

Article

Not peer-reviewed version

---

# Novel Approach to Conceptual Design of Enterprise Risk Management Software

---

[Petar Stanojevic](#)\*, [Mirjana Misita](#), Goran Đurić, Bogdan Kuzmanović, Mladen Milošević, Daniel Balos

Posted Date: 25 October 2024

doi: 10.20944/preprints202410.1993.v1

Keywords: eneterprise risk management; software solution; hazard; risk managament



Preprints.org is a free multidiscipline platform providing preprint service that is dedicated to making early versions of research outputs permanently available and citable. Preprints posted at Preprints.org appear in Web of Science, Crossref, Google Scholar, Scilit, Europe PMC.

Copyright: This is an open access article distributed under the Creative Commons Attribution License which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

*Article*

# Novel Approach to Conceptual Design of Enterprise Risk Management Software

Petar Stanojevic <sup>1,\*</sup>, Mirjana Misita <sup>2</sup>, Goran Đurić <sup>2</sup>, Bogdan Kuzmanović <sup>3</sup>, Mladen Milošević <sup>4</sup> and Daniel Balos <sup>5</sup>

<sup>1</sup> Faculty of Security Studies, Gospodara Vučića 50 Belgrade, Serbia

<sup>2</sup> Faculty of Mechanical Engineering, Kraljice Marije 16, Belgrade, Serbia

<sup>3</sup> Faculty of Technical Science, Dositeja Obradovića 6, Novi Sad, Serbia

<sup>4</sup> Faculty of Security Studies, Gospodara Vučića 50 Belgrade, Serbia

<sup>5</sup> MPA - Materials Testing Institute University of Stuttgart, Germany

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

**Abstract:** The problem is how to create a comprehensive “tool”, applicable to any company, which will allow to achieve multiple effects at the same time, such as adhering to the ISO 31000 procedure, connecting risks and company goals in the manner defined by the COSO framework (by connecting the elements of the organizational structure with the company goals), assessment of all types of risks that a company may face, including technical, enable decision support and given visualization of data and effects. Solving this general problem requires solving many specific problems such as the creation of a specific risk matrixes for each company that will express its risk appetite but also to give the possibility of a comprehensive overview of all possible types of consequences, linking entities one-to-many and many-to-one in order to link the elements of the organizational structure to the goals that can be and common to several units, the acquisition of potential risks based on the knowledge of external experts, which overcomes the limitation of insight from the company and introduces elements of artificial intelligence, the application of standards for the evaluation of technical risks such as EN 16991 or API 580, 581 etc. while enabling the management of the implementation project and evergreening in the future. Our research question is can an integral model be made that will solve the above problems in an integrated way. The goal is to create software that will support this solution and that will be practically applicable. Solving such a complex problem of connecting various theoretical and practical aspects required creation of a special algorithm for connecting project activities, risks, organizational structure, goals, knowledge, data management and software. The algorithm, model and software were developed and successfully tested in two Serbian companies.

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

## 1. Introduction

The problem of identifying company risks, their classification, assessment, prescription of risk mitigation measures, residual risk assessment, risk prioritization, i.e., risk management is an increasingly complex task, even though there is a large number of software in the market for a holistic approach to risk management. 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 just a part 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 the development of the new organizational climate. [1–7]. Some common

methodologies used in ERM software for risk assessment include: 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 streamlined risk management processes, there are also some potential disadvantages to consider: complexity, customization requirements, data quality, overreliance of technology, resistant to change, cost, regulatory compliance challenges, cybersecurity, etc. [16–25].

Some of those disadvantages like customization to requirements, resistance to change and regulatory compliance are affecting the universality and sustainability of the 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 in 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,
- 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, 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

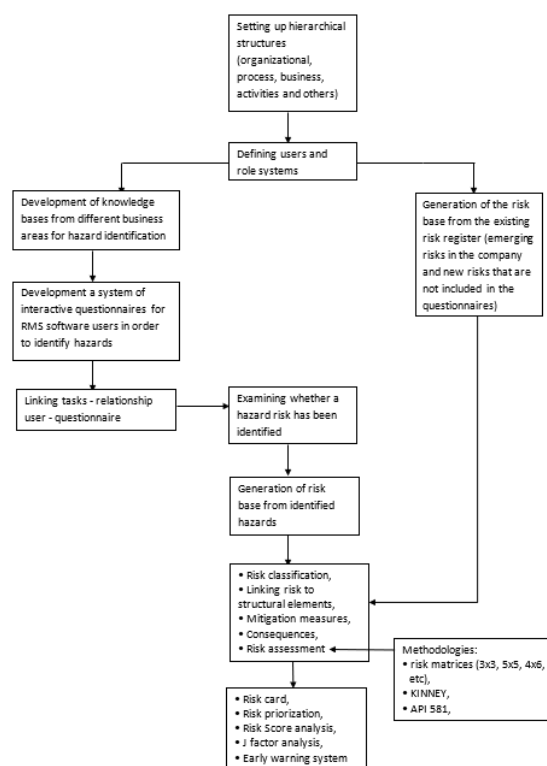
In this paper, a methodology for the design of ERM software was generated such that the software solution relies on the following principles:

