RISK MANAGEMENT MAGAZINE

Vol. 19, Issue 3
September – December 2024

EXCERPT

https://www.aifirm.it/rivista/progetto-editoriale/

Enhancing IT Project Success Through Risk and Vulnerability Management: the Armenian Case

Armen Ghazaryan, Soomela Moosa Moghadam, Inesa Grigoryan

Enhancing IT Project Success Through Risk and Vulnerability Management: The Armenian Case

Armen Ghazaryan (Armenian State University of Economics – ASUE), Soomela Moosa Moghadam (Armenian State University of Economics – ASUE), Inesa Grigoryan (Armenian State University of Economics – ASUE)

Corresponding author: Armen Ghazaryan (armenghazaryan@mail.ru)

Abstract

The research aimed to identify and evaluate the risks associated with IT projects, particularly focusing on their impacts. Despite numerous efforts, a significant number of software projects still fail to achieve success; however, these risks can be effectively managed. This study outlines methodologies for examining how different risks influence software projects, using statistical analyses and models to uncover causal relationships. A survey was also conducted to assess critical risk factors, highlighting three key factors that have the greatest influence. The findings suggest that addressing these factors can improve decision-making, thereby increasing the likelihood of project success.

Keywords: Armenian IT organizations, IT risk strategies, risk management, risk analysis, risk identification, risk monitoring, financial risks

1. Introduction

The purpose of this work is to identify both planned and unplanned risks encountered in the projects based on the experience of IT organizations and to analyze them. To achieve this goal, the following tasks were set:

- consider widely used methods for risk management in IT projects, including their pros and cons;
- collect data through a survey on the impact of risks on project performance in IT organizations;
- use statistical analysis to make a brief and meaningful summary of the main features of the database, analyze the differences between different categories of risks and the interrelationships between risks;
- divide the set of variables to be studied by means of factor analysis into a small number of groups, reducing the factors we have;
- use logistic analysis to find out which risks have a higher probability of impact on the success of the project;
- present summary conclusions and recommendations related to risks, management in IT projects.

The database for this article was formed by the data of a survey conducted among specialists of IT organizations, and the information basis included the researches, articles dedicated to IT projects by foreign authors of the IT sector, analyses conducted by international organizations, reports by the Project Management Institute (PMI), and completed reports and other materials.

Insights from foreign IT authors provide a global perspective, enriching the understanding of risk management practices. Analyses conducted by international organizations contribute to a comprehensive understanding of the challenges facing IT projects worldwide. Involving IT professionals, project managers, and organizational leaders in the research process provides a holistic view of the challenges and opportunities associated with risk management.

To pursue a comprehensive understanding of IT project risks, the research methodology employed in this study emphasizes advanced analytical tools. Table and graphic representation, descriptive, single factor (Anova: Single factor) and correlation analysis (Correlation) tools of MS-Excel software package, as well as factor analysis methods were used as research tools. The use of statistical techniques such as machine learning algorithms and predictive modeling enables more nuanced analysis of complex data sets. This methodological rigor goes beyond traditional approaches, providing a deeper understanding of the complex relationships between variables and the potential emergence of unpredictable risks.

This research seeks to provide actionable insights that can empower organizations to successfully face the complexities of modern projects. By examining widely used methods, surveying practitioners, and applying advanced statistical analyses, the study aims to contribute to a more nuanced understanding of risks in the ever-evolving technology landscape.

The expected results can serve as a practical guide for organizations, offering strategic recommendations for effective risk management in IT projects. In general, it can be concluded that the results along with the knowledge and tools can be useful for mitigating risk management problems in IT projects under the conditions of uncertainty. Integral to effective risk management is the ability to learn from experience, both successes and failures. Organizations that foster a culture of continuous learning and adaptation build resilience from the ground up. Each project becomes a repository of lessons, contributing to the organizational knowledge base. This approach not only strengthens risk management capabilities, but also fortifies the organization against future uncertainties.

The paper is organized into five sections. Section 1 introduces the background, aim, and significance of the study, while Section 2 provides a literature review on IT risk management, categorizing risks into pure and financial. Sections 3, 4, and 5 cover the research methodology, analysis and results, and the study's conclusions, respectively, highlighting key findings and their implications for IT project management.

2. Literature review

Risk management is a critical component of any organizational strategy, particularly in IT projects, where risks are dynamic and multifaceted. Unlike traditional forms of risk management that focus on general business or operational risks, IT risk management specifically addresses the uncertainties and challenges that arise from the use of information technology. It is essential to distinguish between pure risks, which involve the possibility of loss without any potential for gain, and financial risks, which can include both potential losses and gains depending on investment outcomes. This section explores the specificities of IT risk in the literature, with a focus on cybersecurity, data integrity, system downtime, and regulatory compliance, while addressing both pure and financial risks. IT risk, as defined by ISACA (2013), refers to the possibility that a given event or action could negatively impact the performance, security, or operational capacity of an organization's IT systems. IT risks are unique due to their rapidly changing nature, the complexity of IT infrastructures, and the broad range of potential threats, such as technological obsolescence, cyberattacks, and human error. These risks require tailored approaches that address both pure and financial risks, given the central role of IT in modern businesses.

Pure risks involve scenarios where only negative outcomes are possible, such as data breaches, system failures, or malware attacks. These risks typically require proactive management strategies aimed at preventing or minimizing potential damage. For example, the increasing frequency of cyberattacks has led to heightened attention to cybersecurity risks. Studies by Aven (2016) and Ponemon Institute (2020) highlight how breaches can lead to data loss, legal consequences, and reputational damage, all of which are forms of pure risk. To mitigate these risks, organizations are encouraged to implement strong security protocols, including firewalls, encryption, and continuous monitoring.

Financial risks, on the other hand, involve decisions where there is a chance of both loss and gain. For instance, investments in new IT systems, such as cloud infrastructure or advanced cybersecurity tools, carry financial risks. While the investment may lead to improved efficiency or enhanced security, there is also the potential for cost overruns or underperformance. McNeil et al. (2015) discuss how financial risk management tools, such as cost-benefit analysis, scenario planning, and sensitivity analysis can help organizations balance these risks, ensuring that investments in IT align with both the potential benefits and the risks involved.

One of the most critical aspects of IT risk management is cybersecurity, which is consistently ranked as a top concern for organizations (Deloitte, 2018). The literature emphasizes the evolving nature of cybersecurity threats, including phishing attacks, ransomware, and data breaches. A study by Westerman et al. (2014) shows how breaches can result in the loss of sensitive data, disruption of operations, and damage to customer trust. These are classic examples of pure risks in the IT domain—there are no potential gains from such events, only negative outcomes.

However, managing these risks often involves financial decisions, such as investing in cybersecurity solutions, hiring experts, or adopting cloud-based security services. In these cases, the financial risk of over-investment must be balanced with the pure risk of a breach, demonstrating the dual nature of risk in IT management.

The integrity and availability of data are also key risk areas in IT projects. Bezzina and Terribile (2019) highlight how issues, such as data corruption, accidental deletions, or unauthorized access can compromise the value and usability of critical business information. Downtime, whether caused by system failures or cyberattacks, can result in significant financial losses, especially in sectors that rely heavily on digital operations, such as finance and e-commerce (Henderson, 2017).

System downtime introduces a combination of pure and financial risks. Pure risks arise when downtime results in immediate losses, such as lost transactions or reduced customer satisfaction. Financial risks are present when organizations invest in preventative technologies such as redundant systems or disaster recovery plans, as these investments must be justified through potential cost savings or performance improvements (Schmidt and Altman, 2018).

As IT systems handle increasing amounts of personal and sensitive data, compliance with data protection regulations becomes a significant risk factor. Failure to comply with laws, such as the GDPR or HIPAA can lead to severe fines and legal action, creating a pure risk scenario. Choudhury and Vithal (2020) argue that organizations must not only protect data but also ensure that their systems and processes comply with relevant regulations. Compliance risks often lead to financial risks when organizations must invest in compliance measures, audits, or tools, such as encryption and data loss prevention (DLP) systems. These financial risks, while necessary, require careful planning and budgeting to ensure that they do not outweigh the benefits of regulatory compliance.

As highlighted, risk management in IT must address both pure risks (where the objective is loss prevention) and financial risks (where investments in IT infrastructure or risk mitigation are evaluated for potential gains and losses). This duality is essential in the IT field, where technology evolves rapidly and investments can quickly become outdated or ineffective. De Marco and Lister (2003) underscore the need for proactive risk management that distinguishes between these two types of risks, allowing for a balanced approach that mitigates losses while capitalizing on technological advancements.

