RiskMIS: A Web-Based Risk Management Information System

Alya Thiab Almutairi, Kassem Saleh
Department of Information Science-College of Life Sciences, Kuwait University,
Sabah Al Salem University City, P.O. Box 5969, Safat 13060, Shadadiya, Kuwait

***Abstract*—Risk management is the systematic process of identifying, assessing, monitoring, and responding to risks in projects and ongoing operations. Effective execution of risk management activities is essential for the successful completion of projects and the achievement of key performance indicators in operational environments. In recent years, organizations have increasingly emphasized the proactive identification and mitigation of risks before they materialize. Consequently, risk assessment is addressed early in the lifecycle and continuously revisited to ensure the proper functioning of ongoing operations and the successful delivery of projects. A central tool in the risk management process is the risk register, which consolidates all critical and relevant information related to identified risks. The risk register serves as a focal point around which risk management activities are organized. It is inherently dynamic and must be continuously updated to reflect changes in risk exposure and response strategies. When properly managed, the risk register supports informed decision-making and enables managers to handle risks in a systematic and timely manner. The primary objective of this study is to bridge theory and practice by developing a risk management information system centered on a comprehensive risk register. The study presents the design of the proposed system using established modeling techniques and diagrams, followed by the development of a functional prototype based on modern web technologies. Finally, a demonstration of the prototype is provided to illustrate its capabilities and practical applicability.**

Keywords*—Risk management; risk management information system; risk register; project risk; decision support systems

I. Introduction

Risks are inherent in the management of projects and ongoing operations. Managers are therefore expected to be capable of identifying and anticipating risks that may affect organizational activities. In practice, however, risks are often neglected or inadequately managed, either because they are perceived as unlikely to occur or because risk management is viewed as an unnecessary overhead. Some managers also tend to associate risk solely with negative outcomes to be avoided. In reality, risk is an integral part of organizational performance and value delivery, making effective risk management essential for business success. In today's rapidly changing environment, organizations face increasing levels of uncertainty, and their resilience and sustainability depend largely on how well risks are managed.

The importance of risk management is particularly evident in information systems projects. The Standish Group's CHAOS report [35] indicates that approximately 69% of such projects partially or completely fail. Empirical evidence shows that integrating risk management into the project development process significantly improves the likelihood of successful project execution and deployment. The same principle applies to ongoing business operations, where unmanaged risks can undermine performance and continuity.

A wide range of standards, guidelines, and best practices has been proposed to support risk management in general and project risk management in particular. Notable examples include the ISO 31000 risk management guidelines [16] and the Project Risk Management framework of the Project Management Body of Knowledge (PMBOK) published by the Project Management Institute [28]. Studies indicate that 71% of projects that systematically apply risk management practices succeed in meeting customer expectations with respect to time, quality, and cost [6].

As part of a preliminary investigation, 28 leading RMIS and risk register tools were systematically analyzed through provider websites, email questionnaires, live chats, and limited demo access. The comparative analysis revealed several unmet limitations in existing solutions. Most tools primarily target medium and large enterprises, with limited accessibility for small organizations or individual users. Additionally, many systems are complex, expensive, require extensive configuration, and often integrate risk management as a secondary function within broader project management platforms rather than offering a focused and streamlined risk register solution.

Furthermore, access restrictions, quote-based pricing models, installation requirements, and limited web or mobile availability reduce usability and flexibility. These findings highlight a practical and conceptual gap in the availability of a lightweight, web-based, accessible, and cost-effective RMIS designed specifically to simplify risk management processes while maintaining usability, scalability, and security. Therefore, the proposed RiskMIS addresses this identified gap by offering a simplified, web-based, and broadly accessible solution adaptable across various domains without heavy customization requirements.

Among the tools used to support risk management, the risk register plays a central role. It provides a structured repository for documenting identified risks, their characteristics, and planned responses, and it serves as the focal point for risk analysis, prioritization, and monitoring. Despite its importance, existing research has largely focused on theoretical aspects of risk management—such as risk categorization, probability,

impact, and prioritization—while paying limited attention to the design and structure of the risk register itself. Some studies propose domain-specific risk registers or spreadsheet-based approaches. For example, [37] suggests a reference risk register for project management and outlines steps for its implementation using Excel, while Burcar, Radujković, and Vukomanović [5] propose a methodology for developing a risk register in construction projects using software support such as relational databases. However, these studies provide limited guidance on how to systematically design and implement a comprehensive risk register or how to embed it within an integrated risk management information system. Moreover, existing solutions are often domain-specific and lack adaptability across different organizational contexts.

This study addresses these limitations by presenting the systematic development and implementation of RiskMIS, a comprehensive risk management information system designed around a dynamic and reusable risk register. The system supports the structured documentation of risks and response strategies to enhance the success of projects and ongoing operations. To develop the proposed tool, we adopted a Software Development Life Cycle (SDLC) approach based on the waterfall model, encompassing analysis, design, implementation, testing, and maintenance phases [34].

The study begins with an extensive analysis of existing approaches and relevant literature to consolidate risk register concepts and identify suitable theories related to risk categorization, prioritization, probability, and impact. It then specifies the functional and non-functional requirements of the proposed system, followed by the detailed design and implementation of a working prototype. The development process includes algorithm design, database conceptual modeling, system architecture, activity and state diagrams, graphical user interface design, and data structure definition. The database was designed using the Entity Relationship (ER) model, while Unified Modeling Language (UML 2.5) diagrams were used to represent behavioral and structural aspects of the system [25]. The prototype was implemented as a web-based application using the ASP.NET Core framework, developed in C#, with Microsoft SQL Server 2018 used for data management. The system was subsequently tested to verify that it meets its specified requirements and intended functionality.

The remainder of this study is organized as follows: Section II presents background concepts related to risk and risk management. Section III defines and analyzes the functional and non-functional requirements of the proposed system. Section IV describes the design and implementation of RiskMIS. Section V demonstrates the system prototype. Finally, Section VI discusses the findings, draws conclusions, and outlines directions for future work.

Despite the structured design of RiskMIS, several limitations remain. The system has not yet been validated through longitudinal case studies in real organizational environments, and quantitative performance metrics have not been formally established. Technical benchmarking under high operational loads has not been conducted, limiting conclusions regarding scalability and database efficiency. Additionally, formal security assessments, version control mechanisms, and comprehensive data lifecycle management strategies have not yet been fully implemented. The system has not been empirically validated across multiple sectors, and structured user training and adoption frameworks have not been systematically evaluated. These limitations highlight areas for further empirical and technical development.

II. Background

This section provides background information on risks and risk management, including risk terminology, risk classification, operational and project risk management, risk management frameworks and processes, risk registers, and risk assessment criteria.

A. Risk Terminology

Risk is commonly defined as the probability of an event occurring and the consequences associated with that event [14]. It is typically characterized by three fundamental elements: the event itself, its probability of occurrence, and its impact [29]. In general terms, risk refers to any event or condition that may hinder an organization from achieving its objectives. This study focuses on negative risks, hereafter referred to simply as risks. Effective risk management aims to minimize adverse impacts while enabling organizations to sustain performance and achieve desired outcomes.

Organizations classify risks based on their nature, context, and specific concerns [26]. Although no universal risk classification system applies to all organizations, many adopt classifications proposed by relevant standards, frameworks, or prior research [13]. The terms *risk classification*, *risk categorization*, *risk typing*, and *risk taxonomy* are often used interchangeably to describe the grouping of risks according to defined criteria.

Risks may be categorized by source, type, timescale, or nature of impact. For example, risks can affect financial performance, operational activities, infrastructure, reputation, or market position. A structured risk classification system facilitates risk identification, responsibility assignment, comparison of similar risks, and the definition of risk management scope. Consequently, organizations often tailor their classification schemes to align with their specific activities and objectives [13]. For instance, Larson and Gray [19] propose a generic Risk Breakdown Structure (RBS) based on risk sources, while a similar RBS for generic projects is presented in [12].

B. Operational and Project Risk Management

Organizations face multiple types of risks, and categorization plays a key role in their effective identification [11]. Common categories include operational, project, organizational, and commercial risks. Operational risks arise from routine organizational activities and typically result from human error, process failures, or deficiencies in systems and controls [9]. Such risks often affect service quality, efficiency, and reliability [13].

Project risk management, in contrast, focuses on uncertainties that may affect project objectives throughout the project lifecycle. It encompasses planning for risk management, risk identification, qualitative and quantitative analysis,

response planning, and ongoing monitoring and control [28]. The objective is to minimize negative risks while maximizing positive risks, or opportunities. Effective project risk management is widely recognized as a critical factor in successful project delivery [30].

Projects progress through a defined lifecycle from initiation to closure [28]. Numerous lifecycle models exist, often tailored to specific industries or organizational contexts. Organizations typically select lifecycle models that best align with their operational needs and governance structures.

C. Risk Management Processes and Frameworks

Effective risk management requires well-defined processes supported by appropriate risk management frameworks [30]. According to [15], risk management is the systematic application of policies, procedures, and practices to activities such as communication, consultation, context establishment, risk identification, analysis, evaluation, treatment, monitoring, and review. These processes are formalized within widely adopted standards and frameworks, including ISO 31000, the IRM Standard, BS 31100, and the COSO ERM framework [13].