- Connecting ISO 31000 and COSO framework,
- Application of expert knowledge in hazard identification,
- Connecting hazard and risk,
- Determination of risk appetite and adjustment of the risk matrix accordingly (5x5 matrices, 3x3 matrix, etc.) for as much 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:

- External experts input knowledge in database: This step involves external experts providing their insights and knowledge into a centralized database.
- 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 give possibility for internal experts to see their risks from a different angle, that is, from external expertise and the generated heuristic knowledge base.
- Hazard database is generated according to internal experts' answers: Based on the responses provided by internal experts, a hazard database is compiled or updated.
- Form this point joint team work of internal and external experts is needed to make suitable decision: Is a hazard a risk? At this juncture, there's a decision point where the experts evaluates whether a hazard identified in the database poses a risk or not.
- If Yes, then the flowchart branches out further:
  - Additional steps might include risk assessment, risk mitigation strategies, etc.
- If No, then the flowchart may lead to actions such as:
  - Further assessment to understand why it's not considered a risk.
  - Updating the hazard database accordingly.

- Closing the assessment loop.
- 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)
- Risk Management process, updating classification, updating mitigation measures, updating risk assessments, etc.
- 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.



**Figure 1.** Methodology for the design of ERM software.

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.

### 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 now called RMS software was developed by the same authors and with same leading idea - to develop a software of this kind, and was completely refurbished, has major improvements in software solutions and functionalities and was implemented in the two following projects realized in companies in the fields of Public transportation and Petroleum industry. In any case, it is a completely new author's work.

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 system,
- 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 the definition of new decision trees if a user has the need to store specific knowledge in the identification of risk sources, 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 tim (external)
  - c. Stuctures
  - d. Organisational structure
    - i. Hierarhical structure of processess
    - ii. Hierarhical structure of strategic objecitves
    - iii. Hierarhical structure of business areas
    - iv. Hierarhical 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 support the parallel simultaneous cooperative work of many users with the same and simultaneous parallel sessions with independent and shared data warehouses,
- the system support 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 Web based solution, with data in SQL database and knowledge base in separate repository with separate modules for reporting and analysis.

Architecture layers are:

- 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.

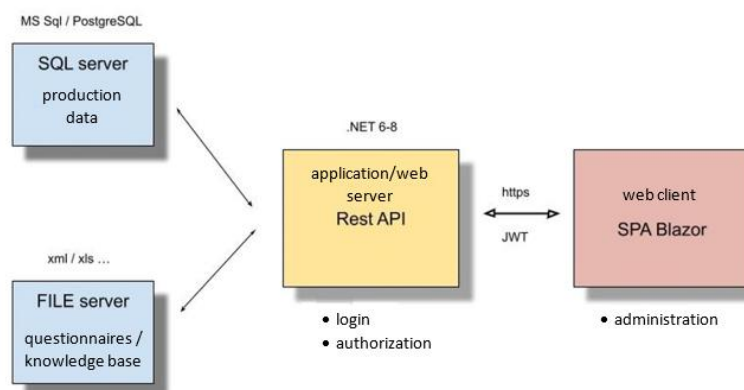


Figure 2. Architecture of the software solution.

### 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 [26],
- Investments,
- Security risks,
- Managing environmental responsibilities according to the ISO 14000 standard
- Workplace (safety) risks,
- Information security management system according to the ISO 27000 standard,
- Food safety management system according to the ISO 22000 standard,
- Occupational safety and health management system according to the ISO 45001 standard,
- SEVESO standard and others.

Some of presented business areas has 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. 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 2 at least three alternative answers (Yes, No), while some questions have 7 alternative answers.