The literature reveals that IT risk management involves complex, multi-dimensional risks that require both preventive and strategic financial planning. Effective management must consider the specificities of IT risks, such as cybersecurity, data integrity, system downtime, and compliance, while distinguishing between pure and financial risks. Organizations that implement comprehensive IT risk management strategies are better positioned to avoid negative outcomes while also leveraging opportunities for growth and innovation. In his research Dale Cooper emphasizes that risk management in projects is important for:

- managers, as it improves the basis for making appropriate decisions to meet operational requirements and achieve project objectives;
- the project staff, as it helps to identify things that can go wrong in the project process and suggests ways to solve them effectively;
- end-users, as it contributes to meeting needs and achieving value for money in the acquisition of key assets and capabilities;
- suppliers and contractors, because a sensible approach to risk in projects leads to better planning and better results for sellers as well as buyers;
- financiers who need to ensure that they receive a financial reward commensurate with the risks involved;
- insurers who require the comfort that risks are intelligently managed within the plan to determine how much to charge and whether to charge residual risk funding.

Risk management drives better business and project outcomes by providing insight, knowledge, and confidence to make better decisions. In particular, it supports better planning for contingencies, better allocation of resources to risks and alignment of project budgets, and better decision-making on the best allocation of risk among the parties involved in project activities. Together, they lead to increased certainty and reduced overall risk exposure. Risk management also provides a framework to avoid sudden surprises that can be applied at all stages of the project cycle, starting from the earliest stages of evaluating the strategy for the supply, operation, maintenance, and disposal of individual items, facilities, or assets. Risk management will also provide benefits for better accountability and justification in decisions by providing a consistent process that supports decision-making.

During project implementation, the project team oversees all aspects, including risk management. In the article "Risk Management in Distributed IT Projects: Integrating Strategic, Tactical, and Operational Levels" that process is based on the CMMI model and includes 10 activities (Figure 1) aimed at simplifying and improving communication with stakeholders. It integrates the PMBOK Guide and MSF principles, starting with planning, identifying stakeholders, and adapting risk management strategies to align with organizational software development processes.

Among those activities, risk identification involves the project team and stakeholders looking for potential risks using planned techniques. It takes into account the project's requirements, assumptions, and constraints.

A standard list of risks based on previous projects can be used. These risks are then analyzed on a scale of 1 to 5 based on the likelihood and potential impact on project objectives.

The technical manager and the project manager work together to finalize the risk list. The fourth activity focuses on critical risk response planning, specifying response types, responsible parties, and timelines. The fifth activity involves following up on these planned responses and monitoring the probability of risk, and impact.

In the event of risk, unforeseen actions are taken, the control of which is defined in the sixth activity. Reporting of risk status (activity seven) takes place, which is reviewed by senior managers (activity eight).

After the project, the lessons learned are recorded in the risk database for future projects (the ninth activity). The 10th activity involves the review of the risks identified by the technical manager and the project manager.

By following this structured approach, project managers can proactively address risks, make informed decisions, and take the necessary actions to ensure project success.

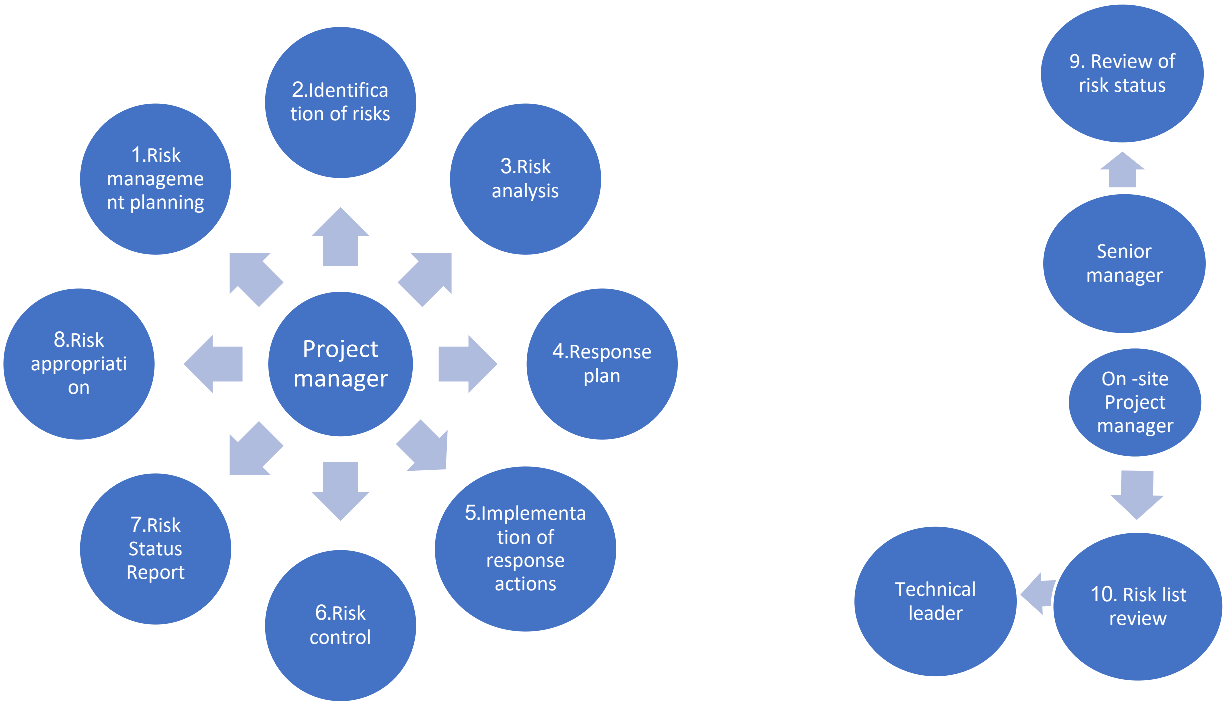


Figure 1. Project allocation to software design centers

Source: Rafael Prikladnicki, J. Roberto Evaristo, Jorge Luis Nicolas Audy, Marcelo Hideki Yamaguti: Risk Management in Distributed IT Projects: Integrating Strategic, Tactical, and Operational Levels, 2006

In their research, Bennett, Lienz, and Lee (2006) addressed the variety and complexity of common IT project risks, classifying them into three main types: internal issues and risks, external issues and risks, and issues and risks in specific IT activities.

Internal issues and risks refer to factors within the organization and project team.

These include team challenges, work being done, business units, governance, projects, and resistance to change. Controlling these problems is usually more feasible.

External issues and risks relate to external stakeholders and factors beyond the direct control of the IT team.

These include vendors, consultants, outsourcing, headquarters, international subsidiaries, technology, and business partners.

These issues are often more complex and political and may take longer to resolve.

Problems and risks in specific IT activities are associated with various phases of IT project life cycle, including analysis, software packages, development, implementation, and operations/support.

Each stage represents a distinct set of challenges.

In his study "Software Risk Management: Principles and Practices", Barry Boehm presents the top 10 software risk points and management techniques for each point:

Risk	Risk management techniques
Lack of personnel	Top talent recruitment, job matching, team building, training
Unrealistic timelines and budgets	Detailed cost and schedule estimation, design, incremental development, software reuse, requirements review, and refinement
Development of incorrect functions and properties	Organization analysis, mission analysis, operations formulation, user surveys and user participation, early user prototyping, quality factor analysis
Poor user interface development	Prototyping, scripts, task analysis, user participation
Over-engineering, adding features or elements	Requirements gathering, prototyping, cost-benefit analysis, cost-based design
A continuous flow of requirements changes	High change threshold, incremental development (postponing changes to later additions)
Defects in outfitted components	Benchmarking, checks, link checking, compatibility analysis
Deficiencies in task performance	Reference checking, pre-auditing, royalty contracts, competitive design or prototyping, team building
Real-time performance deficiencies	Modeling, benchmarking, prototyping, instrumentation
Computer science capability limitation	Technical analysis, cost-benefit analysis, prototyping, reference checking

Table 1. Top ten risks. Source: Barry Boehm "Software Risk Management: Principles and Practices" https://www.cs.virginia.edu/~sherriff/papers/Boehm%20-%201991.pdf, pp. 35

The author emphasizes a structured approach to risk mitigation techniques in IT projects, highlighting the importance of a top-10 risk tracking system. It outlines the following main points:

Risk resolution process. The process of mitigating risk in IT projects involves implementing strategies such as prototyping, simulation, benchmarking, and research per risk management plans.

Risk monitoring. Continuous monitoring of risk mitigation progress is critical to maintaining a closed process. It ensures that corrective actions are taken when needed to stay on track.

Tracking the top 10 risks. A critical aspect of risk management, this technique involves ranking the most important risks in a project and conducting regular reviews led by top management. The reviews focus on the top 10 risks, including their current ratings, history, and progress updates.

Centralization of management. By focusing management's attention on high-risk, high-leverage, and critical success factors, this approach saves time, reduces surprises, and enables managers to make a meaningful difference in project success.

Efficiency. The top-10 risk list ensures that management time is used effectively as it pinpoints issues where management intervention can be most effective.