In the software and information systems domains, several formal risk management methodologies assess risks throughout the development lifecycle [8]. Notable examples include Boehm's risk management model [3], the SEI Continuous Risk Management (SEI-CRM) method [10], the Riskit method [18], the CMMI framework [7], and the Larson and Gray approach [19].

Since its introduction, ISO 31000:2009 has gained widespread adoption due to its comprehensive and flexible structure [2]. Nevertheless, many organizations prefer the PMBOK framework when managing project-specific risks.

Larson and Gray [19] describe a four-step risk management process comprising risk identification, risk assessment, risk response development, and risk response control. The final step include implementing response strategies, monitoring risk triggers, activating contingency plans, updating risk records, and identifying emerging risks. Empirical evidence supports the effectiveness of structured risk management processes. For example, Junior et al. [17] found that applying formal risk management practices and assigning dedicated risk roles significantly improved project success. While project managers remain accountable for overall project outcomes [19], risk managers are responsible for planning, coordinating, and overseeing risk-related activities [4].

D. Risk Register

The risk register is a fundamental component of risk management at both project and organizational levels [13]. Its importance is consistently emphasized in the literature; for instance, Saffin et al. [33] report that 70% of project managers consider the risk register a critical project management tool. A risk register consolidates detailed information about identified risks, including their likelihood, impact, priority, ownership, and response strategies. The risk register should be highly accessible and provide the necessary information about risks [32].

Risk registers vary widely in form and complexity, ranging from simple paper-based documents to sophisticated software solutions. Many organizations rely on spreadsheets or word-processing tools for risk documentation. A study by the Design Information Group at Bristol University found that 67% of respondents documented risks using paper or computer-based registers, with 78% developed internally [27]. While such approaches are accessible, they often lack scalability, consistency, and integration.

Several studies have explored risk register implementation in specific domains. For example, Burcar et al. [4] report positive results from implementing a database-driven risk register in the Croatian construction industry. Other research highlights that a risk register is essentially a structured and continuously updated repository of risk information [37], which may be implemented using documents, spreadsheets, or relational databases [13].

Comparative studies further indicate that theoretical models alone are insufficient for developing comprehensive and reusable risk registers [36]. Domain-specific implementations—such as reference risk registers in information security [24] or electric power generation [20]—demonstrate practical benefits but often lack generalizability. According to the PMBOK Guide [28], a risk register should include identifiers, descriptions, owners, causes, impacts, triggers, response strategies, and status information. To remain effective, it must be continuously updated and treated as a dynamic information resource [13].

Despite their widespread use, spreadsheet-based risk registers present significant limitations. Martins [22] identifies issues related to data organization, version control, collaboration, integration, and usability. These limitations are reinforced by survey findings indicating that while 97% of finance professionals use spreadsheets for risk management, 72% consider them inefficient [1]. Spreadsheet-based tools are particularly vulnerable to access control issues, formula errors, and inconsistent data handling, making them unsuitable for comprehensive and long-term risk management.

E. Risk Criteria and Risk Matrix

Risk criteria define the basis on which risks are evaluated and prioritized and vary according to organizational objectives and context [16]. Establishing clear risk criteria ensures a shared understanding of risk-related terms and assessment scales across the organization.

Following risk identification, risks are analyzed by assessing their probability and impact based on the defined criteria. Each risk is assigned a risk score to support prioritization. Risk analysis may be qualitative or quantitative. Chihuri and Pretorius [6] found that qualitative risk analysis is more commonly used due to its simplicity and ease of interpretation. Although cost-effective, qualitative methods are inherently subjective [30]. Quantitative analysis, while more precise, is less frequently applied because of its complexity. In qualitative analysis, risk scores are typically calculated by combining probability and impact values [33], whereas quantitative analysis numerically estimates potential losses and is often reserved for high-exposure risks [30].

III. ANALYSIS

In this section, we identify the most relevant theories related to risk categorization, prioritization, probability, and impact, and use them to derive the functional and non-functional requirements of the proposed tool.

A. Main Risk Management Elements

Risk management can become complex and time-consuming when inefficient tools are used. Manual and semi-structured approaches, such as word processors and spreadsheets, impose significant limitations on consistency, traceability, and timely decision-making. These limitations highlight the need for an automated and unified risk management tool capable of supporting risk identification, analysis, and treatment throughout the project lifecycle, thereby improving the likelihood of project success.

1) Project life cycle: To ensure applicability across different business domains, the proposed tool adopts a generic predictive project life cycle model consisting of five stages, based on the standardized project lifecycle and best practices defined by the Project Management Institute (PMI). In predictive life cycles, project cost, duration, and scope are defined early in the lifecycle [28].

The first stage, Idea, represents a preliminary concept in which project goals, specifications, and team responsibilities are not yet finalized. Projects in this stage can be modified or canceled without organizational impact, preventing unnecessary allocation of resources to initiatives that may never commence. The second stage, Initiating, involves finalizing project objectives, scope, budget, duration, and assigning project and risk managers. In the Planning stage, the project manager develops detailed plans to meet project requirements within approved constraints. Once the plan is confirmed, the project enters the Executing stage, during which tasks are carried out according to the approved plan. The final stage, Closing, concludes the project and delivers outcomes to the client. In this model, execution and monitoring activities defined by PMBOK [28] are consolidated into a single Executing stage.

Within the tool, projects transition through seven operational states, as illustrated in Fig. 8. Projects are initially created in the Idea state and progress to Initiate, once key details are finalized and responsible managers are assigned. Upon plan development, the project moves to the Plan state. When at least one task enters execution, the project transitions to In Process. A project is marked Completed when all tasks are completed. Projects may also enter On Hold or Canceled states. Only administrators may cancel projects, and only when the project is in the On Hold state. Projects canceled in the Idea state are permanently removed, as they provide no long-term value. Project states are automatically updated based on task status, ensuring consistency between task progress and overall project state. The meaning of each state is summarized in Table I.

TABLE I. PROJECT STATUS OF THE DEVELOPED TOOL

Project State	Meaning	Notes
Idea	The administrator has an idea of a new project discussed or requested by the client but doesn't have a final decision about the duration, budget, and the assigned PM and RM for the project.	This is the first and default status of the project. The administrator is the one who decides to have a new project. The administrator can change the project information. The administrator can delete the project from the tool permanently.
Initiate	The administrator finalizes the contract with the client and decides the start and end date of the project, the budget, and the PM and RM who will be responsible for the project.	The administrator should provide a description of the project. The administrator is Not allowed to make changes to the project information. The project will be available to PM and RM to work in. Administrator cannot delete the project after initiation.
Plan	PM divides the project into tasks, each task with a start and end date, cost, and requirements (goals to be achieved in specific tasks). Project being in Plan status when at least one task is created for the project.	The project will be in plan status when PM starts making tasks for the plan. The plan should be within the duration and budget decided by the administrator. Requirements for each task will be used as indicators of the completion of the task goal. If PM confirms the plan the project still in plan status but ready to start, all tasks will be in "Not Started" status. PM can cancel tasks after confirming the plan . If all tasks are canceled the project becomes in canceled status.
In Process	If PM starts at least one task (task in "In Process" status or "Delay" status) the project status becomes “In process” automatically even if there canceled tasks or “On hold”.	Administrator or PM cannot cancel or delete a project in the "In Process" state The project state changes automatically by the tool based on the tasks of the project.
Completed	If all tasks status is "Completed", even if some tasks are in the "Canceled" state	-
On Hold	Tool make the project status "On Hold" automatically when at least one task "On hold" and no task "In Process" or "Delay".	Administrator can delete the project and become in canceled state. This will make the status of "Not Started" tasks and "On Hold" tasks to "Deleted" and keep their cost and scope values to be used in the overall project calculations.
Canceled	Tool make the project state "Canceled" automatically if all tasks status is "Canceled" or when the Administrator cancels the project when it is "On Hold" state	Project with "Canceled" status, their data will be stored in the tool and not deleted, and users can see the report of the project.

2) Task life cycle: During the Executing stage, the approved project plan is implemented through task execution. Tasks progress through three primary steps: Not Started, In Process, and Completed. Once the project plan is confirmed, all tasks default to the Not Started state. Project managers may initiate tasks, moving them to In Process, and continuously monitor their progress. Tasks are marked Completed once all defined requirements are achieved.

In addition to these steps, tasks may assume one of six possible statuses. Tasks that have not started may be canceled and are subsequently treated as non-existent. If an executing task exceeds its planned duration, it is marked as Delayed. Tasks in In Process or Delayed states may be placed On Hold, at which point the project manager records the associated cost and scope. On-hold tasks may later be resumed or completed, with final cost and scope values recorded upon completion.

3) Project success criteria: To ensure general applicability, project success in the proposed tool is evaluated using the triple constraint model—cost, time, and scope. By embedding this triangle within the predictive project life cycle, the tool allows project and risk managers to continuously assess the impact of identified risks on the key project constraints. This approach aligns with the Project Management Institute's PMBOK Guide, which emphasizes the integration of scope, schedule, and budget management across the project lifecycle, and is further reinforced by ISO 31000:2018 principles, which highlight the importance of assessing risk impact on organizational objectives. Consequently, the proposed provides a structured method to manage risks while maintaining balance among the critical project parameters, ensuring both effective risk management and project success.