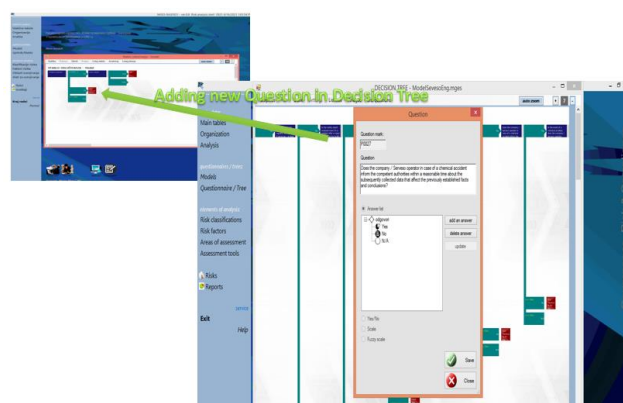


Figure 3. Knowledge database design [26].

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 latest question.

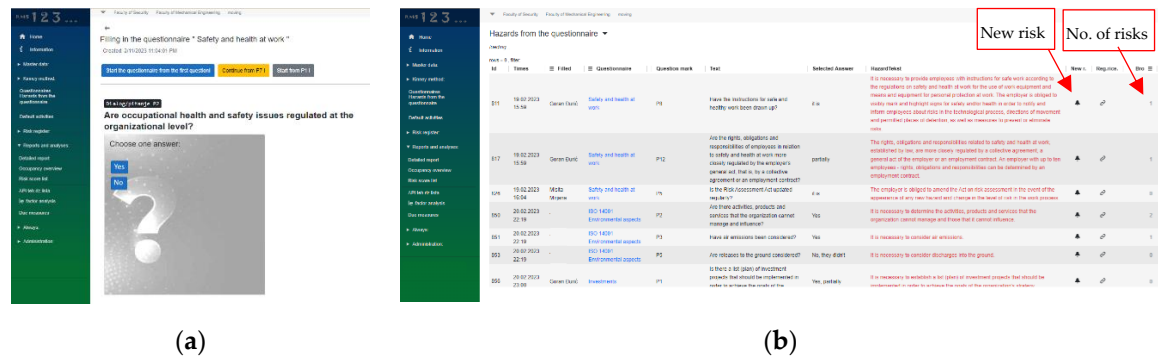


Figure 4. (a) Questionnaire – interaction with use; (b) generated hazard database as a result of questionnaire inputs.

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).

3.3. Project Management

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

- linking the respondent's ID to the appropriate questionnaire, so that the user could have an overview of unfinished tasks when logging in to the RMS software
- more than one users need to fill out the same questionnaire (for example, in the specific example we had 4 people in charge of fire protection), which indicates that it is necessary to prevent 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.

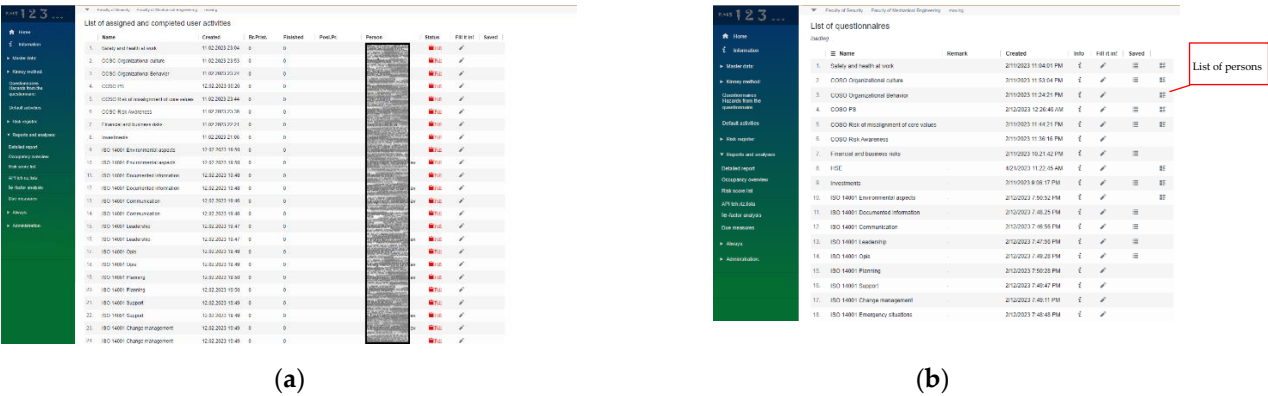


Figure 5. (a) Task management; (b) List of Questionnaires.

In the list of questionnaires, Figure 5b, we have an overview of the responsible persons 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.

3.4. COSO Framework

The Committee of Sponsoring Organizations of the Treadway Commission (COSO) Internal Control—Integrated Framework, originally issued in 1992, in 2023 issued supplemental guidance for organizations to achieve effective internal control over sustainability reporting (ICSR) [27]. 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, for example: 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 refined hierarchical structures on the example of the company Petroleum industry, while Figure 6b,c shows a more detailed organizational and process structure.

