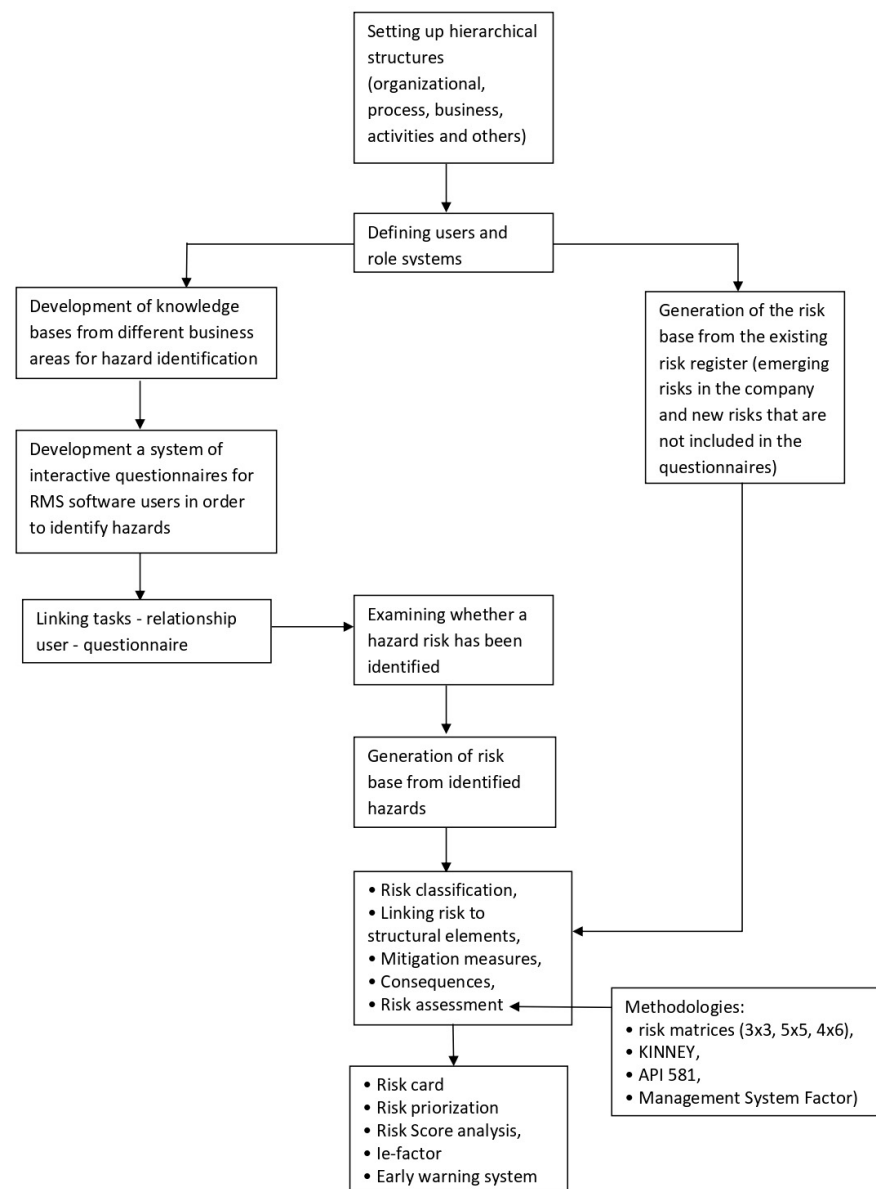


Figure 1. Methodology for the design of ERM software.

3. Software Solution RMS

The basic software solution for business risk management was initially developed within the Fund for Innovation project of the Republic of Serbia entitled “Knowledge transfer through the design of a software application for managing business risks in business-production systems based on artificial intelligence” (No. 1086). The RMS software, as it is now called, was developed by the authors of the aforementioned project and with same leading idea—to develop a software of this kind. It was completely refurbished with major improvements in software solutions and functionalities, and was implemented in the two following projects realized by companies in the fields of public transportation and the petroleum industry. In both cases, the software was the work of a completely new author. The petroleum industry is one of the leaders in the application of risk management, and therefore the software was developed for their needs. The initial version of Base Resource Document (BRD) was published in 1994 to an API lead sponsor group project. Since then, risk analysis has been applied in the petroleum industry and is an industry standard. ISO 31000 was adopted in 2009 and represents a basic, generally accepted methodology for risk analysis that is applicable regardless of industry. It is similar to the COSO framework.

The application itself in concrete organizations did not particularly affect the creation of software solutions, except for technical risks, but it was useful to bring the solutions closer to the practical needs of users.

RMS version 0.955.230725 is a holistic risk management system with an integrated expert system for following purposes:

- Implementation of the procedure of risk source identification in business-production systems;
- Usage of expert knowledge from more than 52 business areas;
- Usage of risk management standards like ISO 31000 and COSO approach;
- Usage of applicable technical standards like API 580;
- Integrated knowledge database allows updating, expanding, or adapting to a specific business-production decision tree system;
- Integrated knowledge database enables definition of new decision trees if a user has the need to store specific knowledge in the identification of risk sources that are characteristic for a particular business system.

The RMS software solution for risk management contains several modules:

1. Home page
2. Information
3. Master data
 - a. Responsible persons (internal experts)
 - b. Expert team (external)
 - c. Structures
 - d. Organizational structure
 - i. Hierarchical structure of processes
 - ii. Hierarchical structure of strategic objectives
 - iii. Hierarchical structure of business areas
 - iv. Hierarchical structure of different risk groups
4. Project Management (management of tasks)
5. The Kinney Method
6. Risk-Based Inspections (API 580 and similar)
7. Questionnaires/Models
8. Hazards
9. Elements of analysis (Elements of risk matrices, Risk calculation, etc.)
10. Risks Register
 - a. New risk
 - b. List of risks
 - c. Risk cards
 - d. Registers
11. Risk Reports and Analysis
12. Detailed report
 - a. Occupancy overviews
 - b. Risk Score list (risks structured from largest to smallest (or by other criteria))
 - c. Ie-factor (Investment effectiveness) analysis
13. Administration
14. Logout

3.1. RMS Architecture

RMS architecture characteristics are:

- The system supports the parallel simultaneous cooperative work of many users with the same and simultaneous parallel sessions with independent and shared data warehouses;
- The system supports execution on virtual machines;

- The system is not limited by the number of entities and the amount of data processed other than the hardware resources involved, and the limitations of the RDBMS used.

Conceptual design is based on a Web-based solution, with data in a SQL database and the knowledge base in separate repository with separate modules for reporting and analysis.

Architecture layers are, Figure 2:

- Client layer—any web-enabled devices, single page application (Blazor)—Web application with interactive user interface;
- Business layer—server, .NET 8, Rest API logic services;
- Data layer—server, MS SQL server/PostgreSQL server, Windows/Linux;
- Questionnaire layer/knowledge base—file server, Windows/Linux, Server part: Rest API: Microsoft .NET 8, DB: MS SQL server, optional PostgreSQL. Client part: Blazor WebAssembly, optional Blazor Server.