Each task is assessed based on actual expenditure, execution duration, and degree of requirement fulfillment. Aggregated task-level metrics determine overall project success. Risks directly influence these dimensions, thereby affecting both task performance and overall project outcomes.

4) Risk management process: The proposed tool supports a collaborative risk management process involving administrators, project managers, risk managers, and team members. Upon project initiation, roles are clearly assigned to ensure separation of duties. Although organizations may adopt different risk management models, most follow a common process comprising risk identification, assessment, response, and monitoring. This structure aligns with the principles and risk management process defined in ISO 31000:2018, upon which the design of the proposed tool is conceptually grounded. In the proposed system, risks are identified collaboratively by project and risk managers, with input from team members using techniques such as brainstorming. Identified risks are reported through the system and recorded in the risk register. Risks are then categorized, assessed, and prioritized based on defined criteria. Risk managers prepare response strategies and assign risk owners responsible for implementation under the supervision of the project manager. The risk manager continuously monitors risks, including secondary risks, and updates the register as new risks emerge.

5) Risk register content: Based on the preceding analysis, the risk register in the proposed tool includes the following attributes: risk name, description, owner, probability, impact on cost, time, and scope, detectability, urgency, status, classification, response strategy, and secondary risk information. The structure of this risk register is aligned with the recommendations of the Project Management Institute as outlined in the guide of PMBOK.

6) Risk classification: Given the absence of a universally applicable risk classification system, the tool allows organizations to define and customize their own classifications. A default two-level classification structure is provided to simplify risk identification and reduce ambiguity. This structure consists of main categories and subcategories with no limit on the number of entries. The default classification is based on the Larson and Gray framework, which includes four main categories and corresponding subcategories, as discussed in Section II A.

7) Risk criteria: The tool incorporates a generic risk criteria framework covering probability, impact on cost, time, and scope, detectability, and urgency. Each factor is defined on a five-level scale (1–5) with percentage-based definitions to minimize ambiguity.

The risk probability is categorized, as shown in Table II. The risk detection is categorized, as shown in Table III. Risk urgency is defined using a binary scale distinguishing urgent and non-urgent risks (see Table IV). Task scope completion is also evaluated using a predefined scale (see Table V).

Organizations are required to specify their risk attitude by ranking probability, impact, and detectability according to importance. These rankings influence risk scoring, project status evaluation, and the calculation of risk impact on cost, schedule, scope, and response effectiveness.

TABLE II. RISK PROBABILITY SCALE

Score	Description	Definition
1	Almost Never	The risk is 1% or less expected to occur in the project.
2	Low	The risk is more than 1% expected to occur in the project.
3	Moderate	The risk is 20% and more expected to occur in the project.
4	High	The risk is 50% and more expected to occur in the project.
5	Almost Certain	The risk is 90% and more expected to occur in the project.

TABLE III. RISK DETECTION SCALE

Score	Description	Definition
1	Almost Certain	The probability that the risk will be detected is more than 90% certain.
2	High	The probability that the risk will be detected is more than 50%.
3	Moderate	The probability that the risk will be detected is more than 25%.
4	Low	The probability that the risk will be detected is more than 5%.
5	Almost Impossible	The probability that the risk will be detected is 0%.

TABLE IV. RISK URGENCY SCALE

Score	Description	Definition
1	Urgent Risk	The risk needs an immediate action
0	Unurgent Risk	The risk can wait

TABLE V. TASK SCOPE SCALE

Score	Description	Definition
1	Poor	Less than 60% of the task requirements have been met.
2	Fair	61% - 80% of the task requirements have been met.
3	Good	More than 81% of the task requirements have been met, and some essential requirement not done yet.
4	Very Good	All essential requirements of the task have been done, but there are some remaining low priority requirements not done.
5	Excellent	All the requirements of the task have been met exactly as mentioned in the plan.

8) Risk matrix: The proposed tool employs qualitative risk analysis to prioritize risks. Precise definitions of probability and impact ensure consistent interpretation across the organization. Risk scores are derived by combining probability and impact values, using either the highest or average impact when multiple dimensions are affected.

For example, consider the risk "The technology is new and the project team lacks sufficient experience, leading to delays". If the likelihood of occurrence is between 1% and 20%, the probability is classified as Low (score = 2). Based on the defined criteria, the impact may be assessed as Moderate for cost (score = 3) and Catastrophic for both time and scope (score = 5). The resulting risk score is then calculated using the predefined qualitative formulas, supporting systematic prioritization and treatment.

$$Risk\ Score = p * \max_{1 \le c,t,s \le 5}(c,t,s)$$

where, p is the probability of occurrence, c is the impact in cost, t is the impact in time, and s is the impact in scope. By applying this equation, the risk score of the risk will be computed as follows:

$$Risk\ Score = 2 * \max_{1 \le c,t,s \le 5}(3,5,5)$$

$$Risk\ Score = 2 * 5 = 10$$

The risk score using the average impact is expressed using the following formula:

$$Risk\ Score = p * \frac{c+t+s}{3}$$

where, p is the probability of occurrence, c is the impact in cost, t is the impact in time, and s is the impact in scope. By applying this equation, the risk score will be computed as follows:

$$Risk\ Score = 2 * \frac{3+5+5}{3}$$

$$Risk\ Score = 2 * \frac{13}{3} = 8.67$$

The risk score based on the average impact reduces the priority of risk compared to the highest impact score. So, the risk score calculation can have a critical impact on how the risk is evaluated and dealt with. In [31], the authors proposed a new formula to calculate the risk score by adding a detection score to the well-known risk analysis method and they found that it improves risk prioritization. The Risk Priority Number (RPN) is expressed using the following formula:

$$Risk\ Score = p * i * d$$

where, p is the probability of occurrence, i is the impact of risk, and d is the detectability score. Detectability is the capacity of the organization to detect the risk before it happens [23]. The importance of detectability is important even if the risk is having low probability and low impact. If not detected, the risk can cause a big loss to the project [31]. In our example, if the RM uses techniques and tools to easily detect the risk that the project team is unfamiliar with the new technology, the detectability of risk is "High" with a score of (2) based on Table III.

RPN gives the same weight for the three components of the risk score. That may result in inaccurate risk assessment [21]. It neglects the importance of each component for the organizations and assumes that each organization considers probability, impact, and detectability with the same importance. In [21], the authors proposed a new method to solve the issue of the weights' difference of risk components by generating measures based on the weights of the probability, impact, and detectability taken from a domain expert.

The developed tool prioritizes risks in the new proposed methodology based on the previously discussed measures. The prioritization process has six steps. First, the organization should specify its risk criteria which should include in addition to the references of the risk probability, impact in cost, time, and scope, and detectability, and score, the rank of the risk probability, impact, and detectability from the most important to least. The importance rank indicates the weight of each component, the first component in the rank indicates that it's

the most important component factor to the organization and needs more attention, so it will take the weight of (3). On the other hand, the second and third components in the organization ranks of importance will have the same weight of (1), which means that those components are less important to the organization compared to the first one. The organization rank of importance can be set by the Risk Manager in the developed tool using "Risk Settings" page.

Secondly, after determining the weights, the RM should specify the risk scores of the probability, impact on cost, time, and scope, and detectability for risks. The third step is performed by the tool using the following formula to calculate the risk score for each risk:

$$Risk\ Score = \begin{cases} \left(p * g(p)\right) + \left(\frac{c+t+s}{3}\right) + d, if\ g(p) > g(i)\ and\ g(p) > g(d) \\ p + (\max(c,t,s) * g(i)) + d, if\ g(i) > g(p)\ and\ g(i) > g(d) \\ p + \left(\frac{c+t+s}{3}\right) + \left(d * g(d)\right), if\ g(d) > g(p)\ and\ g(d) > g(i) \end{cases}$$

where, p is the probability of occurrence, i is the impact of risk, d is the detectability score, g(p) is the weight of probability, g(i) is the weight of impact, g(d) is the weight of detectability, c is the impact on cost score, t is the impact on time score, s is the impact on scope score. By applying this equation based in the previous number of the provided example, and by assuming that the most important risk component to the organization is the impact which gives impact component weight of (3) and both the probability and detectability weight of (1), the risk score will be computed as follows:

$$Risk\ Score = \begin{cases} \left(p * g(p)\right) + \left(\frac{c+t+s}{3}\right) + d, if\ g(p) > g(i)\ and\ g(p) > g(d) \\ p + \left(\max(c,t,s) * g(i)\right) + d, if\ g(i) > g(p)\ and\ g(i) > g(d) \\ p + \left(\frac{c+t+s}{3}\right) + \left(d * g(d)\right), if\ g(d) > g(p)\ and\ g(d) > g(i) \end{cases}$$

The second part of the formula will be used to calculate the risk score, since the weight of impact is greater than both the weight of portability and detectability.

$$Risk\ Score = p + (\max(c,t,s) * g(i)) + d$$

$$Risk\ Score = 2 + (\max(3,5,5) * 3) + 2$$

$$Risk\ Score = 2 + (5 * 3) + 2 = 19$$

In the fourth step, we convert the resulting risk score from a range between 5 and 25 to be in a range from 1 to 5 using the following formula:

$$Risk\ Score_{1-5} = \left((Risk\ Score_{5-25} - 5) * \left(\frac{1}{5}\right)\right) + 1$$