Adaptability. The list can evolve with new concerns added and others removed based on their priority and progress, making it a dynamic and adaptive risk management tool.

In summary, the author advocates a structured, effective, and dynamic approach to reducing risk in IT projects by tracking top 10 risks, which keeps management focused on critical success factors and accelerates problem resolution.
Published by the Project Management Institute, *The Standard for Risk Management in Portfolios, Programs, and Projects* (2019) highlights the various techniques and methodologies used in IT project risk management, providing a comprehensive overview of the tools and processes used in the risk management lifecycle. It categorizes these techniques into three main types: templates and lists, process techniques, and quantitative techniques. These methods are designed to help identify, assess, and mitigate risks in IT projects. Risk management planning in the planning phase is very important to establish a common understanding of the risk approach and to document the risk management plan, which includes elements such as risk methodology, organization, roles, and communication plans.

Risk identification is a key step that includes techniques such as brainstorming, Delphi, interviews, historical data analysis, and SWOT analysis Tharanga, D. (2020). The book highlights the importance, threats, and opportunities of the methods.

Qualitative and quantitative risk analysis techniques help prioritize risks and provide a basis for resource allocation and response planning. Techniques such as affinity diagrams, probability and impact matrices, and sensitivity analysis play an important role at this stage.

Quantitative risk analysis aims to determine the overall risk for project objectives using methods such as decision tree analysis, expected monetary value (EMV) calculations, and Monte Carlo simulation.

In summary, risk management is an integral part of effective management, serving as the basis for achieving strong business and project outcomes, and effective procurement of goods and services.

Systematic risk identification, analysis, evaluation, and review of results significantly contribute to the success of projects. Researchers have developed a number of risk management methods in IT projects and different techniques and methodologies used in management, which can be selected to adapt to the needs, requirements and circumstances of the project. Risk should be considered in the earliest stages of project planning, and activities should continue throughout the project. Risk management plans and measures should be an integral part of the organization's management processes.

As IT systems become a critical competitive element in many industries, technology projects become larger, connecting more parts of the organization and putting the company at risk if something goes wrong. Unfortunately, projects often go wrong. Research by McKinsey with the University of Oxford shows that half of all large IT projects, defined as projects with an initial cost of more than $15 million, massively blow their budgets. On average, large IT projects are delivered 45 percent over budget and 7 percent over time, while delivering 56 percent less value than forecast. Software projects face the highest risks of cost and schedule overruns.

In a study of more than 5,400 IT projects by McKinsey and Oxford University's Center for Major Project Management, after comparing budgets, schedules, and projected performance benefits with actual costs and results, these IT projects were found to have a total of $66 billion in overruns, more than the GDP of Luxembourg Heygate (1994). It also found that the longer a project is planned to run, the more likely it is to run over time and budget, with each additional year spent on the project increasing cost overruns by 15 percent.

Surveys of IT leaders have shown that the key to success is embracing four values that together make up the IT project methodology:

- a focus on strategy and stakeholder management instead of focusing solely on budget and planning
- assimilation of technology and project content
- building effective teams
- following key project management practices, such as strict quality checks.

Failure to master two of these typically accounts for almost half of the costs, while poor performance on the second two measures accounts for an additional 40 percent of the overhead.

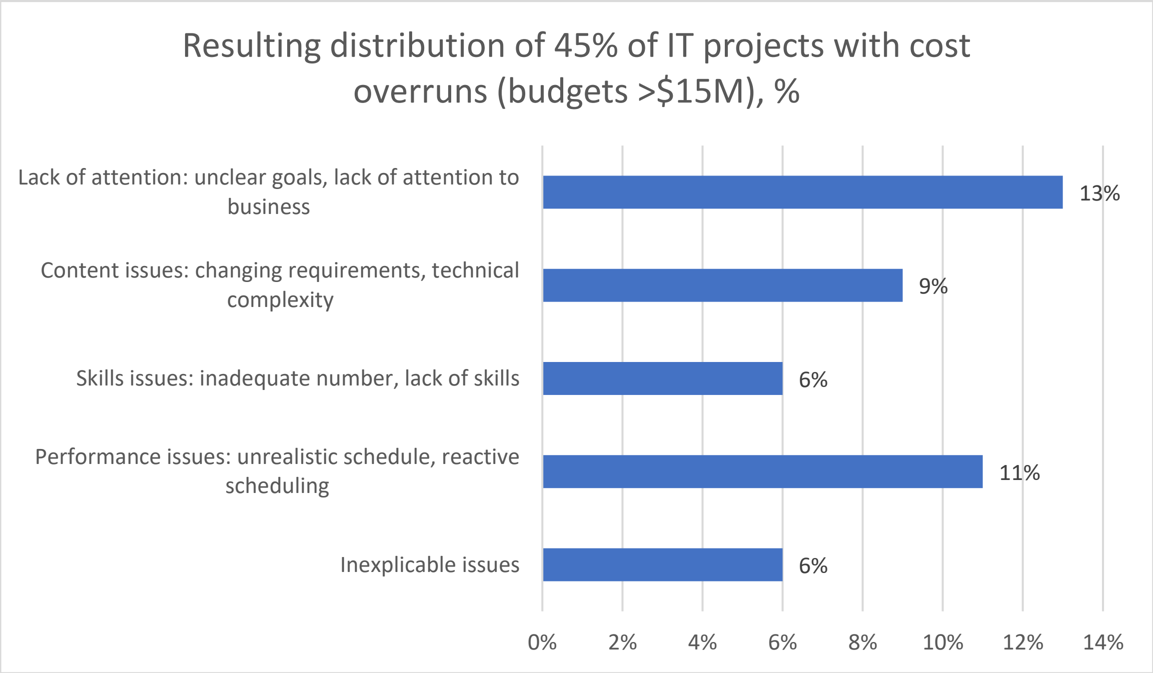


Figure 2: Four groups of problems identified by IT managers as causing most project failures

Source: https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/delivering-large-scale-it-projects-on-time-on-budget-and-on-value

The latest CHAOS study by the Standish Group, published in 2020, suggests a link between decision-making and project success. Teams with high decision-making skills deliver successful projects (63%) compared to skilled (28%), moderately skilled (20%), and non-skilled teams (18%) (Johnson, J. and Mulder, H., 2020).

Skill level	Successful	With challenges	Failed
With high skills	63%	30%	7%
With average skills	28%	61%	11%
With moderate skills	23%	51%	29%
With bad skills	18%	47%	35%

Table 2 Delaying decision skills. Source: Jim Johnson and Hans Mulder, 2021, "Endless Modernization: How Infinite Flow Keeps Software Fresh"

Over the past 25 years, the Standish Group has collected and studied 2,500 to 5,000 new project cases annually. Over those 25 years, they have added and changed observations to better understand why some projects succeed and others fail.

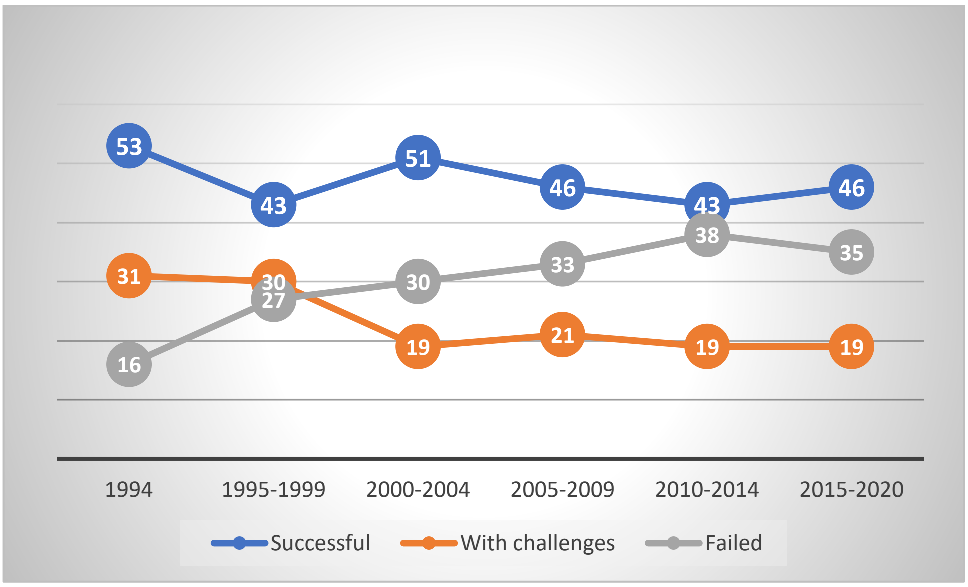


Figure 3: CHAOS survey

Source: Johnson, J. and Mulder, H., (2020). Endless modernization. Technical report, The Standish Group International, Incorporated.