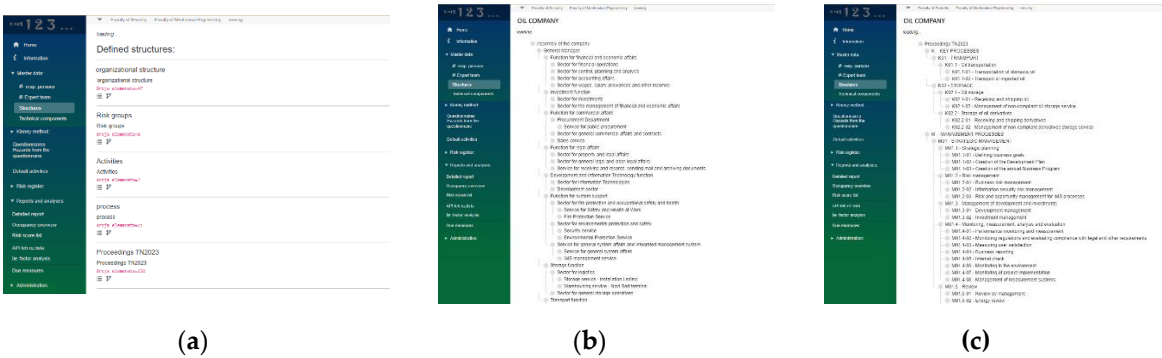


Figure 6. (a) Structures; (b) Organizational structure (c) Processes structure.

3.5. Risk Assessment

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

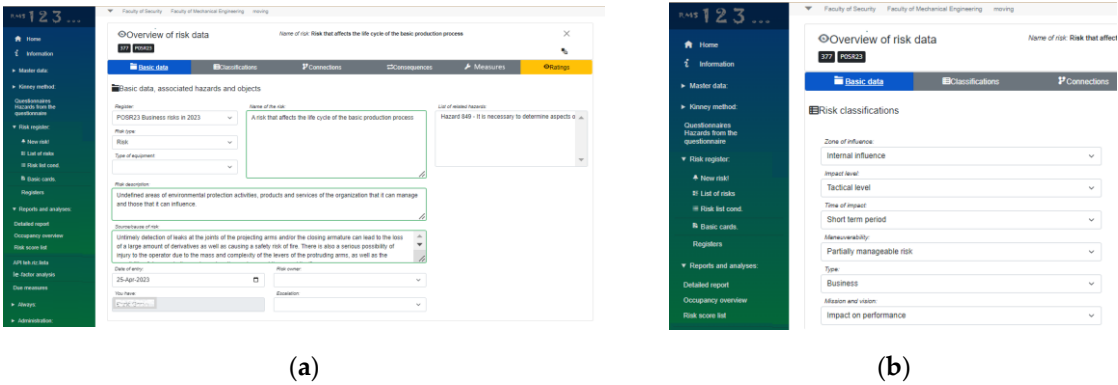


Figure 7. (a) Risk basic data; (b) Risk classification.



Figure 7b shows risk classification card in detail. Classifications can be made according to the 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 of the observed risk with the defined elements of hierarchical structures (COSO framework). One risk can be associated with one or more elements within each of the defined hierarchical structures.

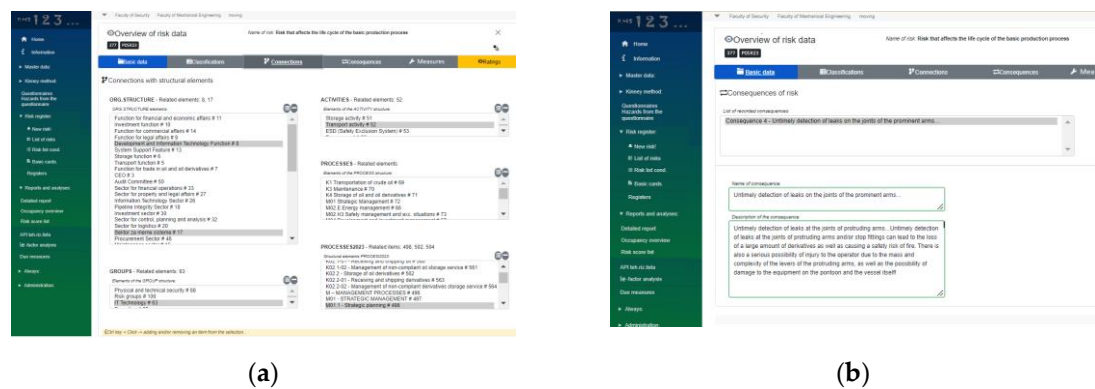


Figure 8. (a) Connections with structures; (b) Consequences.