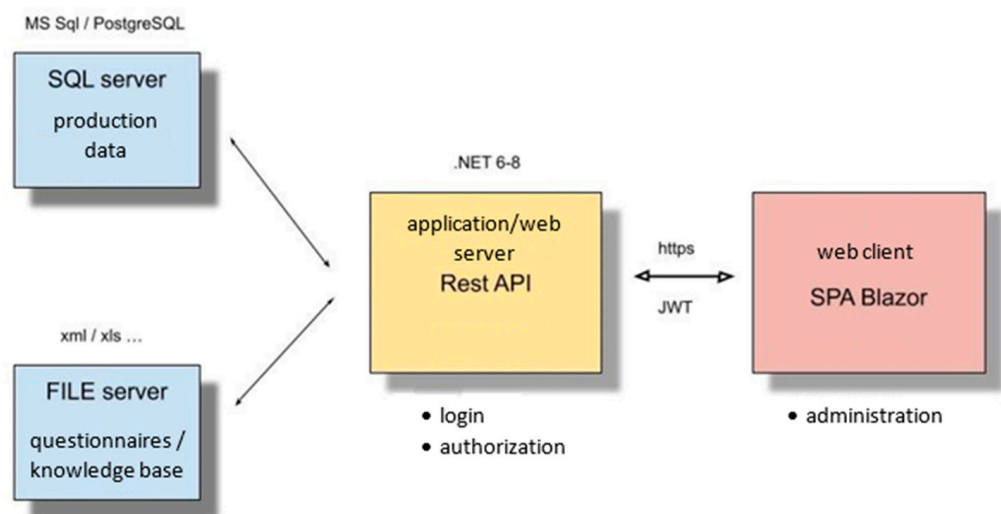


Figure 2. Architecture of the software solution.

The separation of the knowledge base and a SQL-based data repository was necessary due to the management and protection of expert models and questionnaires, the application of cryptographic methods and securing the right of use for individual files. The strict division of responsibilities to different components of the software system, and the use of a relational database, enable multitasking work and ensure the high elasticity and scalability of the system. In this way, the modular architecture enables the introduction of new functionalities and the application of cutting-edge technologies without the need for changes in other parts of the system.

3.2. Knowledge Database

Knowledge in software solution RMS version 0.955.230725 is located in different questionnaires for the following 52 business areas, to name a few:

- Safety and health at work;
- Business risks;
- COSO framework [28];
- Investments;
- Security risks;
- Managing environmental responsibilities according to the ISO 14000 [29] standard
- Workplace (safety) risks;
- Information security management systems according to the ISO 27000 [30] standard;
- Food safety management systems according to the ISO 22000 [31] standard;

- Occupational safety and health management systems according to the ISO 45001 standard [32];
- SEVESO standard [33] and others.

Some of the presented business areas have several questionnaires (for example, the ISO 14000 standard has a questionnaire for documentation, for communication, for leadership, planning, support, change management, etc.).

For the storage of knowledge in the mentioned areas, the representation of knowledge using IF THEN production rules was used. By using production rules for certain areas, knowledge is stored in the form of a decision tree, while for other areas a decision network is generated. External experts, based on their know-how, define possible hazards that may appear through appropriate questionnaires. Internal experts, based on their knowledge of circumstances in the organization define the risks that may appear through questionnaires or via direct entering into the system. Figure 3 shows the process of building a decision tree in the RMS software tool. Depending on the nature of the observed topic, some questionnaires have about 50 questions in the interactive process with the user, while some questionnaires have up to 245 questions. In questionnaires, a question can have minimum of two alternative answers (Yes, No), while some questions have seven alternative answers.

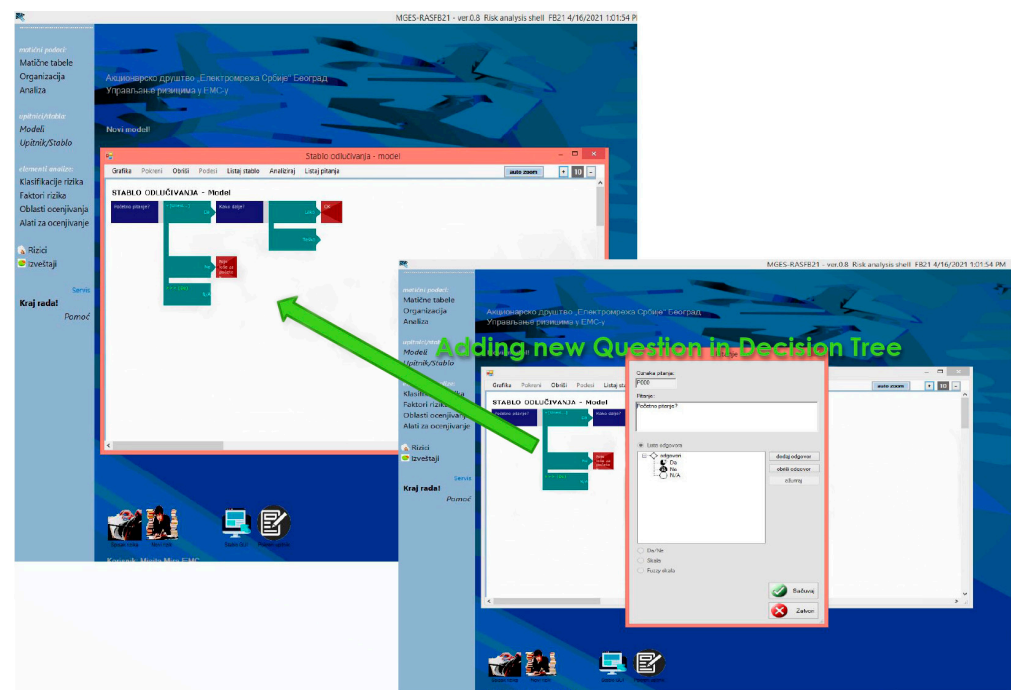


Figure 3. Knowledge database design [34].

Figure 4a shows the interface when the user interacts with the questionnaire for the “Safety and health at work” business area. During the interaction with the expert system, a user sees the numbered question, offered answers, and the user can stop the interview process at any time and continue later from the current question.

Figure 4b shows a part of the generated hazards database that comes from filling in the questionnaire by the user. These hazards represent potential risks, and their translation into the risk database is enabled only after the RMS software user confirms that it is indeed a risk (Figure 4b, new risk label). In this way, overloading of the risk register with records representing identified hazards that do not present a significant risk to the observed company is prevented. The last column in the hazard database (Figure 4b) represents the number of related risks, because one hazard can be related to several types of risks (for example, an oil pipeline leak can be related to a risk related to environmental protection and asset management (financial) risks or even reputational one).