3. Research methodoly

Risk assessments can be conducted to varying degrees of depth and detail using one or more different methods. Some common methods of risk identification include:

- Brainstorming method
- Delphi method
- SWOT analysis
- Root cause identification

Brainstorming is a technique for generating ideas among individuals or groups of people, where the ideas and thoughts of one individual serve to stimulate ideas among other participants. It is important to note that brainstorming belongs to the class of Synectics methods, which are not widely used due to their complexity. The key to this method is to carefully consider each idea. In practical application, the brainstorming method can encounter obstacles, because as a result, many ideas can be proposed that will be difficult or impossible to develop.

The Delphi method uses an anonymous survey of experts to identify risks. As a result, initial responses from experts are collected, subject to further analysis and generalization, and only then sent back to experts for review and further interpretation of risks based on the responses of others. This method allows you to analyze the risks several times, coordinate them, but one of the disadvantages is that it requires the participation of every member of the group, it takes a lot of time and is a heavy burden.

SWOT (Strength, Weakness, Opportunity and Threat) is a method that examines each aspect of SWOT to increase the breadth of risks being considered. This method focuses on internal (organizational strengths and weaknesses) and external (opportunities and threats) factors. The method has become very popular when conducting research in various business sectors, but one of the weaknesses of the SWOT analysis is the superficiality of the evaluated factors, only a qualitative description of the factors, and subjectivity. The conclusions drawn on its basis are descriptive without recommendations and priorities. The results of its implementation need additional analysis and methodological data, which will make it difficult to get an understanding in the field of risk management.

Root cause analysis helps identify additional dependent risks. Identified risks can be linked to their common root causes. The essence of this method is the detailed consideration of all possible risks, which are initially the result of certain activities and the creation of cause-and-effect relationships. One of the disadvantages of this method is the need for documentation, on which the identification, disclosure and analysis of risks can be based.

Taking into account the limitations of these methods the survey method was chosen for quantitative risk analysis. To conduct the survey, risks encountered in IT projects were grouped based on previous studies into the following categories:

- Project scope and requirements risks
- Resource risks
- Schedule risks
- Technological risks
- Communication risks
- Quality and compliance risks
- Security risks

For each category, four questions were included to assess the impact of the given risk on a scale of 1-5. This will allow for comparing the average impact within each category, as well as identify which categories have the highest and lowest average impacts.

The main objective of this survey is to study and evaluate the impact of various risks on project performance in IT organizations. To achieve this, the quantitative approach chosen allows for data collection, statistical analysis and generalization of results. The survey design is consistent with the research objective of assessing the multifaceted nature of risks within IT organizations. In this way, we can systematically collect quantitative data on respondents' perceptions.

This method is an effective way to reach geographically dispersed IT professionals, which is important to gain a wide range of perspectives, and the digital nature of the data it is based on provides clarity of interpretation. Additionally, given the dynamic nature of the IT industry, this approach allows us to assess current approaches and responses to risk.

To carry out the survey, IT organization specialists were selected as the target. Given the dynamic and multifaceted nature of IT project environments, a purposive sampling approach is most appropriate for this study. Purposive sampling allows you to choose those participants who have the necessary knowledge and experience in the field of risk management of IT projects and are familiar with the risks inherent in the projects. Selection criteria were developed to include a diverse range of IT professionals, including project managers, team members and stakeholders, to ensure a holistic perspective. To mitigate potential bias, the survey recruited participants from a variety of industries, project sizes, and geographic locations. This diversity minimizes the risk of skewed data, ensuring that the results are applicable to a wide spectrum of IT projects. In addition, anonymity and confidentiality were emphasized throughout the survey to encourage honest and unbiased responses. Fifty-seven participants were included in the survey due to practical constraints, such as time and budget. The study's narrow focus on specific IT project risk management measures provides a targeted approach, justifying the use of a smaller sample size. This sample size is adequate to capture key insights and patterns related to IT project risk management and allows for meaningful comparisons. This is presented in the attached Appendix 1. The survey was conducted online, which facilitated its effective dissemination among IT professionals and expedited the data collection process.

According to the obtained results, several steps were included for data analysis, providing a comprehensive analysis:

Data filtering and preparation: Before starting the analysis, the data collected during the research is filtered and prepared. This includes checking responses for completeness and accuracy. Missing or irregular data points are corrected to enhance the reliability of subsequent analyses.

4. Analysis

In this work, the analysis of the impact of risks of IT projects was carried out based on the data obtained from the results of the survey. There are seven factors in the database:

- Project scope and requirements risks
- Resource risks
- Schedule risks
- Technological risks
- Communication risks
- Quality and compliance risks
- Security risks

Analysis and construction of models were conducted using Excel and SPSS programs. To summarize and analyze the survey responses, descriptive statistics (Descriptive Statistics) were implemented in the work, to gain insight into various aspects of project management. Descriptive statistics provide a concise and meaningful summary of the key features of a database (Abbott, 2014).

By comparing mean scores, standard deviations, and other measures, we can identify areas of relatively higher or lower consensus. This helps prioritize areas that may require more attention in project management.

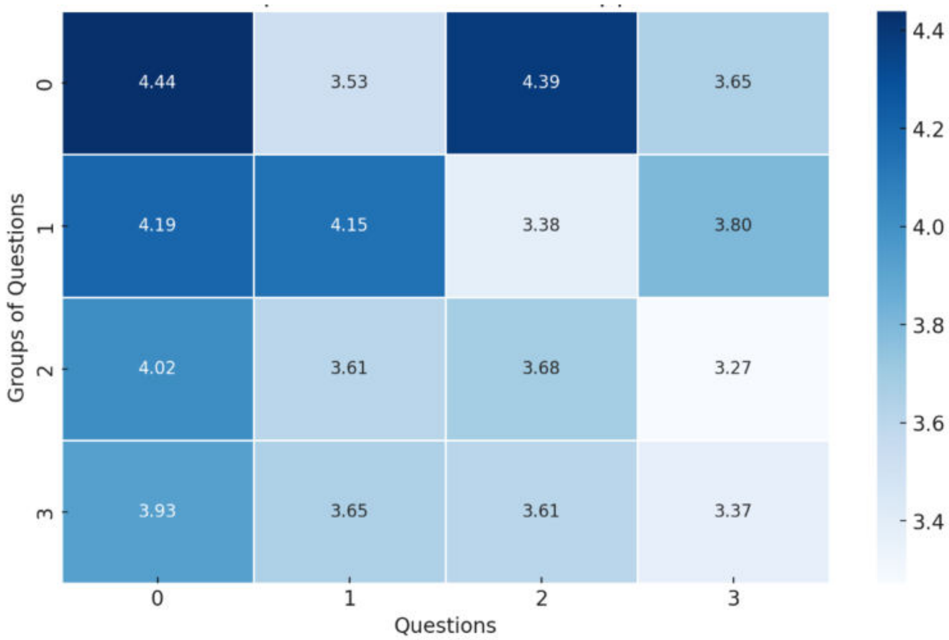


Figure 4. Heatmap of Mean Values from results of statistical description

Source: https://docs.google.com/spreadsheets/d/1iN0XTUMgNtdcN-u71HKxpIANs0-bCodf/edit?gid=766945934#gid=766945934

The figure 4 heatmap based on the mean values extracted from results of statistical description. The color gradient helps highlight the higher risk factors in darker shades, while lower values appear lighter, making it easier to visualize the significance of different risks. As we can see, the average value of insufficient or unclear program requirements of 4.44 suggests a high impact.

This can lead to project delays, cost overruns, and possible revisions, negatively impacting overall project performance. A mean of 3.53 for frequent project scope changes indicates a moderate effect. Although not as stringent as the unclear requirements, it carries the potential for increased costs and extended schedules. With a mean of 4.39 for ambiguous project objectives, this indicates a high impact. Uncertainty can lead to misunderstandings, affecting project implementation and increasing the likelihood of economic losses. A mean of 3.65 for alignment with stakeholder expectations indicates a moderate impact.

This can lead to discrepancies between project outcomes and stakeholder expectations, which can affect project success. A mean of 4.19 for underbudgeting indicates a high impact. This can lead to a lack of resources, affecting the quality of the project resulting in economic losses. Lack of necessary knowledge and skills: A mean of 4.15 indicates a high impact. Inadequate skills can lead to errors, delays, and cost overruns, adversely affecting project economics.

With a mean of 3.38 for resource constraints, there is a moderate effect. This can lead to challenges, but may not be as severe as budget-related risks. A 3.80 average for supplier or vendor-related risks allows for a moderate impact. Problems with suppliers or vendors can cause delays or cost overruns. A mean of 4.02 for Unreasonable Project Schedule suggests a high impact. Unrealistic schedules can lead to rushed work, errors, and increased costs. A mean of 3.68 for unplanned delays, a mean of 3.65 for technology compatibility issues, a mean of 3.61 for security vulnerabilities, and a mean of 3.37 for integration challenges indicate a moderate impact.