By applying the risk score result from the previous equation, the final result will be computed as follows:

$$Risk\ Score_{1-5} = \left((19 - 5) * \left(\frac{1}{5}\right)\right) + 1$$

$$Risk\ Score_{1-5} = \left(14 * \left(\frac{1}{5}\right)\right) + 1 = 3.8$$

In the fifth step, we add another factor or component that can affect the prioritization of risks. We add an Urgency scale that can also be determined by the RM for each risk. Risk Urgency is determining which risk in the list of risks should be dealt with first before others [29]. Organizations should define risk urgency in their risk criteria. In the developed tool, we have an urgency scale from 0 to 1: 1 means that the risk needs immediate action, while 0 means the risk can wait. 0 is the default urgency status for all risks. The developed tool deals will urgent risk based on the value of the risk score. The following formula shows how the tool will deal with risks that are specified as urgent by the RM:

$$Risk\ Score_{1-5} = \begin{cases} 5, if\ u = 1\ and\ Risk\ Score_{1-5} \geq 4 \\ Risk\ Score_{1-5} + 0.75, if\ u = 1\ and\ Risk\ Score_{1-5} \geq 3 \\ Risk\ Score_{1-5} + 0.50, if\ u = 1\ and\ Risk\ Score_{1-5} \geq 2 \\ Risk\ Score_{1-5} + 0.25, if\ u = 1\ and\ Risk\ Score_{1-5} \geq 1 \\ Risk\ Score_{1-5}, if\ u = 0 \end{cases}$$

where, u is the urgency score. So, to continue with the previous example, if the risk is urgent, the final risk score of the risk will be calculated by the system by adding 0.75 to the risk score because the urgency is 1 and the risk score is greater than 3 as shown in the following evaluation of the formula:

$$Risk\ Score_{1-5} = \begin{cases} 5, if\ u = 1\ and\ Risk\ Score_{1-5} \geq 4 \\ Risk\ Score_{1-5} + 0.75, if\ u = 1\ and\ Risk\ Score_{1-5} \geq 3 \\ Risk\ Score_{1-5} + 0.50, if\ u = 1\ and\ Risk\ Score_{1-5} \geq 2 \\ Risk\ Score_{1-5} + 0.25, if\ u = 1\ and\ Risk\ Score_{1-5} \geq 1 \\ Risk\ Score_{1-5}, if\ u = 0 \end{cases}$$

$$Risk\ Score_{1-5} = Risk\ Score_{1-5} + 0.75$$

$$Risk\ Score_{1-5} = 3.8 + 0.75 = 4.55$$

The final step is performed by the system by providing the user with a risk score definition, as shown in Table VI. In our example, the risk is considered "Serious".

TABLE VI. RISK SCORE SCALE

Score	Description	Definition
1	Negligible	Risk Score is less than 2.
2	Minor	Risk Score is greater or equal to 2.
3	Moderate	Risk Score is greater or equal to 3.
4	Serious	Risk Score is greater or equal to 4.
5	Critical	Risk Score is 5.

9) Risk impact: In the developed tool, any risk added to the project will affect the cost, time, and scope of the project according to the definitions mentioned in Table VII.

TABLE VII. RISK IMPACT SCALE IN COST, TIME, AND SCOPE

Score	Description	Definition		
		Risk Impact on Budget	***Risk Impact on Schedule***	***Risk Impacton Scope***
1	Trivial	The risk has an impact on the budget of the project by less than 5%.	The risk has an impact in the project schedule by less than 5%.	The risk has barely a noticeable impact on the scope of the project.

2	Low	The risk has an impact on the budget of the project by less than 10%.	The risk has an impact on the time of the project by less than 10%.	The risk has an impact on the scope of the project.
3	Moderate	The risk has an impact on the budget of the project by less than 25%.	The risk has an impact on the time of the project by less than 25%.	The risk has an impact on the scope of the project by more than 50%.
4	High	The risk has an impact on the budget of the project by less than 50%.	The risk has an impact on the time of the project by less than 50%.	The risk has an impact on the essential requirements of the project.
5	Catastrophic	The risk has an impact on the budget of the project by greater than 50%.	The risk has an impact on the time of the project by greater than 50%.	The risk has an impact on the project to end in unacceptable project by the client.

For example, if a serious risk which has a high impact on the cost of the project (r = 4, as mentioned in Table VII) is added to a project which has a budget of 1000 USD, the actual cost is 300 USD, and the needed money to finish the remaining tasks is 600 USD, the following formula will be used:

$$Risk\ Impact\ Cost_{\text{USD}} = \begin{cases} n * 0.05, & if\ r = 1 \\ n * 0.10, & if\ r = 2 \\ n * 0.25, & if\ r = 3 \\ n * 0.50, & if\ r = 4 \\ n * 1.00, & if\ r = 5 \end{cases}$$

where, r is the risk impact on cost score, and n is the needed money to finish remaining tasks. By implementing the formula in the example, the result will be as follows:

$$Risk\ Impact\ Cost_{\text{USD}} = \begin{cases} n * 0.05, & if\ r = 1 \\ n * 0.10, & if\ r = 2 \\ n * 0.25, & if\ r = 3 \\ n * 0.50, & if\ r = 4 \\ n * 1.00, & if\ r = 5 \end{cases}$$

$$Risk\ Impact\ Cost_{\text{USD}} = n * 0.50$$

$$Risk\ Impact\ Cost_{\text{USD}} = 600 * 0.50 = 300\ KD$$

So, the risk may incur a loss of 300 USD, which will be added to the actual project cost and the needed money to finish the remaining tasks. The result is 1200 USD, which makes the project overbudget. In the same manner, the risk impact on time will be calculated. If the same risk has moderate impact on the time of the project (r = 3, as mentioned in Table VII), the tool will find the needed days to finish the remaining tasks, let's say in our example it is 30 days, then the same formula will be used where n is the needed days to finish the remaining tasks, finally, we compute the ceiling of the result to find the result in days.

$$Risk\ Impact\ Time_{\text{Day}} = \begin{cases} \lceil n * 0.05 \rceil, & if\ r = 1 \\ \lceil n * 0.10 \rceil, & if\ r = 2 \\ \lceil n * 0.25 \rceil, & if\ r = 3 \\ \lceil n * 0.50 \rceil, & if\ r = 4 \\ \lceil n * 1.00 \rceil, & if\ r = 5 \end{cases}$$

$$Risk\ Impact\ Time_{\text{Day}} = \lceil n * 0.25 \rceil$$

$$Risk\ Impact\ Time_{\text{Day}} = \lceil 30 * 0.25 \rceil = \lceil 7.50 \rceil = 8\ \text{days}$$

The risk impact on scope will be calculated in a different manner. For example, if the risk has a low impact on the scope of the project (from Table VII the r value is 2), and the current scope of the project is very good (the n value is 4 based on Table V). The scope will be calculated as follows:

$$Risk\ Impact\ Scope_{1-5} = \begin{cases} 1, & if\ n < \text{r} \\ (\text{n} - \text{r}) + 1, & if\ n \geq \text{r} \end{cases}$$

where, r is the risk impact on the scope of the project, and n is the actual scope of the project. So, by implementing the formula, the scope of the project will be as follows:

$$Risk\ Impact\ Scope_{1-5} = \begin{cases} 1, & if\ n < \text{r} \\ (\text{n} - \text{r}) + 1, & if\ n \geq \text{r} \end{cases}$$

$$Risk\ Impact\ Scope_{1-5} = (\text{n} - \text{r}) + 1$$

$$Risk\ Impact\ Scope_{1-5} = (4 - 2) + 1$$

$$Risk\ Impact\ Scope_{1-5} = 3\ (Good\ based\ in\ Table\ \text{V})$$

Finally, the analyzed serious risk is estimated to increase project cost by USD 300, delay project delivery by approximately eight days, and reduce the project scope to a *Good* level. When multiple risks exist within a project, each risk independently affects the project cost and schedule. However, the impact on project scope is determined by identifying the risk with the highest scope impact score and applying the Risk Impact on Scope formula accordingly.

10)Risk response strategy: During the risk response phase, the Risk Manager (RM) defines the actions required to treat each identified risk. Risk response strategies are generally categorized as responses to either negative risks (threats) or positive risks (opportunities) [29]. The proposed tool focuses exclusively on negative risks and supports four standard response strategies: acceptance, mitigation, transference, and elimination [26].

Acceptance involves acknowledging the risk without taking proactive action, whereas elimination seeks to remove the risk entirely by addressing its root cause. Mitigation aims to reduce the likelihood and/or impact of the risk, while transference shifts responsibility for managing the risk and its consequences to a third party [29]. In the proposed tool, acceptance retains the risk's impact within the project, while elimination removes its effects. Mitigation and transference strategies influence project performance based on predefined impact scales specified by the project manager. Any selected response strategy is documented and made available to the project manager and risk owner for implementation. Additionally, response strategies may generate secondary risks, as discussed in the following subsection.

11)Secondary risks: The execution of a risk response strategy may introduce new risks, commonly referred to as secondary risks [4]. The proposed tool explicitly supports the identification and management of such risks by allowing risk managers to link secondary risks to their originating response strategies. Secondary risks are initially assigned a Pending status and transition to Open once the associated response strategy is implemented.