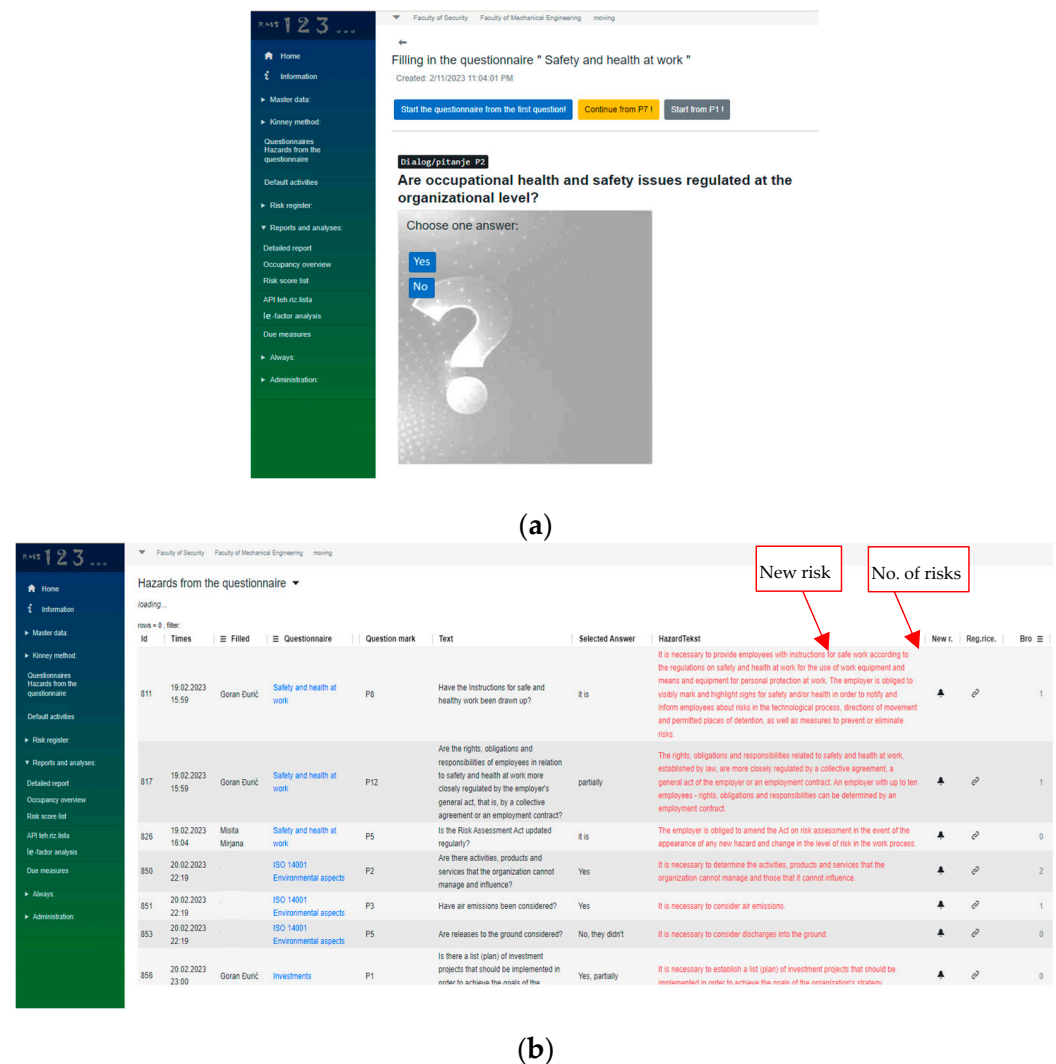


Figure 4. (a) Questionnaire—interaction with use; (b) generated hazard database as a result of questionnaire inputs.

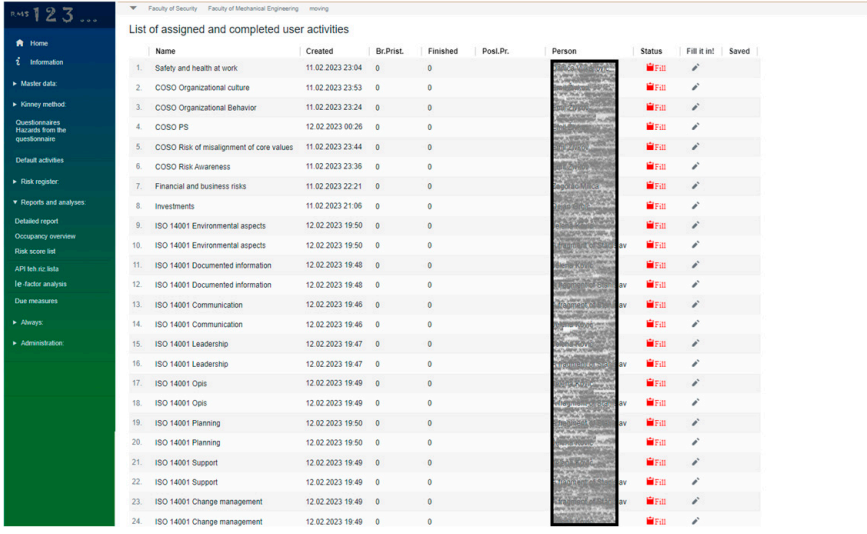
3.3. Project Management

Project management in the process of identification, classification, prescription of risk mitigation or elimination measures, and risk assessment is a complex task with the following characteristics:

- Linking the respondent's ID to the appropriate questionnaire, so that the user can have an overview of unfinished tasks when logging in to the RMS software.
- More than one user must fill out the same questionnaire (for example, in the specific example we had four people in charge of fire protection), which indicates that it is necessary to prevent the duplication of hazards in the hazard database, but also to save all respondents' answers.

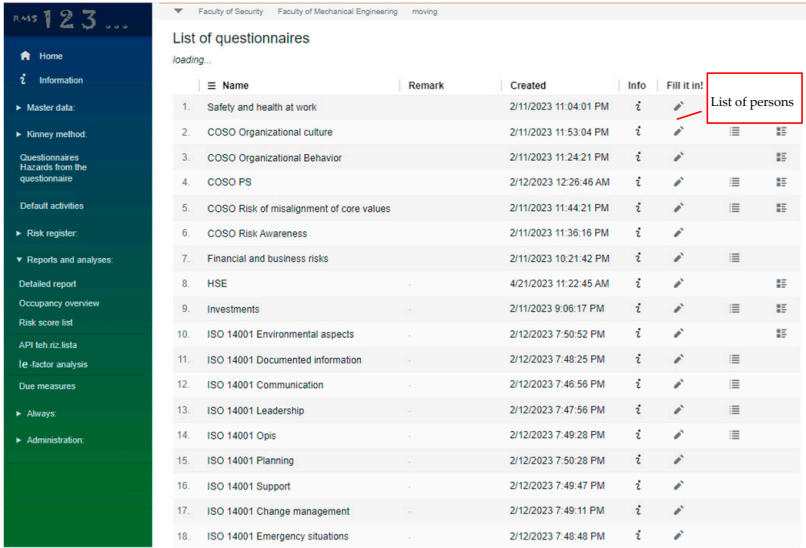
Figure 5 shows the task management, the name of the questionnaire and the person who needs to fill in the questionnaire, with an overview of the status and report of completing the questionnaire.

In the list of questionnaires, Figure 5b, we have an overview of the persons responsible for filling out each questionnaire and a direct link to the answers entered by the responsible persons in the RMS system. All screen displays (Figures 4b and 5a,b) can be sorted by any column or searched by name, which facilitates the process of managing individual questionnaires and respondents' answers.