Meanwhile, a mean of 4.20 for poor communication between stakeholders and a mean of 4.16 for the risk of not meeting quality standards indicate a high impact. A mean risk of a security breach of 3.98 suggests moderate exposure.

Security breaches can lead to additional costs to address vulnerabilities and potential economic losses. Overall, the research findings highlight significant economic risks associated with various aspects of project management. Prioritizing risk mitigation strategies, ensuring effective communication, and allocating sufficient resources and budget are critical to minimizing economic losses and increasing project success.

Addressing areas such as insufficient budget allocation, poor communication, and security vulnerabilities should be a priority in project management strategies. Regular monitoring of project plans and adaptation to risk assessment are essential to successful project outcomes. It is important to note that these interpretations are based on statistical measurements and may not capture the full complexity of individual projects. The specific context of projects and industry standards must be taken into account when making strategic decisions.

In summary, the high-impact risks are insufficient budget allocation, unclear project requirements, unreasonable project schedules, poor communication, and security vulnerabilities. These areas require special attention because of their potential to significantly affect project outcomes and economic outcomes.

Moderate impact risks include resource constraints, dependence on external factors, technological challenges, and compliance issues. Although not as severe as high-impact risks, they also require active management to prevent negative consequences. In the next step, Anova's Excel program was applied to the database.

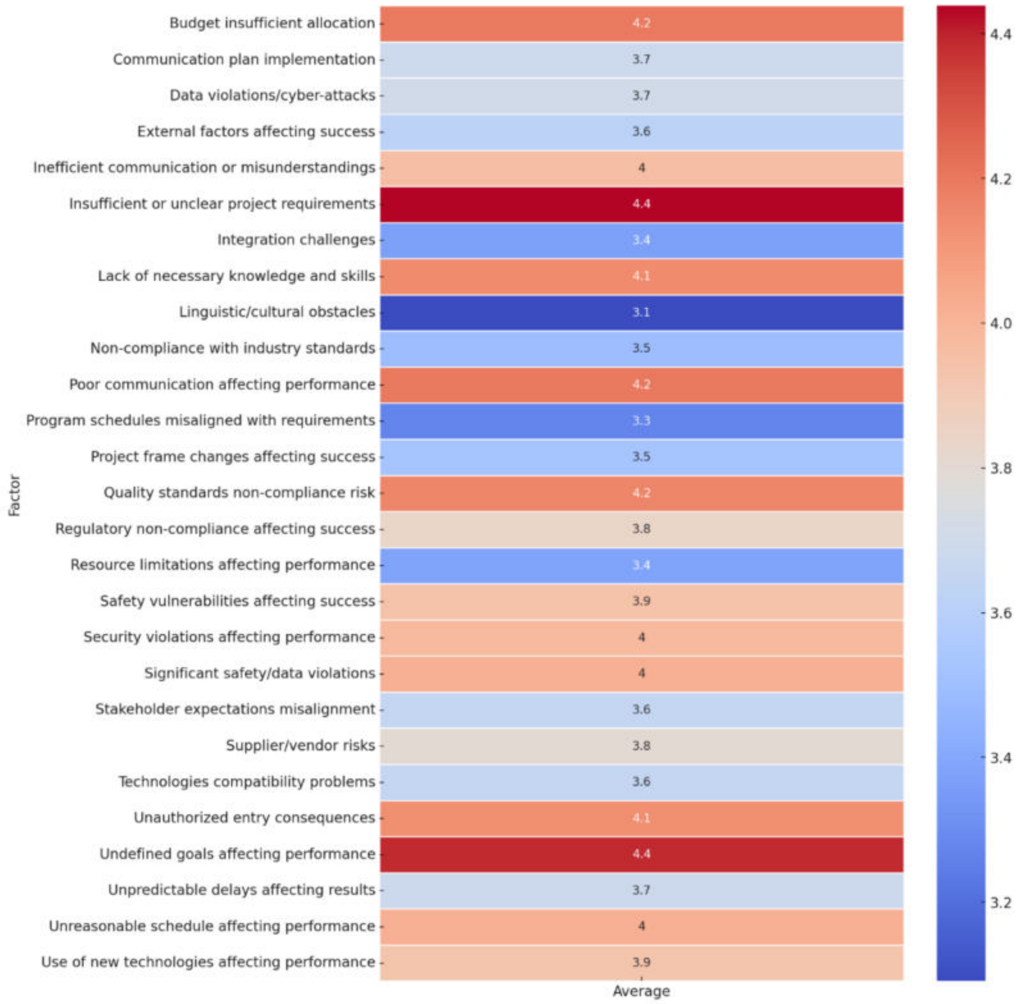


Figure 5. Heatmap of factors affecting project performances

Source: https://docs.google.com/spreadsheets/d/1iN0XTUMgNtdcN-u71HKxpIANs0-bCodf/edit?gid=1317595904#gid=1317595904

The figure 5 heatmap representing the average impact of various factors on project performance. The color intensity highlights the severity of each factor, with warmer colors indicating a higher average impact

The analysis shows significant differences between the different groups of the database, that is, the differences between the seven risk categories we identified, for each of which four questions were included. Hence, it is assumed that certain project risk factors differ significantly between different projects, regions, or divisions of the organization. Significant differences between groups suggest that these factors may have significant economic consequences. For example, in project management, the different risk levels of different projects can lead to significant differences in resource allocation, profitability, or the overall success of those projects. Understanding these significant differences can help better allocate resources. Economically, efficient allocation of resources based on these fluctuations can increase efficiency, minimize costs, and maximize revenues. For example, if some risk factors differ significantly between projects, prioritizing resource allocation based on those differences can optimize project outcomes. Significant variation between groups can also highlight areas with potential for improvement or growth. Economically, it can identify strengths or opportunities to reduce weaknesses in certain areas, leading to improved performance or market advantages. Recognizing significant differences between groups is important for risk management and investment strategies. Economically, this indicates the need for tailored risk mitigation approaches or targeted investment strategies based on these differences to optimize returns and minimize potential losses. In contexts outside of project risks, significant variation between groups may indicate different market segments or customer behavior. Understanding these differences can help target marketing strategies or customize services to meet specific customer needs, potentially increasing market penetration and revenue generation.

In general, the significance of variation between groups in ANOVA analysis has economic implications, and guides decision-making processes, resource allocation strategies, risk management, and opportunities for growth and market advantage in different segments or categories.

The resulting p-value of 1.1537E-23 is significantly decreasing and contradicts the null hypothesis. Such a p-value indicates, that in the context of the analysis, there are significant discrepancies between group means, which means significant variation within the variables studied. At the same time, the F-statistic of 6.822, which exceeds the critical F-value of 1.493, further supports the rejection of the null hypothesis. This statistical conclusion indicates a high level of confidence in confirming the existence of significant differences between the different groups included in the database. A significant difference observed between groups highlights different risk profiles, disparities in resource allocation or possible different market conditions among different project typologies or organizational segments. This difference may imply disproportionate resource utilization efficiency or distinct levels of risk exposure, thereby requiring specific strategic approaches to effective management and resource optimization. Furthermore, the statistical significance clarified by ANOVA analysis suggests the need for decision-making strategies. The statistical validation of significant differences highlights the importance of using these variations as potential avenues for growth and competitive advantage. Identifying and exploiting these differences can uncover hidden market opportunities, inform market penetration strategies, and facilitate tailored product and service offerings, thereby promoting market competitiveness and economic flexibility.

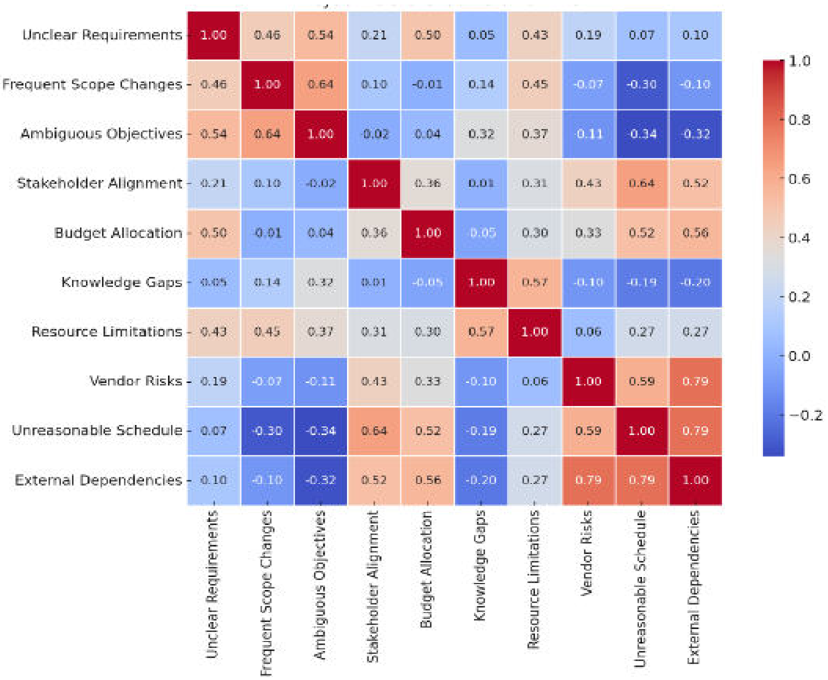


Figure 6. Project Factors Correlation Matrix

Source: https://docs.google.com/spreadsheets/d/1iN0XTUMgNtdcN-u71HKxpIANs0-bCodf/edit?gid=1366267207#gid=1366267207

The figure 6 heatmap based on the mean values. Here is the visual correlation matrix for the project-related factors. Each cell displays the correlation coefficient between pairs of factors, with color gradients indicating the strength and direction of the correlation.