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

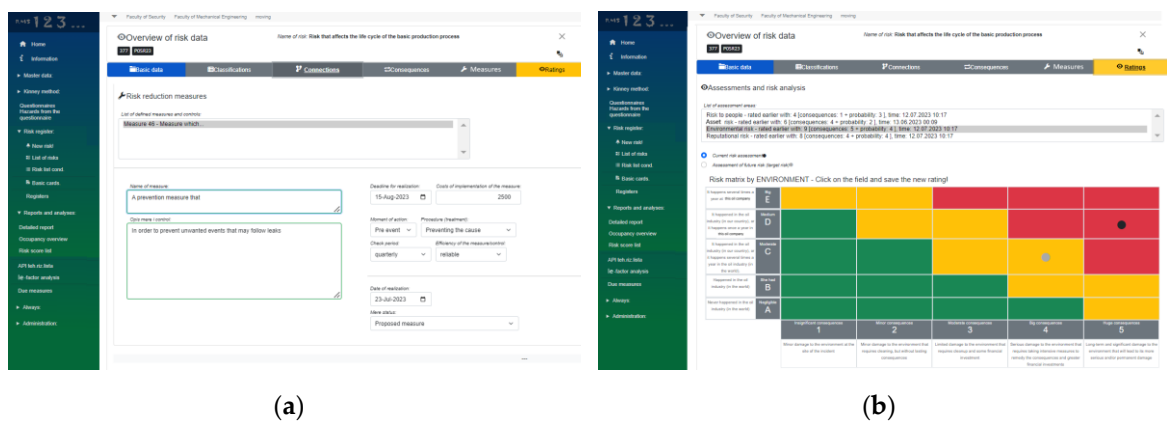


Figure 9. (a) Measures; (b) Risk assessment.

Figure 9b shows the risk assessment card. The observed risk can be evaluated using 4 risk matrices, namely: risk to people, risk to the environment, risk to property and risk to the reputation of the observed organization. Categorization by x and y axis on these 4 matrices is different taking

into account to the different nature of the consequences. For example, for the human risk matrix, the consequences are: 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. This risk matrices differs from the other three metrics because it contains 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 recommended actions to mitigate or eliminate the observed risk. All 4 built-in matrices in the RMS software solution 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.

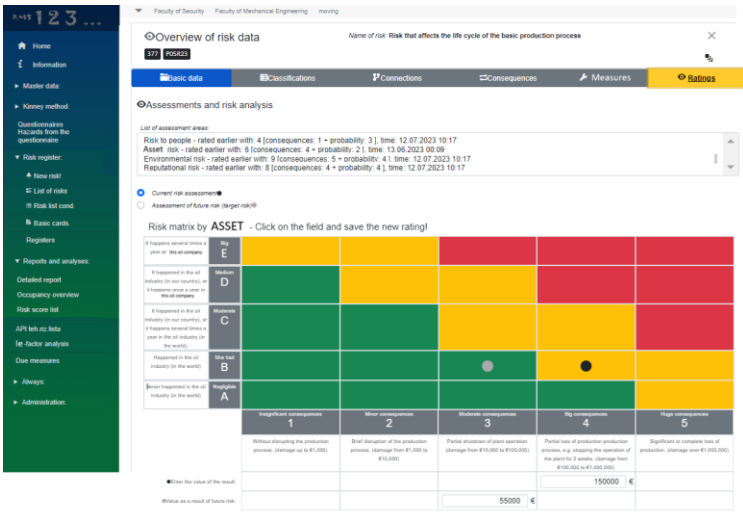


Figure 10. Risk matrices for assets (financial).

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, a Ie-factor (Investment effectiveness) analysis is carried out, based on which risks are prioritized in relation to the effectiveness of recommended actions for risk mitigation or elimination.

3.6. Supported Methodologies

As shown in the previous chapter, one of the built-in risk assessment methodologies in the RMS software is risk matrices adaptation tool according to the specific organization risk appetite. 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. 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, 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 Kinney method, Figure 11.