Name	Created	Br.Priat.	Finished	Post.Pc.	Person	Status	Fill it in!	Saved
1. Safety and health at work	11.02.2023 23:04	0	0			Full		
2. COSO Organizational culture	11.02.2023 23:53	0	0			Full		
3. COSO Organizational Behavior	11.02.2023 23:24	0	0			Full		
4. COSO PS	12.02.2023 00:26	0	0			Full		
5. COSO Risk of misalignment of core values	11.02.2023 23:44	0	0			Full		
6. COSO Risk Awareness	11.02.2023 23:36	0	0			Full		
7. Financial and business risks	11.02.2023 22:21	0	0			Full		
8. Investments	11.02.2023 21:06	0	0			Full		
9. ISO 14001 Environmental aspects	12.02.2023 19:50	0	0			Full		
10. ISO 14001 Environmental aspects	12.02.2023 19:50	0	0			Full		
11. ISO 14001 Documented information	12.02.2023 19:48	0	0			Full		
12. ISO 14001 Documented information	12.02.2023 19:48	0	0			Full		
13. ISO 14001 Communication	12.02.2023 19:46	0	0			Full		
14. ISO 14001 Communication	12.02.2023 19:46	0	0			Full		
15. ISO 14001 Leadership	12.02.2023 19:47	0	0			Full		
16. ISO 14001 Leadership	12.02.2023 19:47	0	0			Full		
17. ISO 14001 Opis	12.02.2023 19:49	0	0			Full		
18. ISO 14001 Opis	12.02.2023 19:49	0	0			Full		
19. ISO 14001 Planning	12.02.2023 19:50	0	0			Full		
20. ISO 14001 Planning	12.02.2023 19:50	0	0			Full		
21. ISO 14001 Support	12.02.2023 19:49	0	0			Full		
22. ISO 14001 Support	12.02.2023 19:49	0	0			Full		
23. ISO 14001 Change management	12.02.2023 19:49	0	0			Full		
24. ISO 14001 Change management	12.02.2023 19:49	0	0			Full		

(a)



Name	Remark	Created	Info	Fill it in!	List of persons
1. Safety and health at work		2/11/2023 11:04:01 PM			
2. COSO Organizational culture		2/11/2023 11:53:04 PM			
3. COSO Organizational Behavior		2/11/2023 11:24:21 PM			
4. COSO PS		2/12/2023 12:26:46 AM			
5. COSO Risk of misalignment of core values		2/11/2023 11:44:21 PM			
6. COSO Risk Awareness		2/11/2023 11:36:16 PM			
7. Financial and business risks		2/11/2023 10:21:42 PM			
8. HSE		4/21/2023 11:22:45 AM			
9. Investments		2/11/2023 9:06:17 PM			
10. ISO 14001 Environmental aspects		2/12/2023 7:50:52 PM			
11. ISO 14001 Documented information		2/12/2023 7:48:25 PM			
12. ISO 14001 Communication		2/12/2023 7:46:56 PM			
13. ISO 14001 Leadership		2/12/2023 7:47:56 PM			
14. ISO 14001 Opis		2/12/2023 7:49:28 PM			
15. ISO 14001 Planning		2/12/2023 7:50:28 PM			
16. ISO 14001 Support		2/12/2023 7:49:47 PM			
17. ISO 14001 Change management		2/12/2023 7:49:11 PM			
18. ISO 14001 Emergency situations		2/12/2023 7:48:48 PM			

(b)

Figure 5. (a) Task management; (b) List of questionnaires.

3.4. COSO Framework

In 2023, the Committee of Sponsoring Organizations of the Treadway Commission (COSO) Internal Control—Integrated Framework (originally issued in 1992) issued supplemental guidance for organizations to achieve effective internal control over sustainability reporting (ICSR) [28]. One of the key principles in the COSO framework is the connection of different hierarchical structures (organizational units) with organizational goals and related risks, in order to monitor progress in mitigating or eliminating risks according to defined elements of hierarchical structures and consequently achieving goals. In the RMS software solution, therefore, it is possible to set the necessary number of hierarchical structures, such as the following examples: organizational, process, strategic goals, activities, risk groups, business units, or others. The addition of a new structure is enabled by entering it from an Excel file. Figure 6a shows a list of defined hierarchical structures in the example of the company from the petroleum industry, while Figure 6b,c shows a more detailed organizational and process structure.

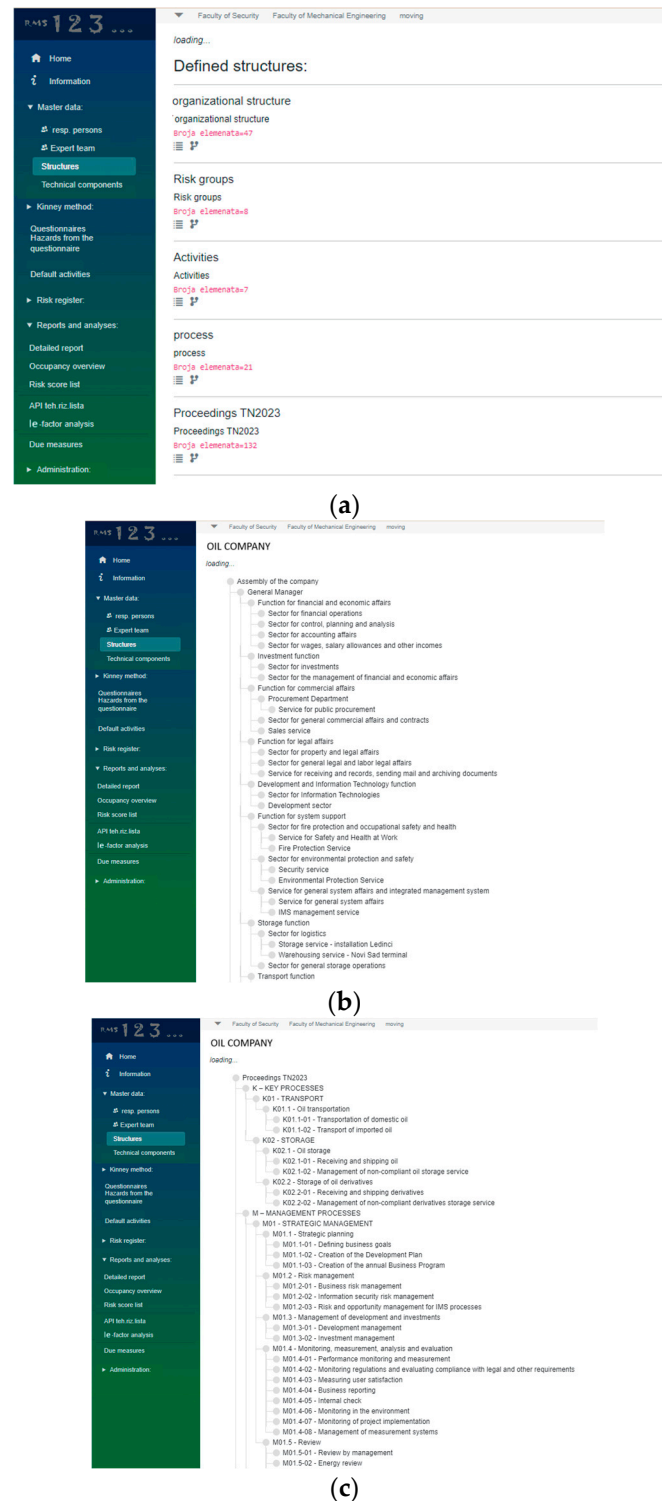


Figure 6. (a) Structures; (b) Organizational structure (c) Processes structure.