Correlation analysis provides insights into the relationships between various project management factors. We find that insufficient or unclear project requirements are positively correlated with frequent project scope changes and ambiguous project objectives (Shi, H., et al., 2017). Stakeholder expectations may not align well with project objectives when requirements are unclear. Under-budget allocation is positively related to resource constraints and supplier or vendor-related risks. The lack of necessary knowledge and skills among team members has a weak positive correlation with resource constraints. Unreasonable project schedules are weakly positively associated with externalities and unanticipated delays. Project schedules may not match actual project requirements well, indicating potential scheduling challenges. The use of new technologies is positively correlated with technology compatibility issues, security vulnerabilities, and integration challenges. Technology-related factors have an impact on project performance, especially in terms of compatibility and security. Poor communication among project stakeholders is positively associated with ineffective communication among team members. Language or cultural barriers have a weak positive correlation with project outcomes (Han, P. C., 1996). Implementation of communication plans is positively correlated with effective communication. Failure to comply with industry standards is positively associated with failure to comply with regulatory requirements. Additionally, failure to meet regulatory requirements has a negative correlation with project success.

The risk of not meeting quality standards did not show a strong correlation with other factors in the analysis. Security breach risk has a weak negative correlation with project performance. Program security vulnerabilities do not show a strong correlation with the risk of security breaches. The consequences of unauthorized access to sensitive data or systems have a significant negative correlation with project success.

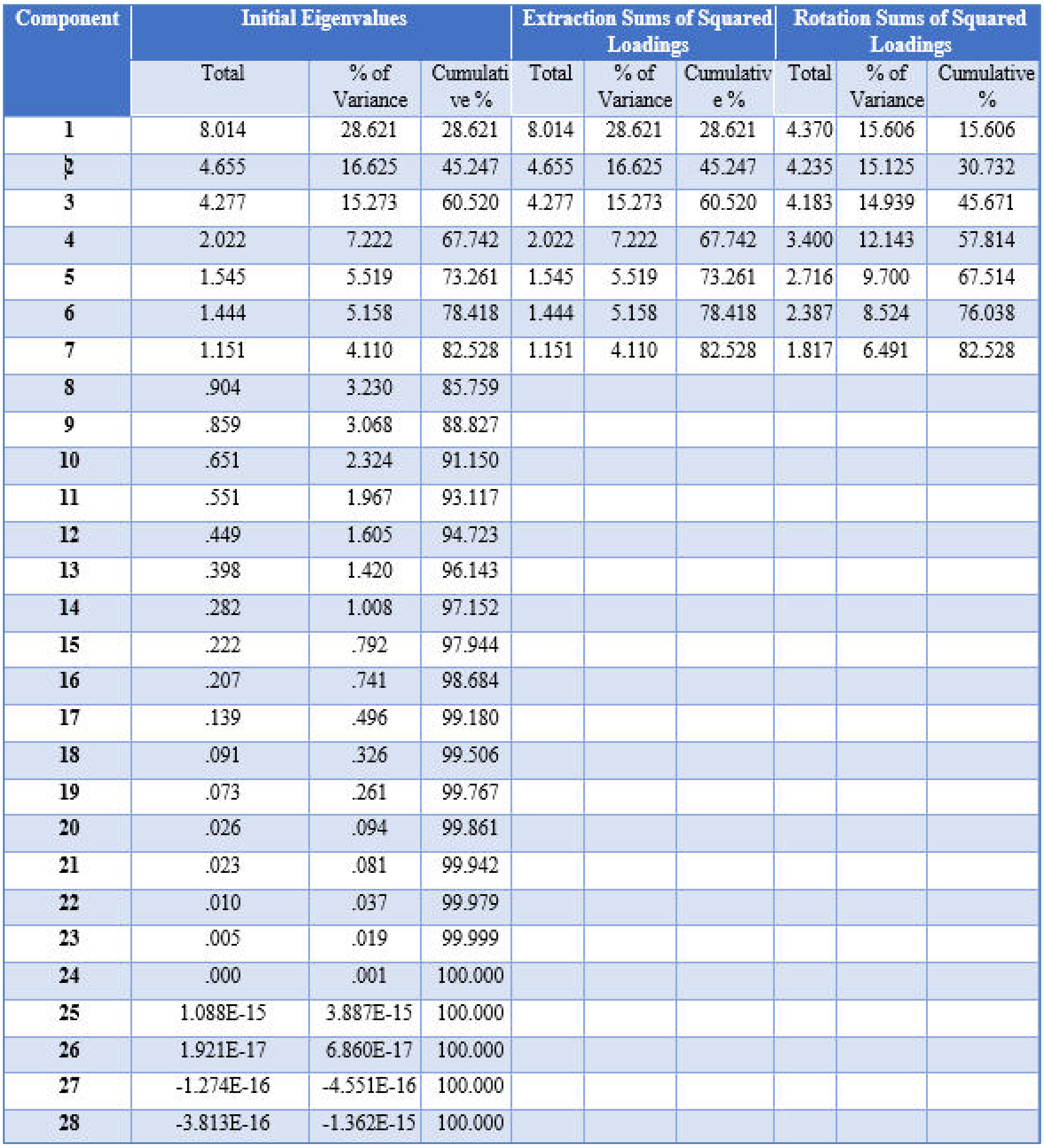
In summary, resource-related factors, including budget allocation and skills, are correlated with project outcomes.

The impact of IT project risks in the work was also investigated through factor analysis of multivariate statistics. Factor analysis is used to identify underlying factors that explain observed correlations between variables in data sets by dividing the set of variables under study into a small number of groups.

The following factors included in the survey were selected for multivariate analysis, the data on which are presented in Table 1:

1. To what extent do inadequate or unclear project requirements affect project performance (X1)?
2. To what extent do frequent project scope changes affect the success of your projects (X2)?
3. Please assess the impact of ambiguous project objectives on project performance (X3).
4. To what extent are the stakeholders' expectations consistent with the project's goals (X4)?
5. How does insufficient budget allocation affect project performance (X5)?
6. Please assess the impact of the lack of necessary knowledge and skills of team members on the success of the project (X6).
7. To what extent do resource limitations (hardware, software, tools) affect project results (X7)?
8. How significant are supplier or vendor-related risks in your projects (X8)?
9. Please assess the impact of unreasonable project schedule on project performance (X9)?
10. To what extent does dependence on external factors affect the success of your project (X10)?

11. To what extent do unforeseen delays affect project results (X11)?
12. To what extent are project schedules consistent with actual project requirements (X12)?
13. How does the use of new technologies affect the implementation of the project (X13)?
14. Please assess the impact of technology compatibility issues on project success (X14).
15. To what extent do security vulnerabilities affect the success of your projects (X15)?
16. How significant are integration challenges in your projects (X16)?
17. How does poor communication between project stakeholders affect project performance (X17)?
18. Please evaluate the impact of ineffective team member communication or misunderstanding on project success (X18).
19. To what extent do language or cultural barriers affect the results of your project (X19)?
20. How well is the communication plan followed and implemented in your programs (X20)?
21. How does the risk of non-compliance with industry standards affect project performance (X21)?
22. Please assess the impact of non-compliance with regulatory requirements on project success (X22).
23. To what extent does the risk of not meeting quality standards affect the results of your project (X23)?
24. How significant are the consequences of security or data breaches due to non-compliance with security standards or regulations in your projects (X24)?
25. How does the risk of security breaches affect project performance (X25)?
26. Please assess the impact of project security vulnerabilities on project success (X26).
27. To what extent do data breaches or cyber-attacks affect the results of your project (X27)?
28. How significant are the consequences of unauthorized access to sensitive data or systems in your projects (X28)?