For each secondary risk, the risk manager specifies a description, risk owner, impact attributes, and an appropriate response strategy. For example, consider the risk "The technology is new, and the project team lacks sufficient expertise, leading to delays". If the RM selects an elimination strategy—such as requiring all team members to attend training on the new technology prior to project start—this action may introduce a secondary risk. Specifically, team members attending training may delay their assigned tasks. This secondary risk, "Employees are assigned to mandatory training while project tasks remain incomplete", is initially marked as Pending. Once the primary response strategy is executed, the secondary risk becomes Open, and a corresponding response plan is defined to manage its impact.

12)Project health: Project health is evaluated using three indicators: cost health, time health, and scope health.

- Cost Health: Cost performance is classified as *Within Budget* (green), *Worry* (yellow), or *Critical* (red). The *Within Budget* status indicates that project spending has not entered the cost danger zone, defined as

$CostDangerZone = ProjectBudget - (ProjectBudget \times 5\%)$. Projects within budget but approaching this threshold are marked *Worry*, while projects exceeding the allocated budget or requiring additional funds are classified as *Critical*.

- Time Health: Schedule performance is categorized as *On Track*, *Worry*, or *Delay*. The time danger zone is calculated as

$TimeDangerZone = ProjectDuration - (ProjectDuration \times 5\%)$. A project is *On Track* if the estimated completion date remains within the approved duration. It is classified as *Worry* if delays approach the danger zone but remain within schedule limits, and *Delay* if the projected completion date exceeds the planned end date.

- Scope Health: Scope performance is assessed as *Excellent*, *Good*, or *Poor*. An *Excellent* scope corresponds to a score of 4.5 or higher, *Good* reflects a score between 3 and 4.5, and *Poor* indicates a score below 3.

B. Description and Scope of the Tool

RiskMIS is delivered as a web-based application designed to support organizational risk management activities. The tool enables project management, risk monitoring, and internal communication among users. Its primary focus is on supporting risk managers and project managers in managing risks and their impacts, rather than directly managing task execution by employees.

C. Requirements

A complete and structured specification of the system requirements was developed. Table VIII summarizes the functional requirements of the proposed tool, while Table IX presents the corresponding non-functional requirements.

TABLE VIII. FUNCTIONAL REQUIREMENTS OF THE PROPOSED TOOL

Category	Requirements
General Requirements	• A professional website will be designed and developed to effectively manage project risks in organizations, regardless of the business domain of the organization. • On the tool home page, the purpose and logo of the tool will be shown along with a brief description of the tool. • A link to other pages like About, Contact, Register, and Login should always be reachable from any of those pages and home page. • On the About page, a brief description of the reason for developing the tool will be provided. • On the Contact page, an email of the developer will be provided. • The tool targets organizations from all domains in both government or private sectors, and small, medium, or large organizations. • The tool requires registration of the organization by one Administrator. • Alert should be sent from the system to users if a big change has been done to their project like a new project, a new risk in the project, and requesting a new response strategy. • Users can read alerts by clicking the alert link.
Manage Employees	• The Administrator can create new employees to use the tool by filling the form which contains: the employee's name, email, ID, and role. • The roles of the users of the tool are limited to be A Project Manager, A Risk Manager, and An Employee. • When a new employee is created a verification email will be sent to the user containing a random password, if the user clicks the verification link, the user's account will be activated and then can use the email and the password to log in the tool. • The Administrator can prevent the users from using their accounts without deleting the accounts. • The Administrator can edit the user's information. • Users with the role "employee" cannot use the tool, the only reason why it's created is to assign responsibility to them in taking a practical action toward risk in the supervision of Project Manager.
Manage Risks	• The tool can manage risk by identifying project risks, analyze risks, and prepare a risk response strategy to implement. • It provides the ability to create, open, close, or suspend risks (including secondary risk). • The Risk Manager can create main categories and subcategories for the risks. • Only two-level risk categorization is allowed. • The tool provides default categories that the Risk Manager can use or delete if not needed. • The Risk Manager should specify the risk settings by ranking of probability, impact, and detectability based on its importance to the organization.

	• Risk settings specified by the organization will determine the risk impact in the project budget, time, and scope. • Risk Manager can create risks in the subcategories only and should specify the probability, impact, and detectability value of each risk. • The RM can edit created risks or delete them. • The RM can create response strategies for created risks in four types: accept, mitigate, transfer, and eliminate. • The Risk Manager can add risk to the project by determining the risk, risk owner, and the recommended response strategy. If the response strategy has a secondary risk, the RM should specify the risk owner and the response strategy for the secondary risk • The Project Manager can request a specific response strategy from the Risk Manager to prepare. • All details of project risk and impact are included in the project details. • The Project Manager should specify the implemented response strategy and its effect on cost, time, and scope of the project. • The tool can analyze the risks, calculates the probability and impact of risk on cost, time, and cost, then prioritize risks. • It can save the history of risks. • It provides different types of charts and graphs to represent risk management progress. • It can send notification automatically to the users when the status of risks or projects have changed.
Registration	• In the registration page, the Administrator should provide information about the organization like name and type, and information about the Administrator who will be the representative of the organization in the tool, like full name, civil ID, and password. • If the Administrator email already exists in the tool, an error message should appear, and registration will not be allowed. • Each organization should have only one administrator. • The administrator account is the owner of the organization record in the tool and has the highest privilege. • If the Administrator successfully submits the registration form, an activation email will be sent to the email of the Administrator with the activation link.
Communication	• All users can communicate using the tool by sending and receiving messages. • Users can send a message by filling the form with title, message, attached file if needed, and recipient. • The system will notify the user if there is a new message sent to them. • Users can read messages by clicking the notification of a new message or clicking the messages link to view all received messages.
Manage Projects	• The Administrators can create a new project "idea" by filling the form with the project's name, description, budget, start and end dates, project manager's name, and risk manager's name. • The Projects with status "Idea" will be shown only to the Administrators. • The Administrators can delete the projects with status "Idea" permanently. • The Administrators can edit the project information while in the "Idea" status.
	• The Projects can be initiated by Administrators only if all the project's information is filled. • The Administrators cannot edit Initiated projects. • The Initiated project will appear to the Project Manager and Risk Manager to whom the project is assigned. • If the project is in initiation state, a link will appear to the Project Manager to make a plan for the project • The Administrator can delete the projects after initiation only if it is in the "On Hold" state, the data of the project should be kept. • All users can view the project's details and progress by clicking the details link. • The Project Manager can make a plan to the project by filling a form, which consists of the task name, start and end dates, cost, and the requirements of the task. • The Task start and end dates and the costs should be within the project's budget and duration. • The Project Manager should create at least one task in the plan. • The Tasks of the project can be processed in parallel or serial. • The Project Manager can delete and edit plans or tasks only if the plan is not finalized/ confirmed. • If the Project Manager creates a plan for the project, a link will appear to the Risk Manager to add risks for the project. • The Project Manager can start, delete, on hold, complete, and resume tasks only if the plan is confirmed. • Any action to the task of the project should be stored in the tool like task start date, end date, cost, and scope. • The Project Manager should provide the cost and scope of the task when delete, hold or complete any task. • Task status, cost, time, and scope should be calculated and shown in the project details. • If the Project Manager wants to complete the task after resuming, the cost should be added to the previous cost of the task. • The Project's overall status, progress, and health information like cost, time, and scope should be calculated and updated continuously as the project progress and shown in the project details. • The tool should update the status of the project based on the tasks of the project status. For example, if all tasks are completed, the status of the project is "Completed". If at least one task is started, the project status will be "In process". If all tasks are on hold, the project status will be "On hold" and can be deleted. If all tasks are canceled the project status will be "Canceled". • It provides different types of charts and graphs to represent project management progress.
Logging in	• On the login page, users should fill the form with the email and password. • Only activated user accounts can log in. • Project Managers and Risk Managers can log in using the information in the email that was sent to them from the system which contains the user's email, a random password, and an activation link. • Administrators can log in using the email and password which they entered in the registration form.

	• If users forget the password, they can click the link "Forgot Password" to retrieve a new password from the tool to the user's email.

NONFUNCTIONAL REQUIREMENTS OF THE PROPOSED TOOL

Category	Requirements
Operational Requirements	• Website should be hosted on dedicated Server, with minimum of 2 x vCPU, 4 GB RAM, 2000 GB Bandwidth, 75 GB Disk Space, and 1000 Mbps Connection. • The tool should open from a common web browser like: Chrome, Firefox, IE, Safari, Edge, and Opera. • The tool should be friendly to portal devices like: Mobile and iPad. • The tool should be able to communicate with email web services to operate verification emails. • The tool should be able to communicate with google charts web service to create graphs and charts. • The tool should be able to communicate with the database. • The tool should give users the capability to upload files from different types.
Performance Requirements	• The tool should load in less than 2 secs. • The tool should be available 24/7. • The tool should always give real-time data. • The tool should be easy to navigate.
Security Requirements	• Only those who have registered usernames and valid passwords can access the tool. • Users can access the tool based on their role and function in the organization. • The Organization's projects, tasks, risks, and information should be accessible only to users with the required privileges and assigned jobs. • Login must be very secure with a maximum of three incorrect logins. • A time-out feature should be available on the tool if left idle for more than 5 minutes to protect the integrity of the organization's data. • Only developers of the tool will be able to log in to the backend of the tool to modify it.
Usability	• The tool displays the results and charts in easy to read and understand formats. • The tool is easy to use and facilitates the process of project and risk management. • The tool is user-friendly.