3.5. Risk Assessment

The process of risk management is represented in Figure 7a. It starts with entering basic risk data, such as risk name, type of risk (risk to be assessed, risk that is recorded and not evaluated, opportunity, etc.), linked hazards, risk description, risk source, date, risk owner, organ of escalation, etc. The basic data risk card has additional optional cards, including: risk classification card (Figure 7b), connections with elements of structures (Figure 8a), consequences (Figure 8b), measures (Figure 9a), and assessments (Figure 9b).

External and internal experts perform a team risk assessment while also training internal experts and improving the quality of the output. In this way, the experience of external experts is incorporated into the risk register while simultaneously improving the know-how of internal experts.

Figure 7b shows a risk classification card in detail. Classifications can be made according to the following criteria: zone of influence, level of influence, time of influence, manageability, type, and influence on the mission and vision of the company. Each of the listed categories contains several descriptive options in the drop-down menus. Figure 8a shows the connections between the observed risk and the defined elements of the hierarchical structures (COSO framework). One risk can be associated with one or more elements within each of the defined hierarchical structures and vice versa.

Figure 8b shows the consequence card. One risk can have several consequences, and a more detailed description can be entered in the RMS for each consequence. The card related to Measures (Figure 9a) is one of the more complex cards set up for each risk. It is necessary to point out that one risk can have one or more actions to reduce, mitigate, or eliminate the observed risk. For each recommended action to mitigate or eliminate the observed risk, this card defines:

- the name of the action;
- the description of the action;
- the deadline for the implementation of the recommended action;
- the costs of implementing the recommended action; the start of action (pre- or post-event);
- method of action (whether it is for the purpose of reducing the consequences, or for the purpose of preventing, ignoring, urgent reaction, control, etc.);
- verification period;
- evaluation of the effectiveness of the measure (highly reliable, reliable, partially reliable, insufficiently reliable);
- the date when the measure was implemented;
- and the status of the action (whether it is recommended, approval in progress, approved, implementation in progress, realized, risk transfer limited or impossible to be influenced by the organization).

Based on the entered data on the costs of the implementation of the recommended actions, it is possible to conduct later a Ie-factor (Investment effectiveness) analysis, on the basis of which we conduct the prioritization of risks by the effectiveness of mitigating actions.

(a)
(b)

Figure 7. (a) Risk basic data; (b) Risk classification.

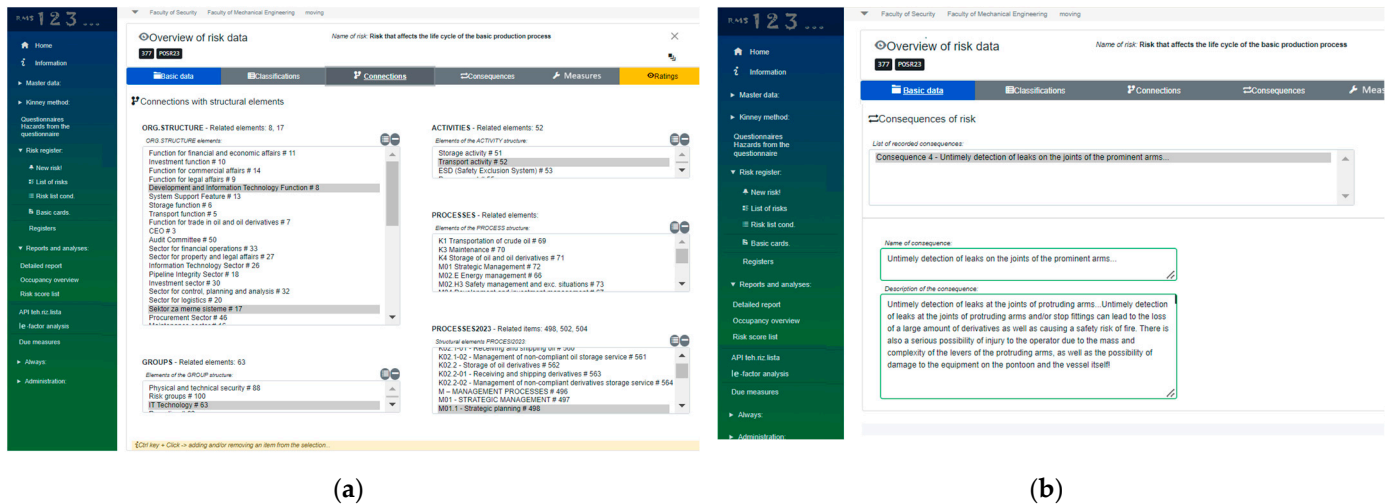


Figure 8. (a) Connections with structures; (b) Consequences.

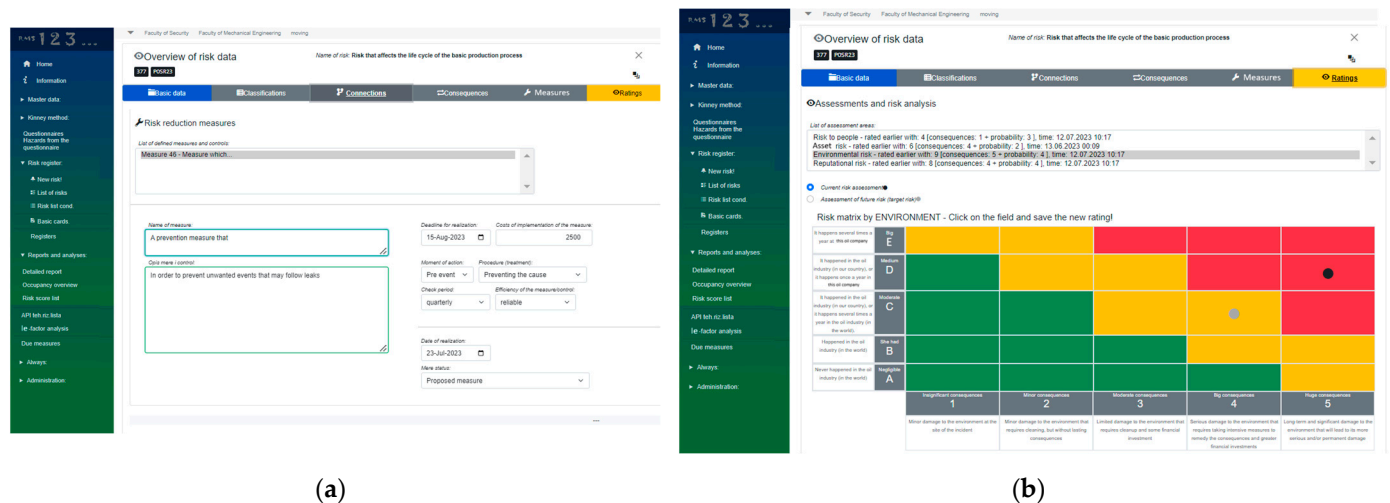


Figure 9. (a) Measures; (b) Risk assessment.