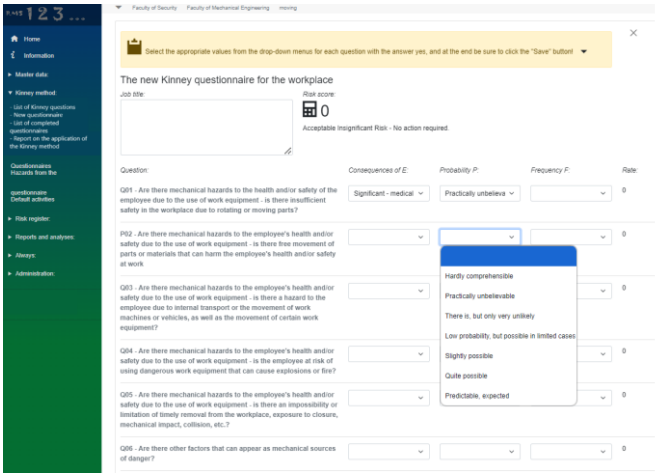


Figure 11. Assessment of workplace (health and safety) risks using Kinney method.

The questionnaire for workplace risk assessment contains 64 questions and the categories 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 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 Petroleum industry company case technical equipment which is examined by this methodology in RMS are: 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 12 shows the risk assessment using a qualitative approach according to the API 581 standard on the example of an atmospheric tank.

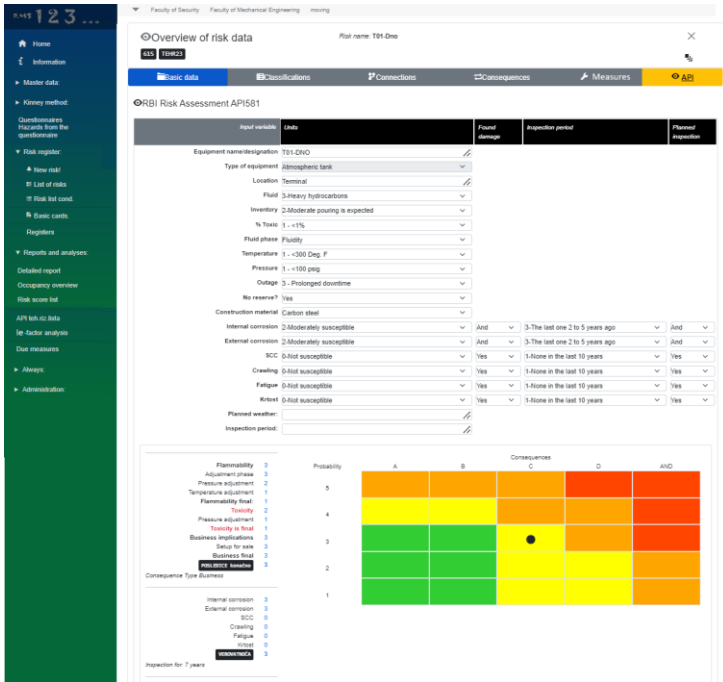


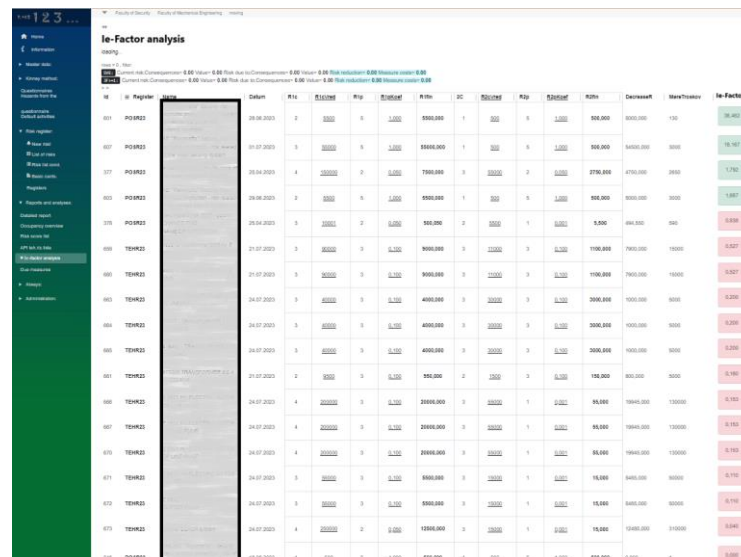
Figure 12. API 581 methodology for technical risks.

$$\text{Ratio coefficient} = \frac{\text{Future value of the risk}}{\text{Current value of risk}} \quad (1)$$
[illegible]