D. Stakeholders

The primary users of RiskMIS are Administrators, Project Managers, and Risk Managers, each interacting with the system according to their assigned roles. The Administrator holds the highest level of privilege and is responsible for creating users and configuring system access. Additional stakeholders include employees from various organizational units who execute risk response actions under the supervision of project managers. The Tool Owner is responsible for system maintenance, monitoring, error resolution, and ongoing updates.

IV. DESIGN AND IMPLEMENTATION

RiskMIS is a web-based Risk Management Information System designed to support organizational risk and project management activities. The tool is freely accessible and can be adopted by organizations of any size or domain, requiring only an internet-connected device and a standard web browser. RiskMIS is framework-agnostic and does not mandate adherence to any specific risk management standard or methodology.

RiskMIS provides integrated support for the core risk management lifecycle, consolidating risk identification, classification, assessment, response, and monitoring into a unified platform. In addition to risk management, the system offers essential project management functionalities, enabling project managers to create, plan, and track projects and tasks across their entire lifecycle. To enhance coordination and responsiveness, the tool also includes an internal communication center and an automated alert system, reducing the need for supplementary project management tools.

The system is implemented using the open-source ASP.NET Core framework and developed in C#. Microsoft SQL Server 2018 is used for data management, and Microsoft Visual Studio 2017 supported the development process. The current implementation comprises approximately 74,800 lines of source code and includes 40 ASPX-based web pages.

1) Overall architecture: RiskMIS follows a three-tier architectural model consisting of the Presentation Layer, Business Access Layer (BAL), and Data Access Layer (DAL). The Presentation Layer provides the user interface through web forms implemented using HTML, CSS, and JavaScript, ensuring compatibility across modern browsers and devices. The BAL, developed in C#, contains the application logic and mediates interactions between the user interface and the database. The DAL encapsulates data persistence functionality and performs Create, Read, Update, and Delete (CRUD) operations on the underlying database implemented using Microsoft SQL Server Management Studio 18.

In addition to core system components, RiskMIS integrates external services for email-based user verification and notification, as well as Google Chart services for visualizing project and risk-related data. The overall system architecture is illustrated in Fig. 1.

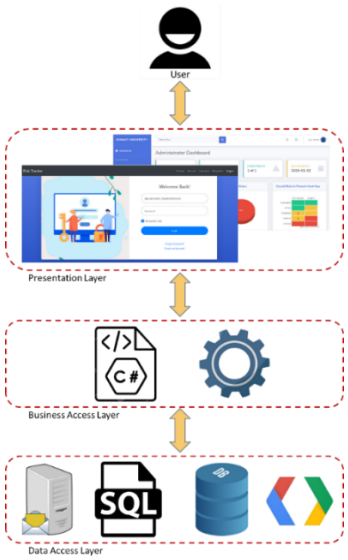

Fig. 1. RiskMIS architecture.

2) Use case model: The system's functionality is captured using a use case model that describes interactions between users and RiskMIS. Three primary user roles are defined: Administrator, Project Manager, and Risk Manager. The Administrator, typically representing top management, holds the highest level of privilege and is responsible for creating and managing users, assigning project and risk managers, and initializing project information. The Risk Manager oversees organizational and project-level risk activities, including risk configuration, prioritization, and monitoring. The Project Manager is responsible for managing the project lifecycle and implementing risk response actions. Fig. 2 presents the use case diagram depicting these roles and their interactions with the system.

Fig. 2. Use case diagram.

3) Activity diagrams: Activity diagrams are used to model and clarify key system workflows. Fig. 3 illustrates the login and dashboard access process common to all users. After credentials are submitted, the system validates the user's email and password against stored records. To enhance security, accounts are temporarily blocked after three consecutive failed login attempts, and a verification email containing a new activation link and password is automatically sent to the user.

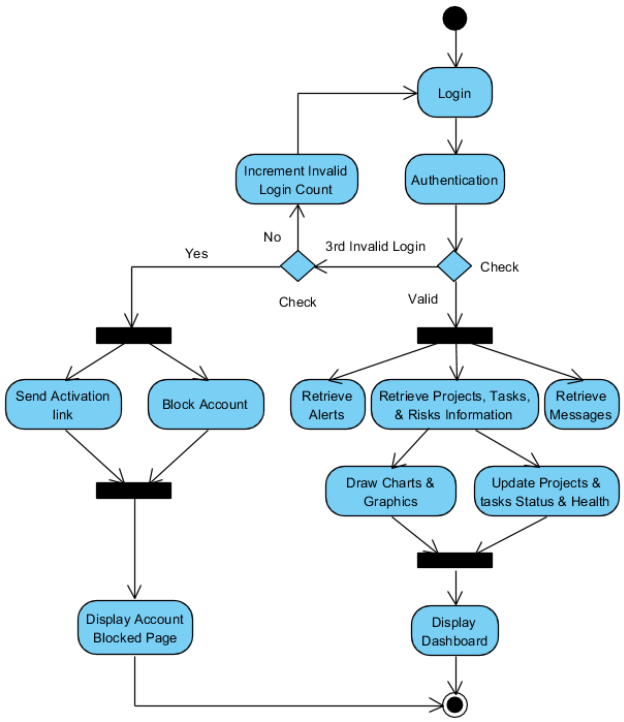

Fig. 3. Activity diagram for dashboard page display.

Fig. 4, Fig. 5, and Fig. 6 present activity diagrams specific to the Administrator, Project Manager, and Risk Manager, respectively, highlighting role-based workflows within RiskMIS.

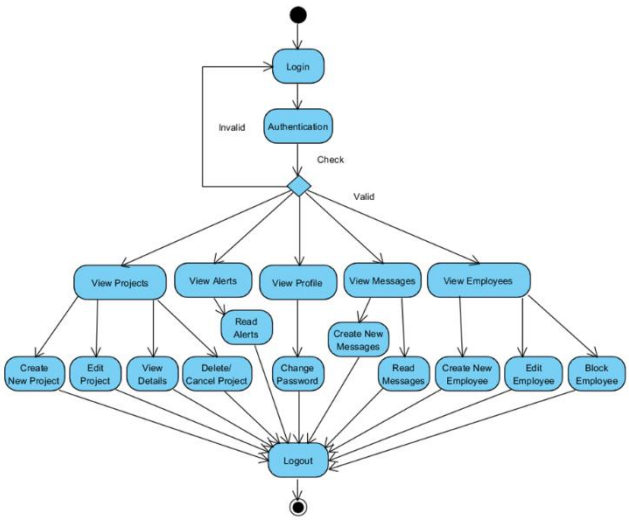

Fig. 4. Activity diagram for the administrator side.

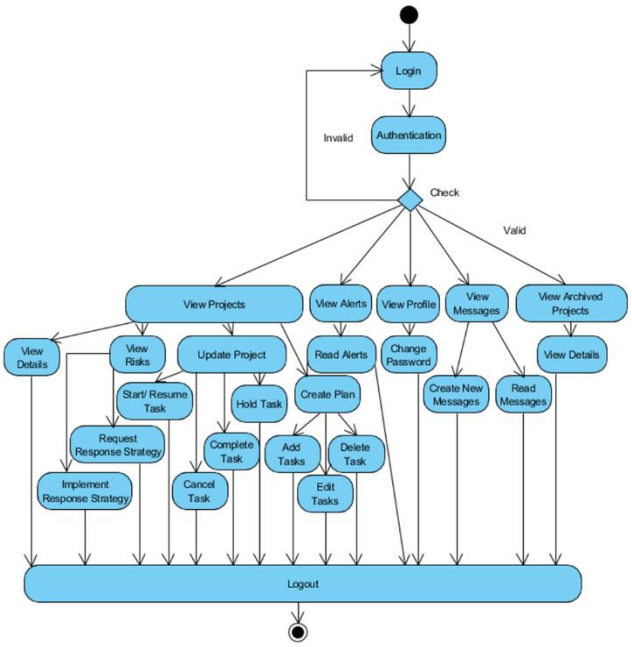

Fig. 5. Activity diagram for the project manager side.

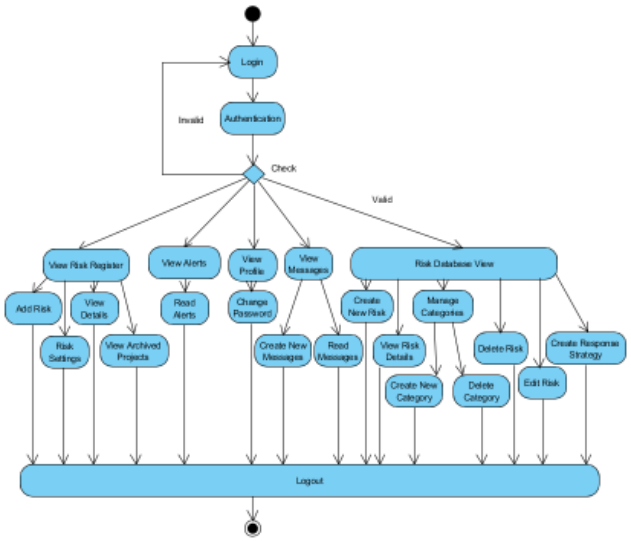

Fig. 6. Activity diagram for the risk manager side.