Figure 9b shows the risk assessment card. The observed risk can be evaluated using four risk matrices, namely: risk to people (safety), risk to the environment, risk to property (assets), and risk to the reputation of the observed organization. Categorization by the x- and y-axes on these four matrices is different taking into account the different nature of the consequences. For example, for the safety risk matrix, the consequences are as follows: grade 1—minor injuries or health effects, grade 2—minor injuries or health effects, grade 3—severe injuries or health effects, grade 4—permanent disability, grade 5—death accident or serious injury (Figure 8b).

Figure 10 shows the risk matrices per asset type of risk. These risk matrices differ from the other three matrices because they contain a financial assessment of the potential damage in the event of an undesirable event, as well as a financial assessment of costs for the implementation of the recommended actions to mitigate or eliminate the observed risk. All four built-in matrices in the RMS software solution (number of matrices is not limited) contain an assessment of the current state (black dot in Figures 9b and 10) and a risk assessment of the future state (gray dot in Figures 9b and 10), which represents the risk after applying the proposed actions and mitigating or eliminating the observed risk.

The assessment of the current level of risk and the future level of risk for all matrices is useful information for the decision-maker in the sense that he can assess the effectiveness of investing in recommended actions for risk mitigation or elimination. On the basis of the above information, an Ie-factor (Investment effectiveness) analysis is carried out, based on

which risks are prioritized in relation to the effectiveness of the recommended actions for risk mitigation or elimination.

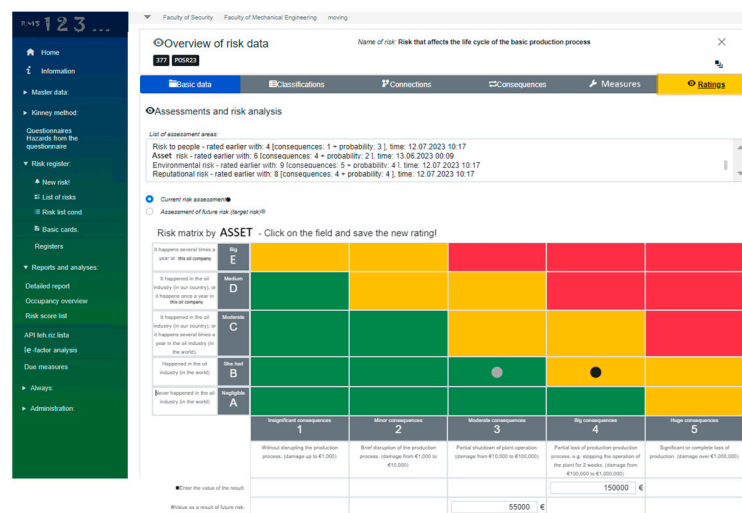


Figure 10. Risk matrices for assets (financial).

3.6. Supporting Methodologies (Tools)

As shown in the previous chapter, one of the built-in risk assessment methodologies in the RMS software is the risk matrices adaptation tool that can be customized according to the specific organization risk appetite. First of all, it is necessary to hold a workshop in the company where the risk appetite and the basic characteristics of the risk matrix are determined. The risk appetite of an organization can be presented in different ways. Some organizations can describe their risks with a 2×2 matrix, and some want a more precise way of determining the risks value using matrices that can be 5×6 (the maximum known in practice). Columns and rows in matrices describe probabilities and consequences. The more there are, the more precisely the risks can be categorized. Each of them has its own descriptive and quantitative values. Also, the heat map provides a basis for decision-making in each organization separately. In order to allow each organization to express its appetite for risks, a piece of software has been created that enables this. Consequently, that matrix is used in the case of all types of risks in order to obtain a total/partial risks portfolio and to combine different risk assessment techniques. If the same risk matrix is used for all risks, then they can be prioritized in the same risk portfolio based on their Risk Score. In general, for different companies, risk matrices must be adjusted in terms of x and y scaling and in relation to the specific ALARP zone and heat map to represent their specific risk appetite. The scalability of matrices is one of the advantages of RMS compared to similar ERM solutions.

However, it is not convenient to assess the risk of the workplace (health and safety) according to risk matrices. Having that in mind, the Kinney method is adopted in most companies as an acceptable methodology for these risks. Therefore, a special module for the purposes of risk assessment of workplaces is built into RMS based on the Kinney method, as shown in Figure 11.

The questionnaire for workplace risk assessment contains 64 questions and the categories, which are as follows: Consequences, Probability, and Frequency according to the Kinney methodology.

RMS for technical equipment uses a qualitative approach to RBI risk inspection and assessment to examine refinery and petrochemical operations for process hazards associated with pressure equipment integrity, according to API 580 and the 581 standard. The qualitative approach is less detailed than the quantitative analysis, and is far less time consuming, but provides a basis for prioritizing a risk-based inspection program (API 581). In the case of a company in the petroleum industry, the technical equipment which

was examined by this methodology in RMS were as follows: pipeline classes API-5L-X42 and C 1212 with a diameter of 168.3 mm, underground tanks, vertical cylindrical tanks, overflow tanks, fuel pumps, pontoon fuel pumps, safety valves on the pipeline, breather safety valves for tanks, line pumps, booster pumps, water pumps, and other equipment. RMS also contains methodology for so-called Level 1 risk assessment for thermal power plants.

Figure 11. Assessment of workplace (health and safety) risks using the Kinney method.

Figure 12 shows the risk assessment using a qualitative approach according to the API 581 standard on the example of an atmospheric tank.

Figure 12. API 581 methodology for technical risks.

- Ie-factor < 1—these results are colored red (in Figure 14), and they indicate that the recommended measures are more expensive than the difference between the future risk value, and that it is not profitable to invest in these mitigating activities.

Ie-Factor
row = 109, filter:
Current risk Consequences= 58,242,895.00 Value= 4,710,504.05 Risk due to Consequences= 18,338,513.00 Value= 4,553,678.50 Risk reduction= -1,914,874.45 Measure costs= 2,720,967.00
Current risk Consequences= 216,000.00 Value= 73,500.00 Risk due to Consequences= 56,500.00 Value= 4,250.00 Risk reduction= 69,250.00 Measure costs= 8,780.00