Component	Initial Eigenvalues			Extraction Sums of Squared Loadings			Rotation Sums of Squared Loadings		
	Total	% of Variance	Cumulative %	Total	% of Variance	Cumulative %	Total	% of Variance	Cumulative %
1	8.014	28.621	28.621	8.014	28.621	28.621	4.370	15.606	15.606
2	4.655	16.625	45.247	4.655	16.625	45.247	4.235	15.125	30.732
3	4.277	15.273	60.520	4.277	15.273	60.520	4.183	14.939	45.671
4	2.022	7.222	67.742	2.022	7.222	67.742	3.400	12.143	57.814
5	1.545	5.519	73.261	1.545	5.519	73.261	2.716	9.700	67.514
6	1.444	5.158	78.418	1.444	5.158	78.418	2.387	8.524	76.038
7	1.151	4.110	82.528	1.151	4.110	82.528	1.817	6.491	82.528
8	.904	3.230	85.759						
9	.859	3.068	88.827						
10	.651	2.324	91.150						
11	.551	1.967	93.117						
12	.449	1.605	94.723						
13	.398	1.420	96.143						
14	.282	1.008	97.152						
15	.222	.792	97.944						
16	.207	.741	98.684						
17	.139	.496	99.180						
18	.091	.326	99.506						
19	.073	.261	99.767						
20	.026	.094	99.861						
21	.023	.081	99.942						
22	.010	.037	99.979						
23	.005	.019	99.999						
24	.000	.001	100.000						
25	1.088E-15	3.887E-15	100.000						
26	1.921E-17	6.860E-17	100.000						
27	-1.274E-16	-4.551E-16	100.000						
28	-3.813E-16	-1.362E-15	100.000						

Table 3. Total Variance Explained. The factor analysis was carried out using the SPSS software package.

Source: https://docs.google.com/spreadsheets/d/1iN0XTUMgNtdcN-u71HKxpIANs0-bCodf/edit?gid=1102970142#gid=1102970142

Accordingly, three factors were selected for analysis. The first explains 28.621% of the total variance, the second explains 16.625%, the third explains 15.273%, and the three factors together explain 60.6% of the total variance (Table 3).
The next step in interpreting the results of the factor analysis is to look at the rotated component matrix of the factor coefficients. This table is the main result of the factor analysis, in which the results of the classification of variables by factors are expressed.
As can be seen from Table 4, the 13 studied variables were classified according to three factors: 5 variables can be included in the first one, 5 variables in the second one, and 3 variables in the third one.

	Component		
	1	2	3
X_{1}	-.143	.204	.056
X_{2}	-.426	.178	-.070
X_{3}	-.133	.139	-.425
X_{4}	.224	.115	.687
X_{5}	.376	.092	.430
X_{6}	.225	.818	-.276
X_{7}	-.245	.814	.226
X_{8}	.045	.053	.491
X_{9}	.041	-.264	.439
X_{10}	.214	.018	.769
X_{11}	.058	.110	.878
X_{12}	-.192	.111	.030
X_{13}	.047	.408	.408
X_{14}	.076	.807	.277
X_{15}	.452	.447	.040
X_{16}	.242	.280	-.014
X_{17}	.170	.671	-.019
X_{18}	.208	.623	-.118
X_{19}	-.167	.293	-.045
X_{20}	-.233	.347	.251
X_{21}	.401	-.019	.316
X_{22}	.203	-.058	.416
X_{23}	.002	.115	.296
X_{24}	.728	-.154	.296
X_{25}	.710	.480	.111
X_{26}	.860	.285	-.038
X_{27}	.713	.123	.071
X_{28}	.864	-.108	.121

Table 4 Rotated Component Matrix.

The table was created by authors using SPSS software. Extraction Method: Principal Component Analysis. Rotation Method: Varimax with Kaiser Normalization.

We tentatively named the first factor "**Project Security Risks**", because it includes the risk of compatibility violations (0.728), the risk of unauthorized access (0.71), the risk of cyber security threats (0.86), the risk of cyber security incidents (0.713), the risk of consequences of unauthorized access (0.864).

The second factor was named "**Project Internal Risks**" because it includes the risk of lack of necessary knowledge and skills of team members (0.82), the risk of resource limitations (0.81), technology compatibility issues (0.807), the risk of communication between stakeholders and (0.671), risk of gaps in team communication (0.623).

The third factor named "**External Risks**" includes three variables: risk of alignment of expectations (0.68), risk of external dependence (0.76), and risk of delay effect (0.879).

Reliability analyses.

According to Cronbach's test, the tabular value was obtained as 0.887, which means that the alpha values of the factors have acceptable values (exceeding 0.5), therefore the data are reliable for conducting analysis.

Thus, since the reliability of the data is checked, the following hypotheses are proposed in the work:

- **Hypothesis 1**. Project security risks are affected by dynamic project factors, such as technological advances, regulatory changes, and human behavior.
- **Hypothesis 2**. Internal project risks affect outcomes.
- **Hypothesis 3**. External risks affect project performance.

To test these hypotheses, the logistic regression model was employed.

The investigated logistic model has the following form:

$$P(Y = 1|X = (X_1, X_2, X_3)) = \frac{e^{\tilde{Y}}}{1 + e^{\tilde{Y}}} = \frac{1}{1 + e^{-\tilde{Y}}}$$

Where:

In our example, the linear regression equation looks like this:

$$\tilde{Y} \ = \beta_0 + \beta_1 X_1 + \beta_2 X_2 + \beta_3 X_3$$

This equation gives the probability that one outcome $Y = 1$ based on the predictors $X_{1,} X_2$ and X_3.

Where:

Project success depends on risk management: $Y_i = \begin{cases} 0, & if\ the\ event\ does\ not\ occur \\ 1, & if\ the\ event\ occurs \end{cases}$

Project security risks: X_1

Project implementation risks: X_2

Risks of external dependence: X_3

Unknown model parameters: β_0, β_1, and β_3.

Therefore, a logistic regression analysis is performed between the factors of the dependent variable (project success depending on risk management) and the independent variables (project security risks, project internal risks, and external risks).

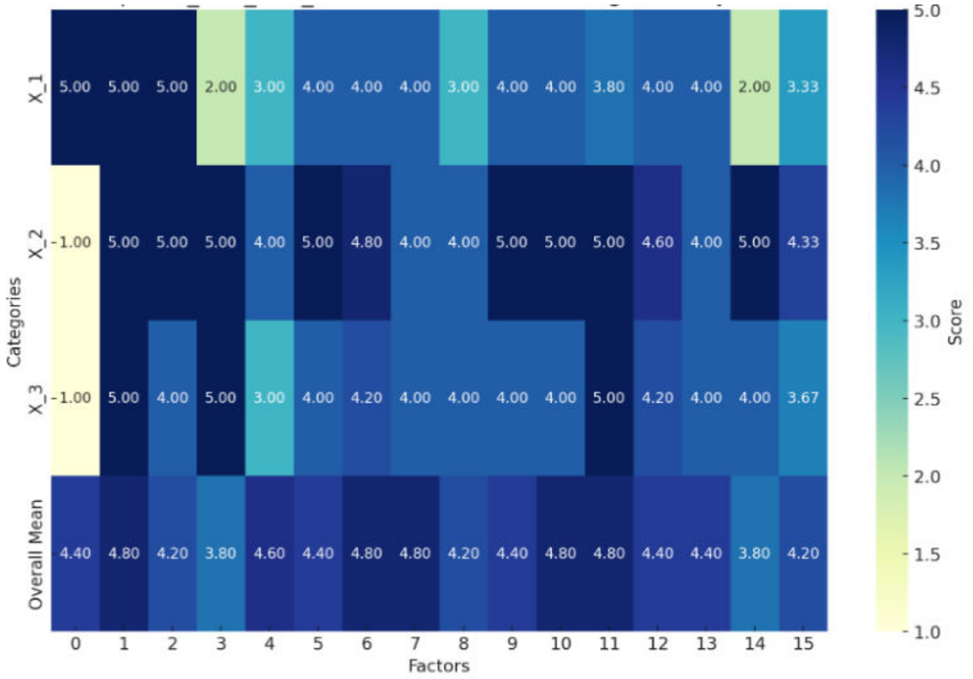
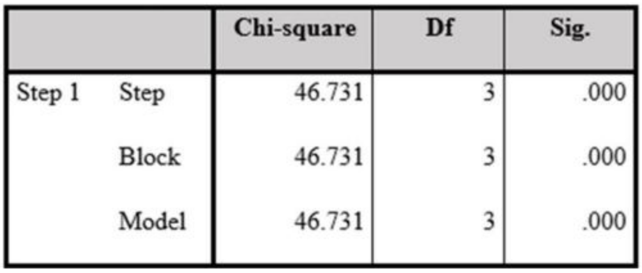


Figure 7. X_1, X_2, X_3 overall mean scores overall average ratings of factors

Source: https://docs.google.com/spreadsheets/d/1iN0XTUMgNtdcN-u71HKxpIANs0-bCodf/edit?gid=1366267207#gid=1366267207

Here is the heatmap of the overall mean ratings for X_1 , X_2 , X_3 and the general average ratings of project factors. Each row corresponds to one of these categories, with the color intensity reflecting the score values across different factors.
The relationship between the dependent variable and the independent variables is checked by applying the Omnibus Tests of Model Coefficients, the results of which are shown in Table 5. The Chi-Square value of the model is 46.731, and the p-value is less than 0.05, which means that our model is highly significant (Table 5).