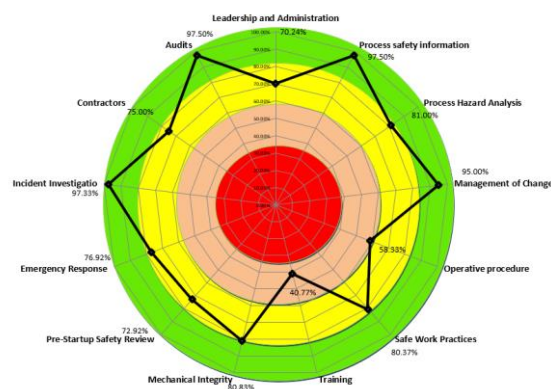
**Figure 13. Risk Score Analysis.**

- $Ie\_factor > 1$  - these results are colored green (in Figure 14), i.e., they indicate that the difference between the future value of the risk and the current value of the risk divided by the total value of the recommended measures is positive and that it is profitable to invest in risk reduction activities
- $Ie\_factor < 1$  - these results are colored red (in Figure 14), and they indicate that the recommended measures are greater than the difference between the future risk value and the current risk value, and that it is not profitable to invest in these mitigating activities.

Management System Factor is one of API 581 risk-based inspection technology procedures for management system evaluation. This is done with the help of questionnaires from API 581, which serve us for 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 example of RMS software solution MSF analysis realization.



**Figure 14. Ie-Factor Analysis.**



**Figure 15. Management System Factor Analysis.**

## 4. Conclusions

The paper presents a new methodology for managing company risks based on the algorithm presented in Figure 1, which enables the implementation of the COSO framework, ISO 31000 and many other technical and organizational standards, work with knowledge bases, project management, the application of different methodologies for identification, classification, assessment of current and future risks for different business areas. 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 Petroleum industry. The existing version of RMS is suitable for implementation in similar companies that deal with transportation, storage, energy production, as well as for other processing companies.

The advantages of using RMS software solutions are online management of project tasks in terms of risk identification, risk calcification, entering/updating list 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 thanks to the ability to assess the future and current value of the observed risk, Ie-factor analysis thanks to the financial assessment of the value of the recommended mitigation actions, as well as the overall prioritization of risks based on the COSO framework by elements of hierarchical structures or application of Risk score and Ie-factor analysis. 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).



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

**Author Contributions:** Conceptualization, P.S., M.M.<sup>2</sup>, G.Đ.; data curation, M.M.<sup>5</sup>, B.K. .; formal analysis, D.B. and P.S.; software, P.S., M.M.<sup>2</sup>, G.Đ.; supervision, M.M.<sup>5</sup>, B.K., D.B., P.S.; validation, G.Đ.; visualization, G.Đ.; writing—original draft, P.S., M.M.; writing—review and editing, P.S., M.M.<sup>2</sup>. 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.

**Data Availability Statement:** Data are available on request.

**Institutional Review Board Statement:** Not applicable.

**Informed Consent Statement:** All subjects gave their informed consent for inclusion before they participated in the study.

**Acknowledgments:** This paper has been published as a part of the project that is financed 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.