ID	Register	Name	Datum	Rtc	RtcVed	Rtp	RtpVed	R1 fin	PC	R2Ved	R2p	R2Ved	R2fin	DecreaseR	MeritTroskov	Factor
601	POSIR23		28.06.2023	2	5500	5	1.000	5500,000	1	500	5	1.000	500,000	5000,000	130	38.402
607	POSIR23		01.07.2023	3	55000	5	1.000	55000,000	1	500	5	1.000	500,000	54500,000	3000	18.167
377	POSIR23		25.04.2023	4	150000	2	0.050	7500,000	3	55000	2	0.050	2750,000	4750,000	2650	1.792
603	POSIR23		29.06.2023	2	5500	5	1.000	5500,000	1	500	5	1.000	500,000	5000,000	3000	1.667
376	POSIR23		25.04.2023	3	10001	2	0.050	500,050	2	5500	1	0.001	5,500	494,550	590	0.638
659	TEHR23		21.07.2023	3	90000	3	0.100	9000,000	3	11000	3	0.100	1100,000	7900,000	15000	0.527
660	TEHR23		21.07.2023	3	90000	3	0.100	9000,000	3	11000	3	0.100	1100,000	7900,000	15000	0.527
663	TEHR23		24.07.2023	3	40000	3	0.100	4000,000	3	30000	3	0.100	3000,000	1000,000	5000	0.200
664	TEHR23		24.07.2023	3	40000	3	0.100	4000,000	3	30000	3	0.100	3000,000	1000,000	5000	0.200
665	TEHR23		24.07.2023	3	40000	3	0.100	4000,000	3	30000	3	0.100	3000,000	1000,000	5000	0.200

Figure 14. Ie-Factor Analysis.

The Management System Factor is one of the API 581 risk-based inspection technology procedures for management system evaluation. This is done with the help of questionnaires from API 581, which serve as an additional recording of the situation in a certain organization. It is a powerful tool for determining technical risks, but it also generally speaks about the state of an organization according to several criteria. Figure 15 shows an example of MSF analysis realization in the RMS software solution.

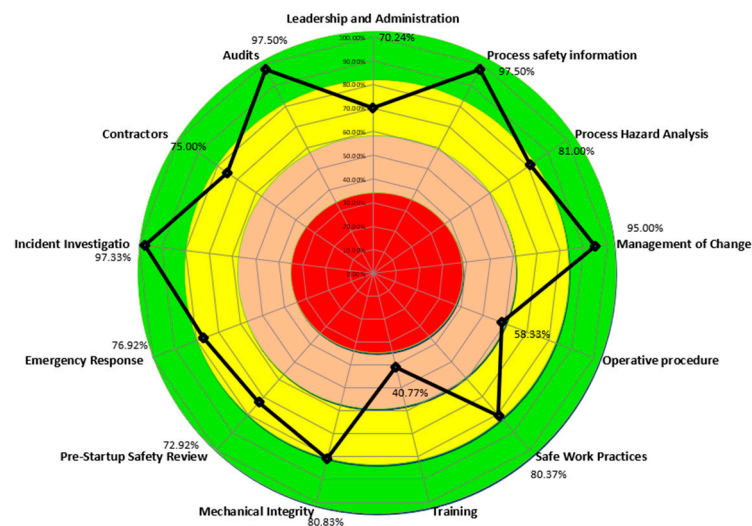


Figure 15. Management System Factor Analysis.

4. Discussion

The advantages of using RMS software solutions are online management of project tasks in terms of risk identification, risk calcification, and entering/updating lists of consequences and mitigation measures, as well as risk assessments. In addition, RMS enables the application of different methodologies for risk assessment depending on the type of observed risks: Risk score analysis is useful because of its ability to assess the future and current value of the observed risk; Ie-factor analysis is helpful thanks to the financial

assessment of the value of the recommended mitigation actions; the overall prioritization of risks based on the COSO framework by elements of hierarchical structures yields valuable insights. The application of risk scores and Ie-factor analysis is very useful as well. There are legal regulations that prescribe the application of certain methods, such as the Kinney method, the application of which is mandatory, at least in Serbia. European (EN), ISO, or similar industrial standards, such as API, are widely accepted in practice. This is the reason that their application is built into the software. Among the advantages of RMS we can mention is that RMS supports different approaches in risk assessment thanks to an integral database in which all risks are located. The advantage of RMS is the scalability of the risk matrix, which facilitates the adaptation of this solution. Cyber security is ensured by data encryption and two servers in the enterprise (one for filtration, verification, and protection) for increased data security. RMS uses a secure version of the http protocol, i.e., https, and authentication is performed on the server side and not only on the client side. Cyber security could be improved by introducing multi-factor authentication and homomorphic encryption.

Customizing the software usually requires making invasive changes to the application code, which means additional costs and additional risks are involved. Therefore, a configuration approach is used, and through the data structures that are part of the system, we enable changes in the behavior of the software and its adaptation to different requirements. Application behavior is data-driven, which positively affects durability and suitability for different organizations. Broad applicability is ensured by the high degree of generality of comprehensive software solutions, and customization relies on entered data that defines the specifics of each individual organization, and this does not require changing the source code.

Problems between internal and external experts can arise for two reasons: (a) gaps in knowledge about possible risks and (b) gaps in knowledge about specific risks of the organization. Filling out a questionnaire or applying one of the quantitative methods is the first step in risk analysis in this case. The next step is the collaboration of internal and external experts, which is described in Section 3.5. Risk assessment. They should work together to overcome any problems that may arise. All available standards indicate that risk analysis must primarily be a team process.

Further development of RMS involves the implementation of machine learning algorithms in order to improve the processes of risk identification, risk classification, identification of possible consequences, definition of the list of mitigation measures, and risk assessments. However, in order to add ML it is necessary to have a sufficient set of previously entered data.

5. Conclusions

The paper presents an innovative methodology for managing company risks based on the integration of the COSO framework, ISO 31000, and many other technical and organizational standards with work with knowledge bases, project management, and the application of different methodologies for the identification, classification, and assessment of current and future risks for different business areas. The essence of the innovation of the RMS solution is in the joint and parallel use of the COSO framework, ISO 31000 standard, API 580 standard, and other applicable standards and mythologies with some elements of AI (expert knowledge in the databases). The main idea of the COSO framework is to link the organization's goals with risks. Namely, each part of the organization should have goals that it must achieve, as well as others specific to itself. Failure to achieve goals is a risk to the organization. Organizational units fit into hierarchically higher organizational units. The risks of a hierarchically higher organizational unit include the risks of lower units, but they also have some specific risks of their own. Only by looking at all the organizational parts and their hierarchy can one get an idea of the risks that they carry with them and manage them according to the needs of the different levels and parts of the organization.

The presented business risk management concept was implemented by designing the software solution RMS version 0.955.230725, which was implemented in two companies the fields of public transportation and the petroleum industry. The existing version of RMS is suitable for implementation in similar companies that deal with transportation, storage, and energy production, as well as for other processing companies.

Author Contributions: Conceptualization, P.S., M.M. (Mirjana Misita) and G.Đ.; data curation, M.M. (Mladen Milošević) and B.K.; formal analysis, D.B. and P.S.; software, P.S., M.M. (Mirjana Misita) and G.Đ.; supervision, M.M. (Mladen Milošević), B.K., D.B. and P.S.; validation, G.Đ.; visualization, G.Đ.; writing—original draft, P.S. and M.M. (Mirjana Misita); writing—review and editing, P.S. and M.M. (Mirjana Misita). All authors have read and agreed to the published version of the manuscript.

Funding: This research was supported by the Science Fund of the Republic of Serbia within its program “IDEAS”—Management of New Security Risks—Research and Simulation Development, NEWSIMR&D, #7749151.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: The raw data supporting the conclusions of this article will be made available by the authors on request.