		Chi-square	Df	Sig.
Step 1	Step	46.731	3	.000
	Block	46.731	3	.000
	Model	46.731	3	.000

Table 5 A test of coefficients for the Omnibus Model. The table was created by authors using SPSS software

In logistic regression, to determine multicollinearity between independent variables, numerical errors must be detected and problematic variables must be excluded from the analysis. Therefore, the standard error (SE) column of the variables in the equation table is checked if there is any value above 2.0. Thus, we can conclude that there is no problem with the variables being significantly dependent on each other, as the SE values in the table are below 2.0.

		B	S.E.	Wald	Df	Sig.	Exp(B)
Step 1[a]	X1	.424	.397	1.137	1	.007	1.231
	X2	.388	.355	1.199	1	.005	1.474
	X3	.271	.377	.515	1	.008	1.654
	Constant	.264	1.929	.019	1	.009	.768

a. Variable(s) entered on step 1: X1, X2, X3.

Table 6. Variables in Equations. The table was created by authors using SPSS software

From the obtained results, it can be seen that the p-value for the project safety risks factor is (0.007), for the internal risks factor (0.005), and for external risks is (0.007), which are less than 0.05 and also less than 0.01, which means that these independent variables are statistically significant (Table 6).
According to the final results, we have the following picture:
Hypothesis 1: Project security risks are affected by dynamic project factors such as technological progress, regulatory changes, and human behavior, the hypothesis is accepted.
Hypothesis 2: The hypothesis that internal risks of the project affect the results is accepted.
Hypothesis 3: The hypothesis that external dependency risks affect project performance is accepted.
The value of Exp (B) for the risk factor of external dependence is 1.654, which means that for each one-degree increase in external dependence on the rating scale, the probability of impact on project performance increases by 1.654 times. In other words, for every one-step increase in the risk level of external dependence, the probability of impact on project performance increases by 65 percent over the previous step. It is observed that there is a highly positive relationship between external dependency risks and the impact on project performance.

The value of Exp (B) for the project safety risk factor is 1.231, which means that increasing the risk by one degree increases the probability of impact on the dynamic factors of the project by 1.231 times. With each degree of increase in the level of security risks of the project, the probability of impact on the dynamic factors of the project increases by 23 percent compared to the previous degree. Thus, it is observed that there is a positive relationship between project security risks and the impact on project dynamic factors.

The value of Exp (B) for the internal risk factor of the project is 1.474, which means that increasing the risk by one degree increases the probability of impact on the results by 1.474 times. With each degree of increase in the level of internal risks of the project, the probability of impact on the dynamic factors of the project increases by 47 percent compared to the previous degree. Thus, it is also observed that there is a positive relationship between internal project risks and their impact on outcomes.
Based on the results of logistic regression, and the results of parameter estimation to extract the probabilities of different situations, we will have the following regression equation:

$$\ln\left(\frac{P}{1-P}\right) = \hat{Y}$$

$$\hat{Y} = 0.264 + 0.424 * 4.4 + 0.388 * 4.8 + 0.271 * 4.33 = 5.154$$

$$p = \frac{1}{1 + e^{-5.154}} = 0.89425692$$

In other words, if the impact of security risks, internal risks, and external risks in the IT organization is rated as high, the success of the project, depending on risk management, is 0.894 or 89.4%.

5. Conclusion

The significance of risk management has grown remarkably for contemporary organizations, as risks can lead to both detrimental losses and potential opportunities. A robust risk management framework can effectively minimize and avert risks. This research delved into the theoretical foundations of risk and essential risk management practices, emphasizing risk identification as a pivotal phase. Various risk assessment techniques were analyzed, each presenting distinct advantages and disadvantages. The findings from the survey underscored critical risks associated with project management, such as cybersecurity vulnerabilities, unauthorized access, skill shortages, resource constraints, and communication deficiencies. A correlation analysis revealed that effective communication and the adoption of technology are essential for the success of projects. Furthermore, logistic analysis demonstrated that external dependencies, security concerns, and internal risks have a substantial influence on project outcomes. To lessen these risks, numerous strategies have been suggested, namely the adoption of strong encryption techniques, the implementation of multi-factor authentication, conducting regular security audits, providing employee training programs, formulating incident response plans, and building a strong sense of security awareness throughout the companies. Moreover, it is advisable to perform geopolitical risk evaluations, remain informed regarding regulatory developments, and mitigate dependence on individual external entities to alleviate external risks. These strategies are designed to foster a secure and resilient environment for IT projects, thereby enhancing their likelihood of success.

Declaration of conflicting interests

The authors declared that there are no potential conflicts of interest for the research, authorship, and/or publication of this paper.

Funding

The authors did not receive any financial support for the research, authorship, and/or publication of this paper.

References

Abbott, M.L., 2014. Understanding educational statistics using Microsoft Excel and SPSS. John Wiley & Sons.

Abubakar, N., & Bello, G. B. (2013). "Strengths, weaknesses, opportunities, and threats (SWOT) analysis on Globacom Ltd". International Journal of Information Technology and Business Management, 16(1), 83-91.

Barry Boehm. (1991) Software Risk Management: Principles and Practices, Available at: https://www.cs.virginia.edu/~sherriff/papers/Boehm%20-%201991.pdf, pp. (3) 33-36.

Bennett, P. L., & Lee, L. (2006). "Risk management for IT projects: How to deal with over 150 issues and risks". XYZ Publishing.

Brad E, Trevor H, Efron, B., and Hastie, Th.M. (2016), Computer-Age Statistical Inference: Algorithms, Evidence, and Data Science. pp. 108-113, Available at: https://hastie.su.domains/CASI_files/PDF/casi.pdf.

Boehm, B. (1991). "Software risk management: principles and practices". IEEE Software, 8(1), 32-41. DOI: 10.1109/52.62930.

Cooper, D. F., Grey, S., Raymond, G., & Walker, P. (2005). "Project risk management guidelines: Managing risk in large projects and complex procurements". John Wiley & Sons.

Dale C, Stephen G, Geoffrey R, and Phil W. (2005) Project Risk Management Guidelines: Managing Risk in Large Projects and Complex Procurements, pp. 2-19.

DeMarco, T., & Lister, T. (2003). "Risk management during requirements". IEEE Software, 20(5), 99-101. DOI: 10.1109/MS.2003.1231167.

Efron, B., & Hastie, T. (2016). "Computer-age statistical inference: Algorithms, evidence, and data science". Cambridge University Press.

Han, P. C. (1996). An investigation of intercultural effectiveness of international university students with implications for human resource development. University of Arkansas.

Heygate, R. (1994). "Being intelligent about "intelligent" technology". The McKinsey Quarterly*, (4), 137-147.

Johnson, J. and Mulder, H., (2020). Endless modernization. Technical report, The Standish Group International, Incorporated.

Johnson, J., & Mulder, H. (2021). Endless Modernization: How Infinite Flow Keeps Software Fresh. Technical report, The Standish Group International, Incorporated.

Kerzner, H. (1998). "Project management: A systems approach to planning, scheduling, and controlling". John Wiley & Sons.

Lee, O. K., & Baby, D. V. (2013). "Managing dynamic risks in the global IT project: Agile risk-management using the principles of service-oriented architecture". International Journal of Information Technology & Decision Making, 12(6), 1121-1150.

Okes, D. (2019). "Root cause analysis: The core of problem-solving and corrective action". Quality Press.

PMI (2019) The Standard for Risk Management in Portfolios, Programs, and Projects, pp. 3-11.

Prikladnicki, R., Evaristo, R., Audy, J. L. N., & Yamaguti, M. H. (2006). "Risk management in distributed IT projects: Integrating strategic, tactical, and operational levels". International Journal of e-Collaboration (IJeC), 2(4), 1-18. DOI: 10.4018/jec.2006100101.

Project Management Institute. (2019). "The Standard for Risk Management in Portfolios, Programs, and Projects". Project Management Institute.

Rafael P, J. Roberto E., Jorge L.N.A, Marcelo H. Y. (2006): "Risk Management in Distributed IT Projects: Integrating Strategic, Tactical, and Operational Levels, pp. 3-4.

Shi, H., Mancuso, N., Spendlove, S., & Pasaniuc, B. (2017). Local genetic correlation gives insights into the shared genetic architecture of complex traits. The American Journal of Human Genetics, 101(5), 737-751.

Skulmoski, G. J., Hartman, F. T., & Krahn, J. (2007). "The Delphi method for graduate research". Journal of Information Technology Education: Research, 6(1), 1-21.

Tharanga, D. (2020). Critical review of risk identification techniques. University of the West of Scotland