4) Finite state machines: RiskMIS behavior is formally represented using four finite state machines (statechart diagrams):

- Account State: Newly created accounts begin in a Not Verified state. Upon email verification, the account transitions to Active. Repeated invalid login attempts result in a Blocked state, from which the account can be reactivated via email verification. Administrators may also suspend or permanently delete accounts, as shown in Fig. 7.

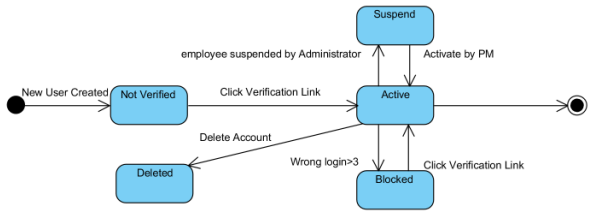

Fig. 7. Statechart diagram for the account state.

- Project State: Projects initially enter the Idea state, where they may be modified or deleted. Once project details are finalized, the project transitions to Initiate, granting access to the Project Manager. Subsequent task creation moves the project to the Plan state, followed by In Process, On Hold, Completed, or Canceled states depending on task progression and administrative actions (see Fig. 8).

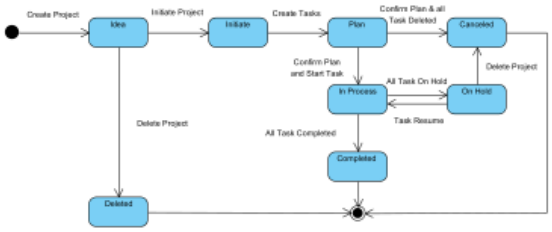

Fig. 8. Statechart diagram for the project state.

- Task State: Tasks start in the Not Started state after plan confirmation. They transition to In Process when execution begins, Delayed if planned timelines are exceeded, On Hold if temporarily suspended, and Completed once all requirements are satisfied (see Fig. 9).

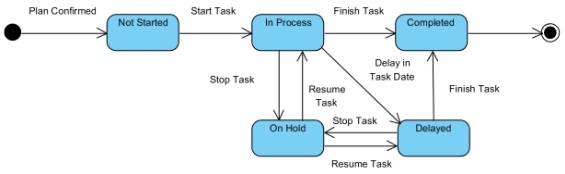

Fig. 9. Statechart diagram for the task state.

- Risk State: Risks initially exist in a Created state and transition to Open when associated with a project. Secondary risks generated through response strategies are initially marked as Pending and become Open once the corresponding response strategy is implemented (Fig. 10).

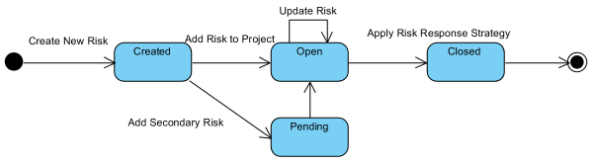

Fig. 10. Statechart diagram for the risk state.

5) Data model using the entity relationship diagram: RiskMIS relies on a relational database to support its functionalities. The database schema, implemented using Microsoft SQL Server Management Studio 18, consists of 14 tables: OrganizationTypes, Organizations, RiskSettings, AlertsFromSystem, EmployeesRole, Employees, Projects, Messages, MessageReceivers, Tasks, Risks, RisksInProjects, ResponseStrategy, and RiskCategories. These entities and their relationships are represented using an Entity Relationship (ER) diagram, as shown in Fig. 11.

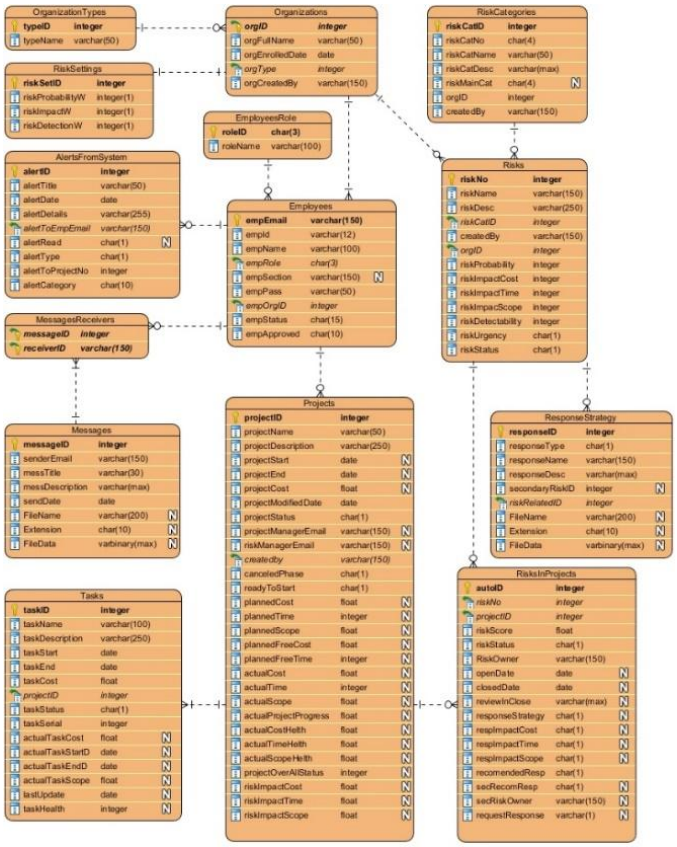

Fig. 11. Database schema for the RiskMIS.

V. Prototype Demonstration

To validate the practicality and effectiveness of the proposed RiskMIS, a fully functional web-based prototype was implemented and evaluated against the requirements defined earlier in the study. Rather than emphasizing user interface details, the demonstration focuses on what the prototype *proves* in terms of integrating project lifecycle management with continuous risk management.

Fig. 12 and Fig. 13 illustrate two important dashboards, which serve as the primary decision-support interfaces for all roles. These dashboards aggregate project and risk data in real-time and present key indicators such as project status distribution, budget utilization, projects at risk, and a risk heat map. This visualization demonstrates the system's ability to transform risk register data into actionable insights, enabling managers to rapidly identify high-risk projects and prioritize response actions without navigating multiple views or reports.

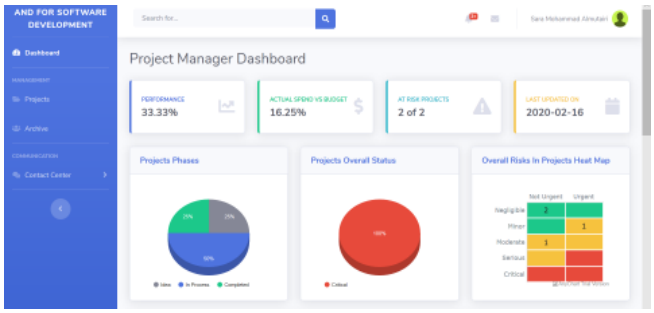

Fig. 12. Dashboard in the RiskMIS: statistics.

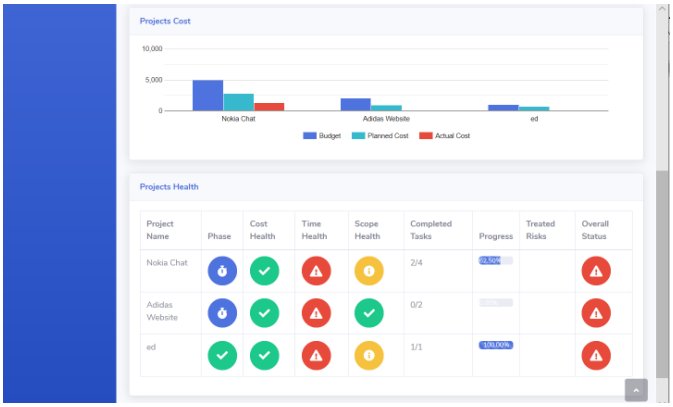

Fig. 13. Dashboard in the RiskMIS: information.

The prototype confirms that project lifecycle control and risk management are tightly coupled. Projects progress through predefined states, and task execution directly influences project health indicators related to cost, time, and scope. As risks are added or updated, their quantified impacts are automatically propagated to project performance metrics, demonstrating that risk assessment is not treated as a static activity but as a continuous driver of project status.

RiskMIS further demonstrates structured and consistent risk handling through a centralized risk register. Risks are categorized, assessed using standardized qualitative criteria, and prioritized according to organizational risk preferences. The prototype shows that recommended response strategies—acceptance, mitigation, transference, or elimination—are systematically linked to project execution. Importantly, the system proves its ability to manage secondary risks generated by response actions, reinforcing continuous monitoring and control throughout the project lifecycle.

Overall, the prototype demonstrates that RiskMIS can effectively unify project management and risk management within a single platform, providing real-time visibility into risk exposure and its operational consequences. This integration supports informed decision-making and proactive risk treatment across projects and ongoing operations.

The current evaluation is limited to functional validation using predefined scenarios and qualitative risk data. Large-scale empirical validation, performance benchmarking, and longitudinal studies in real organizational settings are planned as future work to assess scalability, user adoption, and decision-quality impact.