Conflicts of Interest: The authors declare no conflicts of interest.

References

1. Addo-Tenkorang, R.; Helo, P. Enterprise Resource Planning (ERP): A Review Literature Report. In Proceedings of the World Congress on Engineering and Computer Science 2011—WCECS 2011, San Francisco, CA, USA, 19–21 October 2011; Volume II.
2. Giambona, E.G.; John, R.; Harvey, C.R.; Bodnar, G.M. The Theory and Practice of Corporate Risk Management: Evidence from the Field. *Financ. Manag.* **2018**, *47*, 783–832. [\[CrossRef\]](#)
3. Merna, T.; Faisal, A.T. *Corporate Risk Management an Organizational Perspective*; John Wiley & Sons Ltd.: Hoboken, NJ, USA, 2015.
4. Yun, J. The effect of enterprise risk management on corporate risk management. *Financ. Res. Lett.* **2023**, *55*, 103950. [\[CrossRef\]](#)
5. Mahmood, A.; Lloyd, M. ERP System Implementation in Large Enterprises—A Systematic Literature Review. *J. Enterp. Inf. Manag.* **2017**, *30*, 666–692. [\[CrossRef\]](#)
6. Malik, S.A.; Holt, B.; Freeman, J. Enterprise Risk Management (ERM): A New Way of Looking at Risk Management at an Organisational Level. In Proceedings of the EURO XXVI, Rome, Italy, 16–24 March 2013.
7. Francisku, A.A.; Ridwan, H.; Kevin, B.S. The State-of-The-Art of Enterprise Risk Management Maturity Models: A Review. *Ann. RSCB* **2021**, *25*, 4005–4014, ISSN: 1583-6258.
8. Mahmood, F.; Zahid, A.H. ERP issues and challenges: A research synthesis. *Kybernetes* **2019**, *49*, 629–659. [\[CrossRef\]](#)
9. Fraser, J.; Simkins, B. The challenges of and solutions for implementing enterprise risk management. *Bus. Horiz.* **2016**, *10*, 689–698. [\[CrossRef\]](#)
10. Abrams, C.; von Känel, J.; Müller, S.; Pfitzmann, B.; Ruschka-Taylor, S. Optimized Enterprise Risk Management. *IBM Syst. J.* **2007**, *46*, 219–234. [\[CrossRef\]](#)
11. Stefanou, C.J. A framework for the ex-ante evaluation of ERP software. *Eur. J. Inf. Syst.* **2001**, *10*, 204–215. [\[CrossRef\]](#)
12. Valashani, M.A.; Abukari, A.M. ERP Systems Architecture for The Modern Age: A Review of the State of the Art Technologies. *J. Appl. Intell. Syst. Inf. Sci.* **2020**, *1*, 70–90. [\[CrossRef\]](#)
13. Söderholm, P.; Karim, R. An Enterprise Risk Management framework for evaluation of eMaintenance. In Proceedings of the 1st International Workshop and Congress on eMaintenance, Luleå, Sweden, 22–24 June 2010; ISBN 978-91-7439-120-6.
14. Mohamed, A.A.E.; Eman, N.; Mervat, H.G. Benefits and challenges of cloud ERP systems—A systematic literature review. *Future Comput. Inform. J.* **2016**, *1*, 1–9. [\[CrossRef\]](#)
15. Mohamed, S.S.; Abdulkader, A. A new comprehensive framework for enterprise information security risk management. *Appl. Comput. Inform.* **2011**, *9*, 107–118.
16. Louis, A.C. What’s Wrong with Risk Matrices? *Risk Anal.* **2008**, *28*, 497–512.
17. Arena, M.; Arnaboldi, M.; Azzone, G. Is enterprise risk management real? *J. Risk Res.* **2011**, *14*, 779–797. [\[CrossRef\]](#)
18. Bromiley, P.; McShane, M.; Nair, A.; Rustambekov, E. Enterprise Risk Management: Review, Critique, and Research Directions. *Long Range Plan.* **2015**, *48*, 265–276. [\[CrossRef\]](#)
19. Essex, D.E. The black art of risk. *PM Netw.* **2005**, *19*, 88–92.
20. Patterson, T. *The Use of Information Technology in Risk Management*; IBM Corporation: Austin, TX, USA, 2015; Available online: <https://www.aicpa-cima.com/FRC> (accessed on 1 October 2024).
21. Pandey, S.K.; Mustafa, K. A Comparative Study of Risk Assessment Methodologies for Information Systems. *Bul. Tek. Elektro Inform.* **2012**, *1*, 111–122, ISSN 2089-3191. [\[CrossRef\]](#)

22. Mitterbauer, P.; Pesendorfer, J.; Schmidinger, E. Opportunities and risks of IT solutions for ERM, ACRN Oxford. *J. Financ. Risk Perspect.* **2016**, *5*, 15–29.
23. Dikmen, I.; Birgonul, M.T.; Arikan, A.E. A critical review of risk management support tools. In Proceedings of the 20th Annual ARCOM Conference, Edinburgh, UK, 1–3 September 2004; Khosrowshahi, F., Ed.; Heriot Watt University: Edinburgh, UK, 2014; Volume 2, pp. 1145–1154.
24. Khan, M.A.; Khan, S.; Sadiq, M. Systematic Review of Software Risk Assessment and Estimation Models. *Int. J. Eng. Adv. Technol.* **2012**, *1*, 298–305, ISSN: 2249-8958.
25. *API 580; Risk-Based Inspection*, 2nd ed. American Petroleum Institute: Washington, DC, USA, 2016.
26. *API 581; Risk-Based Inspection Methodology*, 3rd ed. American Petroleum Institute: Washington, DC, USA, 2020.
27. *ISO 31000 Series; Risk Management*. ISO: Geneva, Switzerland, 2018.
28. Committee of Sponsoring Organizations of the Treadway Commission (COSO). *Enterprise Risk Management—Integrated Framework*; Pricewaterhouse Coopers LLP.: Birmingham, AL, USA, 2004.
29. *ISO 14000 Series; Environmental Management*. ISO: Geneva, Switzerland, 2015.
30. *ISO/IEC 27000 Series; Information Security Management Systems*. ISO: Geneva, Switzerland, 2018.
31. *ISO 22000 Series; Food Safety Management Systems*. ISO: Geneva, Switzerland, 2018.
32. *ISO 45000 Series; Occupational Health and Safety Management Systems*. ISO: Geneva, Switzerland, 2018.
33. European Union. *Directive 2012/18/EU of the European Parliament and of the Council of 4 July 2012 on the Control of Major-Accident Hazards Involving Dangerous Substances (Seveso III)*; European Union: Maastricht, The Netherlands, 2012; Available online: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32012L0018> (accessed on 1 October 2024).
34. Stanojevic, P.; Misita, M.; Djuric, G. Software System for Risk Management Based on Artificial Intelligence. In Proceedings of the Second Memorial Scientific Conference “Predrag Maric”, Belgrade, Serbia, 20 March 2023; pp. 144–154, ISBN 987-86-80144-63-4.

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.