**Conflicts of Interest:** There are no conflicts of interest.

## References

1. Addo-Tenkorang R., Helo P. (2011). Enterprise Resource Planning (ERP): A Review Literature Report, Proceedings of the World Congress on Engineering and Computer Science 2011 Vol II WCECS 2011, October 19-21, 2011, San Francisco, USA
2. Giambona, E.G., John R., Harvey, C.R., Bodnar, G.M. (2018). The Theory and Practice of Corporate Risk Management: Evidence from the Field, *Financial Management*, pages 783 – 83
3. Merna, T., Faisal, F., Al-Thani (2015). *Corporate Risk Management An Organisational Perspectiv*, John Wiley & Sons Ltd.
4. Yun, J.(2023). The effect of enterprise risk management on corporate risk management, *Finance Research Letters* 55, 103950.
5. Mahmood, A., Lloyd, M., (2017). ERP System Implementation in Large Enterprises - A Systematic Literature Review, *Journal of Enterprise Information Management*, Vol. 30 Issue: 4, doi: 10.1108/JEIM-07-2014-0071, <http://dx.doi.org/10.1108/JEIM-07-2014-0071>
6. Malik, S.A., Holt, B., Freeman, J. (2013). Enterprise Risk Management (ERM): A New Way of Looking at Risk Management at an Organisational Level, Conference Paper, Conference: EUROXXVI, Rome, Italy
7. Francisku, A.A., Ridwan, H., Kevin, B.S. (2021) The State-of-The-Art of Enterprise Risk Management Maturity Models: A Review, *Annals of R.S.C.B.*, ISSN:1583-6258, Vol. 25, Issue 2, Pages. 4005 - 4014.
8. Mahmood, F., Zahid, A.H. (2019). ERP issues and challenges: a research synthesis, *Kybernetes*, Emerald Publishing Limited 0368-492X DOI 10.1108/K-12-2018-0699
9. Fraser, J., Simkins, B. (2016). The challenges of and solutions for implementing enterprise risk management, *Business Horizons* BUSHOR-1317; No. of Pages 10, <http://dx.doi.org/10.1016/j.bushor.2016.06.007>
10. Abrams, C., von Känel, J., Müller, S., Pfitzmann, B., Ruschka-Taylor, S. (2006). Optimized Enterprise Risk Management, *Computer Science, RZ 3657 (# 99677)*, 24 pages
11. Stefanou, C.J. (2001). A framework for the ex-ante evaluation of ERP software, *European Journal of Information Systems* 10, 204–215
12. Valashani, M.A., Abukari, A.M. (2020). ERP Systems Architecture for The Modern Age: A Review of the State of the Art Technologies, *Journal of Applied Intelligent Systems & Information Sciences*, Vol. 1, Issue 2, Pp. 70-90, August 2020., Available at: [www.journal.research.fanap.com](http://www.journal.research.fanap.com), DOI: 10.22034/JAISIS.2020.103704
13. Söderholm, P., Karim, R. (2010). An Enterprise Risk Management framework for evaluation of eMaintenance, The 1st international workshop and congress on eMaintenance 22-24 June, Luleå, Sweden, ISBN 978-91-7439-120-6
14. Mohamed, A.A.E., Eman, N., Mervat, H.G. (2016). Benefits and challenges of cloud ERP systems e A systematic literature review, *Future Computing and Informatics Journal* 1, 1-9, <http://www.journals.elsevier.com/future-computing-and-informatics-journal/>

15. Mohamed S.S., Abdulkader, A. (2011). A new comprehensive framework for enterprise information security risk management, *Applied Computing and Informatics* 9, 107–118
16. Louis A.C. (2008). What's Wrong with Risk Matrices?, *Risk Analysis*, Vol. 28, No. 2.
17. Arena, M., Arnaboldi, M., Azzone G. (2011) Is enterprise risk management real?, *Journal of Risk Research*, 14:7, 779-797, DOI: 10.1080/13669877.2011.571775
18. Bromiley, P., McShane, M., Nair, A., Rustambekov, E. (2015) Enterprise Risk Management: Review, Critique, and Research Directions, *Long Range Planning*, 48: 265-276.
19. Essex, D.E. (2005). The black art of risk. *PM Network*, 19(9), 88–92.
20. Patterson, T., The Use of Information Technology in Risk Management, September 2015, White Paper, [aicpa.org/FRC](http://aicpa.org/FRC)
21. Pandey S. K., Mustafa K. (2012). A Comparative Study of Risk Assessment Methodologies for Information Systems, *Buletin Teknik Elektro dan Informatika (Bulletin of Electrical Engineering and Informatics)* Vol.1, No.2, June 2012, pp. 111~122, ISSN: 2089-3191
22. Bromiley, P., McShane, M., Nair, A., Rustambekov, E (2014). Enterprise Risk Management: Review, Critique, and Research Directions, *Long Range Planning* xxx, 1-12
23. Mitterbaur, P., Pesendorfer, J., Schmidinger, E. (2016). Opportunities and risks of IT solutions for ERM" *ACRN Oxford Journal of Finance and Risk Perspectives* 5.3, 15-29.
24. Dikmen, I., Birgonul, M.T. and Arikan, A.E. (2004). A critical review of risk management support tools. In: Khosrowshahi, F. (Ed.), 20th Annual ARCOM Conference, 1-3 Heriot WattUniversity. Association of Researchers in Construction Management, Vol. 2, 1145-54.
25. Khan, M.A., Khan, S., Sadiq, M. (2012). Systematic Review of Software Risk Assessment and Estimation Models, *International Journal of Engineering and Advanced Technology (IJEAT)* ISSN: 2249-8958 (Online), Volume-1 Issue-4, pp. 298-305
26. Stanojevic, P., Misita, M., Djuric, G. (2023). Software System for Risk Management Based on Artificial Intelligence, Second memorial scientific conference "Predrag Maric" (on Serbian), pp. 144-154. ISBN 987-86-80144-63-4.
27. Committee of Sponsoring Organizations of the Treadway Commission (COSO) (2004). Enterprise Risk Management - Integrated Framework, Pricewaterhouse Coopers LLP.

**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.