VI. Summary, Conclusion and Future Work

The primary objective of any organization is to deliver high-quality products or services that meet stakeholder requirements within defined time and budget constraints. Effective risk management is essential to achieving this objective, as it reduces uncertainty and supports informed decision-making. Central to this process is the risk register, which serves as a continuously updated repository of risk information and enables systematic identification, analysis, monitoring, and treatment of risks across project lifecycles and ongoing operations.

In this study, we conducted an extensive review of the risk management literature to identify key concepts, challenges, and research gaps. Building on this analysis, we defined the problem, proposed a solution, specified system requirements, and designed, implemented, and tested a comprehensive risk management information system. The main conclusions of this work are summarized as follows:

- Manual versus Automated Risk Management: Manual tools, such as word processors and spreadsheets, are inefficient and error-prone for managing risks. An integrated and automated risk management information system significantly enhances the consistency, efficiency, and effectiveness of risk identification, analysis, and treatment throughout the project lifecycle.
- Central Role of the Risk Register: The risk register is the core component of an effective risk management system. Its value depends on being comprehensive, dynamically maintained, and tightly integrated with all stages of the risk management process.
- Flexible Risk Classification: No single risk classification scheme is sufficient for all application domains. While the Larson and Gray classification is provided as a default, the proposed tool allows organizations to define and adapt classifications that reflect their specific context and risk landscape.
- Organization-Specific Risk Criteria: Consistent risk evaluation requires clearly defined and shared risk criteria. The system provides a generic yet extensible framework for defining risk probability, impacts on cost, time, and scope, detectability, and urgency.
- Generic Risk Management Framework: The tool implements a continuous and domain-independent risk management framework comprising five core activities: risk identification, classification, assessment, response, and monitoring and control. This framework is supported by explicit project and task lifecycles and state models.
- Structured Risk Prioritization: A multi-step risk prioritization methodology is introduced, enabling organizations to weight risk factors according to their priorities, compute risk scores, incorporate urgency, and classify risks on a standardized scale from negligible to critical.
- Integration with Project Performance Metrics: The system automatically propagates risk impacts to project cost, schedule, and scope using predefined formulas, ensuring that risk exposure is transparently reflected in project performance indicators.
- Management of Negative and Secondary Risks: The tool focuses on negative risks and supports systematic selection and implementation of response strategies. It also explicitly models secondary risks arising from response actions, enabling more comprehensive and continuous risk treatment.
- Web-Based and Framework-Agnostic Design: RiskMIS is implemented as a web-based, generic solution that can be readily adopted by organizations of different sizes and domains, without enforcing compliance with a specific risk management standard.

We are planning to evaluate RiskMIS through longitudinal case studies in real organizational settings. User interviews and empirical analyses will be conducted to assess system effectiveness, usability, and organizational impact. Future enhancements may include advanced analytics, intelligent risk trend detection, enhanced notification mechanisms, and broader user participation by enabling employees at all levels to report and review risks directly.

Future research will prioritize rigorous technical and empirical validation of the proposed RiskMIS through systematic performance benchmarking under realistic operational conditions to evaluate response time, scalability, and database efficiency. Clear quantitative evaluation metrics will be established to objectively assess system efficiency, transparency, decision-support effectiveness, and measurable impacts on risk exposure reduction, mitigation timelines, and decision-making accuracy through controlled case studies. In parallel, future work will incorporate formal security assessments covering authentication, authorization, and data protection mechanisms, alongside the integration of version control and change-tracking features to strengthen auditability and governance capabilities. Further studies will examine comprehensive data lifecycle management strategies, including archival policies, regular system maintenance procedures, automated backups, update deployment strategies, and long-term risk retention models. Finally, cross-organizational validation across multiple sectors, together with structured user training and onboarding frameworks, will be explored to enhance generalizability, system adoption, and sustainable usability transition.

References

[1] AFP. (2018). Risk survey report- key findings. Bethesda, MD, Association for Financial Professionals.

[2] Ahmeti, R., & Vladi, B. (2017). Risk management in public sector: a literature review. European Journal of Multidisciplinary Studies, 2(5), 323-329.

[3] Boehm, B. (1991). Software risk management: principles and practices. IEEE Software, 8(1), 32-41.

[4] Burcar, I., & Radujkovic, M. (2005). Risk registers in construction in Croatia. Proceedings of the Twenty First Annual Conference ARCOM, London, 171-178.

[5] Burcar, I., Radujkovic, M, Vukomanovic, M. (2013). Risk register development and implementation for construction projects. Gradevinar, 65(1), 23-35.

[6] Chihuri, S., & Pretorius, L. (2010). Managingrisk for success in a South African Engineering and Construction Project Environment. South African Journal of Industrial Engineering, 21(2), 63-77.

[7] CMMI Product Team. (2002). CMMI for software engineering, Version 1.1, Continuous Representation. Software Engineering Institute.

[8] De Wet, B & Visser, JK 2013, 'An evaluation of software project risk management in South Africa', South African Journal of Industrial Engineering, vol. 24, no. 1, pp. 14-28.

[9] Deloitte Touche Tohmatsu Limited (2017). Global risk management survey (10th ed.). Heightened uncertainty signals new challenges ahead. Deloitte University Press.

[10] Esteves, J., Pastor, J., Rodriguez, N., and Roy, R. (2004). Implementing and improving the SEI risk management method in a University Software Project. IEEE Latin America Transactions, 3(1), 90-97.

[11] GRA. (2005). Risk management guide for small business. Sydney, Global Risk Alliance Pty Ltd jointly with NSW Department of State and Regional Development.

[12] Hillson, D. (2003). Using a risk breakdown structure in project management. Journal of Facilities Management, 2(1), 85-97.

[13] Hopkin, P. (2010). Fundamentals of risk management: understanding, evaluating, and implementing effective risk management. UK, The Institute of Risk Management.

[14] IRM. (2018). A risk practitioners guide to ISO 31000. London, Institute of Risk Management.

[15] ISO. (2009). Guide 73: Risk management- vocabulary. Switzerland, International Organization for Standardization.

[16] ISO. (2018). ISO 31000: Risk Management - Guidelines (3rd ed.). Switzerland, International Organization for Standardization.

[17] Junior, R., & Carvalho, M. (2013). Understanding the impact of project risk management on project performance: an empirical study. Journal of Technology Management & Innovation, 8 (Special Issue ALTEC), 64-78.

[18] Kontio, J. (1997). The riskit method for software risk management, Version 1.00. Computer Science Technical Reports. University of Maryland, College Park, MD, USA.

[19] Larson, E., & Gray, C. (2015). Project management the managerial process (5th ed.). New York, McGraw-Hill

[20] Leva, M.C., Balfe, N., & McAleer, B. (2017). Risk registers: structuring data collection to develop risk intelligence. Safety Science, 100 (part B), 143-156.

[21] Liu, H., Deng, X., & Jiang, W. (2017). Risk evaluation in failure mode and effects analysis. Symmetry, 9 (62), 1-13.

[22] Martins, C. (2017). HoliRisk – risk assessment framework. Instituto Superior Técnico, Portugal.

[23] Mastroianni, S. (2011). Risk management among research and development projects (Master's thesis). Lehigh University.

[24] Mateus, G. (2016). A reference risk register for information security according to ISO/IEC 27005 (Master's thesis). Department of Science and Technology, Instituto Superior Técnico.

[25] Object Management Group. (2017). Unified Modeling Language (UML) Version 2.5.1. https://www.omg.org/spec/UML/2.5.1

[26] Onengiyeofori, O. (2016). Risk management system to guide building construction projects in developing countries: a case study of Nigeria (Doctoral dissertation). Faculty of Science and Engineering, University of Wolverhampton.

[27] Patterson, FD., & Neailey, K. (2002). A risk register database system to aid the management of project risk. International Journal of Project Management, 20(5), 365-374.

[28] PMI. (2025). A guide to the project management body of knowledge: PMBOK Guide (8th ed.). Pennsylvania, Project Management Institute, Inc.

[29] Pritchard, C. (2015). Risk management concepts and guidance (5th ed.). Boca Raton, CRC Press.

[30] Rehacek, P. (2017). Risk management standards for project management. International Journal of Advanced and Applied Sciences, 4(6), 1-13.

[31] Rodage, H., Lei, H. & Ganjeizadeh, F. (2014). Risk management for research and development projects. International Journal of Engineering Research & Technology, 3(10), 824-831

[32] Rorvik, K. (2013). Risk management in a complex frame agreement - a case study from a contractors perspective (Master's thesis). Faculty of Science and Technology, University of Stavanger.

[33] Saffin, T. & Laryea, S. (2012). The use of risk registers by project managers. In: 4th West Africa Built Environment Research (WABER) Conference, 2426 July 2012, Abuja, Nigeria, 1305-1318. Available at http://centaur.reading.ac.uk/30322/

[34] Saleh, K. (2009). Software Engineering (1st ed.). J. Ross Publishing, 26-28

[35] The Standish Group. (2020). CHAOS report 2020: Beyond Infinity.

[36] Uzulans, J. (2016). Project risk register analysis based on the theoretical analysis of project management notion of risk. Economics and Business, 29(1), 43-48.

[37] Vaz, L. (2016). Risk management in information systems projects (Master's thesis). Department of Science and Technology, Instituto Superior Técnico.